SET THEORY AND MATHEMATICS
LECTURE NOTES DEPARTMENT OF LOGIC 2025

RADEK HONZIK

Contents

References

1. Yushiro Aoki, *Discontinuous homomorphsims on $C(X)$ with the negation of CH and a weak forcing axiom*, J. London Math. Soc. **110** (2024), no. 1.
2. Steve Awoday, *Category theory*, Oxford logic guides, no. 52, Oxford university press, 2010, 2nd edition.
3. John T. Baldwin, *The dividing line methodology: model theory motivating set theory*, Theoria **87** (2021), 361–393.
4. H. G. Dales, *A discontinuous homomorphism from $C(X)$*, American Journal of Mathematics **101** (1979), 647–734.
5. H. G. Dales and H Woodin, *An introduction to independence for analysts*, London Mathematical Society Lecture Note Series, 115, Cambridge University Press, 1987.
6. A. Dow, P. Simon, and J. E. Vaughan, *Strong homology and the Proper Forcing Axiom*, Proceedings of the American Mathematical Society **106** (1989), no. 3, 821–828.
7. Bob A. Dumas, *Discontinuous homomorphisms of $C(X)$ with $2^{\aleph_0} > \aleph_2$*, The Journal of Symbolic Logic **89** (2024), no. 2, 665–696.
8. P. C. Eklof and A. H. Mekler, *Almost free modules: Set-theoretic methods, revised edition*, North-Holland, 2002.
9. Paul C. Eklof, *Whitehead's problem is undecidable*, The American Mathematical Monthly **83** (1976), no. 10, 775–788.

10. László Fuchs, *Infinite abelian groups, volume I*, Pure and applied mathematics, A series of monographs and textbooks, no. 36, Academic press/ Elsevier, 1970.
11. Robert Goldblatt, *Topoi: The categorial analysis of logic*, Studies in logic and the foundations of mathematics, no. 98, North Holland, 1984, revised edition.
12. P. J. Hilton and U. Stammbach, *A course in homological algebra*, 2 ed., Graduate texts in mathematics, no. 4, Springer, 1997.
13. Thomas W. Hungerford, *Algebra*, Graduate Texts in Mathematics, no. 73, Springer, 2003, 12th printing.
14. Tomáš Jech, *Set theory*, Springer Monographs in Mathematics, Springer, Berlin, 2003.
15. R. Björn Jensen, *The fine structure of the constructible hierarchy*, Annals of Mathematical Logic **4** (1972), no. 3, 229–308.
16. Saunders Mac Lane, *Categories for the working mathematician*, Graduate Texts in Mathematics, no. 5, Springer, 1997, 2nd edition.
17. Angus Macintyre, *Model theory: Geometrical and set-theoretical aspects and prospects*, The Bulletin of Symbolic Logic **9** (2003), no. 2, 197–212.
18. Menachem Magidor and Saharon Shelah, *When does almost free imply free? (for groups, transversals, etc.)*, Journal of the American mathematical society **7** (1994), no. 4, 769–830.
19. Sibe Mardešić, *Strong shape and homology*, Springer Monographs in Mathematics, Springer, 2000.
20. Saharon Shelah, *Infinite abelian groups, Whitehead problem and some constructions*, Israel Journal of Mathematics **18** (1974), 243–256.
21. R. M. Solovay and S. Tennenbaum, *Iterated cohen extensions and souslin's problem*, Annals of Mathematics **94** (1971), no. 2, 201–245.
22. M. Y. Souslin, *Probleme 3*, Fundamenta Mathematicae **1** (1920).
23. K. Stein, *Analytische Funktionen mehrerer komplexer Veränderlichen zu vorgegebenen Periodizitätsmoduln und das zweite Cousinsche Problem*, Math. Ann. **123** (1951), 201–222.
24. Stevo Todorcevic, *Partition problems in topology*, Contemporary Mathematics, 84, American Mathematical Society, Providence, RI, 1989.
25. B. Velickovic and A. Vignati, *Non-vanishing higher derived limits*, Arxiv, 2021.
26. W. Hugh Woodin, *A discontinuous homomorphism from $C(X)$ without CH*, Journal of the London Mathematical Society **s2-48** (1993), no. 2, 299–315.

1. Introduction

We will discuss three famous independent mathematical problems from various areas of mathematics: from characterization of the real line, to infinite abelian group theory and functional analysis. We will briefly describe their contents, discuss their relevance, and then focus on set-theoretical reformulations which were used by set-theoretics to show their independence.

- SH denotes the statement that there are no Suslin lines.
- WC denotes the statement there exists a non-free Whitehead groups of size ω_1.
- KC denotes the statement that every homomorphism from $C(X)$ (the commutative Banach algebra of continuous real valued functions on an infinite compact space X) into any commutative Banach algebra is continuous.

SH stands for "Suslin hypothesis". Suslin asked in the 1920s, [22], whether one can replace the condition of separability in the characterization of the ordering on the reals by the weaker countable chain condition and still uniquely characterize the reals. A Suslin line is a hypothetical witness for the negative answer: it is a dense complete linear order satisfying the countable chain condition which fails to be separable. Existence of this line is equivalent to the existence of an ω_1-Suslin tree. See the appropriate sections of [14] for details.

WC stands for the "Whitehead conjecture" in the infinite abelian group theory. Whitehead asked in the 1950s whether there exists a non-free abelian group G of size ω_1 such that every surjective homomorphism onto G with kernel $\mathbb{Z}$ splits (a group satisfying this property is called "Whitehead"). By a result of Stein from 1951 every countable Whitehead group is free ($\neg$WC holds in the countable case in our notation). See [9] for a clearly written summary and definitions and the book [8] for more context and generalizations.

KC stands for "Kaplansky conjecture" in Banach algebra theory. Kaplansky asked around 1947 whether every algebra homomorphism from $C(X)$, where X is any infinite compact Hausdorff space and $C(X)$ is the Banach algebra of continuous real valued functions, into any other commutative Banach algebra is continuous ("automatic continuity"). See the book [5] for more details and alternative definitions and [26, 7, 1] for more context a recent development.

Remark 1.1. Suslin, Whitehead[1] and Kaplansky apparently did not commit to a specific solution to their questions. We chose the uniform notation SH, WC, KC for easier reading: All three statements follow from PFA and all of them are refuted from $V = L$.

In all three cases, the key step for showing independence over ZFC is to identify a set-theoretic combinatorial property which is equivalent (or at least implies) the original mathematical statement. For SH, this is the non-existence of ω_1-Suslin trees, for WC the existence of uniformizations of certain colorings of ladders on stationary sets, and for KC the non-existence of strictly increasing maps from 2^{ω_1} ordered lexicographically into ω^ω ordered by eventual domination.

Let us first review additional set-theoretic assumptions which resolve these problem over ZFC. The theorem in particular implies that SH, WC, KC are independent over ZFC.

Theorem 1.2. *The following hold:*

(i) MA_{ω_1} *implies* SH [21] *and* WC [20, 9], *and* PFA *implies* KC [5, 24].

(ii) CH *implies* $\neg$KC [4], $\diamondsuit$ *implies* $\neg$SH [15], *and* $\diamondsuit(S)$ *for every stationary* $S \subseteq \omega_1$ *implies* $\neg$WC [20, 9].

Remark 1.3. The argument for KC in [5] goes by constructing a generic extension via a ccc iteration which yields simultaneously MA_{ω_1} and a combinatorial property which implies KC. Todorcevic noticed in [24, Theorem 8.8] that this combinatorial property already follows from PFA (see [24, p. 87] for more historical details on this point). It is open whether MA_{ω_1} is necessary for KC; see [1] which constructs a model with $\neg$KC, $\neg$CH and a weak fragment of MA_{ω_1}.

[1]It is sometimes suggested that Whitehead conjectured that all Whitehead groups of size ω_1 are free (for instance in [1]) possibly because Stein proved in the early 1950s that all countable Whitehead groups are free. But there is no general consensus on the notation.

2. Set-theoretic background

We will briefly review notions which appear in Theorem 1.2 to make these notes relatively self-contained.

2.1. Stationarity

We will discuss the concept of stationarity only on ω_1, but it is meaningful on any ordinal of uncountable cofinality.

Definition 2.1. A set $C \subseteq \omega_1$ is called *closed unbounded, club* if it satisfies:
(i) C is unbounded in ω_1: for every $\alpha < \omega_1$ there is $\beta \geq \alpha$ with $\beta \in C$.
(ii) C is closed: whenever $\alpha < \omega_1$ is a limit ordinal and $C \cap \alpha$ is unbounded in α, then $\alpha \in C$.

Lemma 2.2. *If C and D are clubs in ω_1, then $C \cap D$ is a club in ω_1*

Proof. We first show that $C \cap D$ is closed. This is clear: if α is a limit ordinal and $C \cap \alpha$ and $D \cap \alpha$ are both unbounded in α, then by closedness of C, D, $\alpha \in C \cap D$.

The key of the proof is to show the unboundedness. Let $\alpha < \omega_1$ be given, we wish to find some $\beta \geq \alpha$ such that $\beta \in C \cap D$. Let us construct by recursion a sequence $\langle c_i \,|\, i < \omega \rangle$ of elements of C and $\langle d_i \,|\, i < \omega \rangle$ of elements of D as follows. Choose $c_0 \in C$ and $d_0 \in D$ so that $\alpha < c_0 < d_0$. In general, in the step $n+1$, choose $c_{n+1} \in C$ and $d_{n+1} \in D$ so that $\dots c_n < d_n < c_{n+1} < d_{n+1}$. Let us denote $c = \sup\{c_i \,|\, i < \omega\}$ and $d = \sup\{d_i \,|\, i < \omega\}$. First note that $c = d$ and that c (and d) is a limit ordinal of countable cofinality. By closedness of C and D, $c \in C \cap D$. □

Exercise. Let C be a club. Let us denote as D the set of all limit ordinals in C. Show that D is a club.

Exercise. Let C be a club and let $\mathrm{Lim}(C)$ be the set of limit points of C, where $\alpha \in C$ is a limit point of C if $C \cap \alpha$ is unbounded in α. Show that $\mathrm{Lim}(C)$ is a club (which is strictly smaller than C).

Exercise. Lemma 2.2 generalizes to countably many clubs C_i: if C_i, $i < \omega$, are clubs, so is $\bigcap_{i \in \omega} C_i$.

Lemma 2.2 allows us to define the *closed unbounded filter* generated by the club sets:

Definition 2.3. The club filter on ω_1, $\mathrm{Club}(\omega_1)$, is defined as follows:

$$\mathrm{Club}(\omega_1) = \{X \subseteq \omega_1 \,|\, \text{there is a club } C \text{ such that } C \subseteq X\}.$$

Note. Under AC, $\mathrm{Club}(\omega_1)$ is never an ultrafilter.

Definition 2.4. Let us denote by $\mathrm{NS}(\omega_1)$ the dual ideal to $\mathrm{Club}(\omega_1)$:

$$\mathrm{NS}(\omega_1) = \{X \subseteq \omega_1 \,|\, \kappa \setminus X \in \mathrm{Club}(\omega_1)\}.$$

We call the ideal $\mathrm{NS}(\omega_1)$ the *non-stationary ideal* on ω_1.

Lemma 2.5. *$X \subseteq \omega_1$ is stationary iff $X \cap C \neq \emptyset$ for every club C.*

Proof. If X is stationary iff $\kappa \setminus X$ is not in $\mathrm{Club}(\kappa)$. This means that there is no C so that $C \subseteq \kappa \setminus X$, or equivalently for any club C, $C \not\subseteq \kappa \setminus X$, which is the same as $C \cap X \neq \emptyset$. □

Exercise. Show that every stationary set S is unbounded, and hence uncountable. *Exercise.* Let us denote by $F(\omega_1)$ the Frechet filter on ω_1:

$$F(\omega_1) = \{X \subseteq \omega_1 \,|\, |\omega_1 \setminus X| < \omega_1\}.$$

Show

$$F(\omega_1) \subsetneq \mathrm{Club}(\omega_1).$$

2.2. Diamonds

Recall the definition of CH:

Definition 2.6. The *Continuum Hypothesis*, CH is defined as follows:

$$2^\omega = \omega_1.$$

Exercise. Show that the following two principles are equivalent to CH:
(i) There is a surjection from $\mathscr{P}(\omega)$ onto ω_1.
(ii) If X is an arbitrary infinite subset of the real line $\mathbb{R}$, then $|X| = \omega$ or $|X| = |\mathbb{R}|$.

The principle CH is relatively weak, the following concept is a strengthening of CH wich much broader range of consequences in mathematics.

Definition 2.7. Let S be a stationary subset of ω_1. We say that $\diamondsuit(S)$ holds if there is sequence $\langle S_\alpha \,|\, \alpha \in S\rangle$ such that $S_\alpha \subseteq \alpha$ for every α and for every $A \subseteq \omega_1$,

$$\{\alpha \in S \,|\, S_\alpha = A \cap \alpha\} \text{ is stationary.}$$

We write $\diamondsuit$ for $\diamondsuit(\omega_1)$.

Under $V = L$,[2] $\diamondsuit(S)$ is true for every stationary S.
$\diamondsuit$ implies CH:

Theorem 2.8. *Suppose $\diamondsuit$ holds, then* CH *holds.*

Proof. Let $\langle S_\alpha \,|\, \alpha \in \omega_1\rangle$ be a diamond sequence. We will show that for every $X \subseteq \omega$ there is some $\alpha \in \omega_1$ such that $X = S_\alpha$. This means that there is a surjection from $\mathscr{P}(\omega)$ onto ω_1, which is equivalent to CH. Let $X \subseteq \omega$ be arbitrary. Since $\langle S_\alpha \,|\, \alpha \in \omega_1\rangle$ is a diamond sequence, the set $\{\alpha < \omega_1 \,|\, S_\alpha = X \cap \alpha\}$ is stationary and in particular unbounded. Choose any $\alpha \geq \omega$ from this set. Then $X = X \cap \alpha = S_\alpha$. □

Note that by a result of Jensen, CH plus $\neg\diamondsuit$ is consistent so the converse of Theorem 2.8 does not hold.

2.3. Forcing axioms

Forcing axioms are axiomatic statements which postulate existence of certain ultrafilters on a wider class of Boolean algebras, not only the powerset algebras. By extending the class of algebras, it is possible to derive from forcing axioms consequences for specific mathematical structures: roughly speaking given a mathematical problem, it is sometimes possible to associate with it a specific Boolean algebra, and the existence of an ultrafilter with certain

[2] An axiom claiming that V is equal to the the *constructible universe* or *Gödel universe*, denoted L. $L \subseteq V$ is always true. Gödel defined L to show in 1930's that CH and AC relatively consistent with ZF.

properties implies a solution to the original problem. This is a remarkable extension of Cohen's original idea for forcing. See [14] for more details and context.

There is a conceptual similarity between compactness principles (consequences of AC) and forcing axioms: they both generalize certain ZFC-theorems, each in a different sense:

- AC implies that every filter in any powerset algebra $\mathscr{P}(X)$ can be extended into an ultrafilter.
- AC implies that given any complete Boolean algebra B and a family of countably many dense open subsets $\{D_n \mid n < \omega\}$ of B there is an ultrafilter on B which meets every D_n (this is a straightforward reformulation of the Baire category theorem).

Forcing axioms postulate the second bullet for uncountably many dense open subsets of a Boolean algebra B. B must come from some fixed class $\mathcal{B}$ of complete Boolean algebras (the larger the class $\mathcal{B}$, the stronger the associated forcing axiom).

Definition 2.9. Given a class $\mathcal{B}$ of complete Boolean algebras, we write $\mathsf{FA}_{\omega_1}(\mathcal{B})$ for the stament that for any $B \in \mathcal{B}$ and any family of dense open subsets $\{D_\alpha \mid \alpha < \omega_1\}$ of B there is an ultrafilter U on B which meets every D_α. We say that U is "partially generic".

Let us review some important classes $\mathcal{B}$. Let "ccc" denote the class of Bolean algebras satisfying the countable chain condition, "proper" the class of proper Boolean algebras, and "stat" the class of Boolean algebras preserving stationary subsets of ω_1. Note that these classes satisfy:

$$\text{ccc} \subseteq \text{proper} \subseteq \text{stat}.$$

Definition 2.10. Let us define the associated forcing axioms:
(i) Martin Axiom, also denoted MA_{ω_1}, is $\mathsf{FA}_{\omega_1}(\text{ccc})$.
(ii) Proper Forcing Axiom, also denoted PFA, is $\mathsf{FA}_{\omega_1}(\text{proper})$.
(iii) Martin Maximum, also denoted MM, is $\mathsf{FA}_{\omega_1}(\text{stat})$.

From the general perspective mentioned above, one can classify mathematical problems according to the associated Boolean algebra B and its class $\mathcal{B}$ such that the problem is decided by the existence of partially generic ultrafilters for B.

2.3.1. Some examples

Suppose $\mathbb{P} = (\mathbb{P}, \leq, 1)$ is a partially ordered set with the greatest element 1; then we say that $p, q \in \mathbb{P}$ are *compatible*, and write $p \mid\mid q$, if there is $r \in \mathbb{P}$ with $r \leq p, q$. We say that p, q are *incompatible* if there are not compatible. We say that $A \subseteq \mathbb{P}$ is an *antichain* if all $p \neq q \in A$ are incompatible. We say that $D \subseteq P$ is *dense* if for every p there is some $q \leq p$ in D and D is *open* if $p \in D$ and $q \leq p$ implies $q \in D$ (downwards closure).

Definition 2.11. We say that $\mathbb{P}$ is ccc (countable chain condition) if every antichain in $\mathbb{P}$ is at most countable.

A paradigmatic example is Cohen forcing for adding new subsets of of ω:

Definition 2.12. $\mathrm{Add}(\omega, \alpha)$, $0 < \alpha$, is a set of all functions p such that $\mathrm{dom}(p) \subseteq \alpha \times \omega$, $|\mathrm{dom}(p)| < \omega$, and $\mathrm{im}(p) \subseteq \{0, 1\}$. We set $p \le q$ iff $q \subseteq p$ (reverse inclusion ordering). $\mathrm{Add}(\omega, \alpha)$ is called the Cohen forcing (at ω). It adds α-many new subsets of ω.

Fact 2.13. *An application of the so called Δ-lemma shows that* $\mathrm{Add}(\omega, \alpha)$ *is ccc for every α. Note that for $\alpha < \omega_1$,* $\mathrm{Add}(\omega, \alpha)$ *is just countable, so it is ccc trivially.*

Let us further define that $G \subseteq \mathbb{P}$ is a filter if G contains the greatest element of $\mathbb{P}$, for every $p, q \in G$ there is some $r \in \mathbb{P}$ with $r \le p, q$, and if $p \in G$ and $p \le q$, then $q \in G$.

The following definition is equivalent to the Boolean algebra version mentioned above:

Definition 2.14 (Martin's axiom, MA_{ω_1})**.** Whenever $\mathbb{P}$ is ccc and $\mathcal{D}$ is a collection of ω_1-many dense sets in $\mathbb{P}$, then for every p there is a filter G containing p which intersects every element of $\mathcal{D}$.

Recall that if $\mathcal{D}$ has size ω, then the respective principle is provable:

Lemma 2.15 (Rasiowa-Sikorski)**.** *Suppose $\mathbb{P}$ is a partially ordered set and $\mathcal{D}$ is a countable collection of dense sets. Then for every p there is a filter G such that $p \in G$ and G meets every element of $\mathcal{D}$.*

Proof. Construct by induction a decreasing sequence of elements in $\mathbb{P}$, $\langle p_n \,|\, n < \omega\rangle$ with $p_0 = p$ and $p_{n+1} \in D_n$. Then define

$$G = \{q \in \mathbb{P} \,|\, \exists n < \omega, p_n \le q\}.$$

□

Remark 2.16. MA_{ω_1} is not provable in ZFC, but by using a forcing argument, it holds that if ZFC is consistent, then so is $\mathsf{ZFC} + \mathsf{MA}_{\omega_1}$.

Let us show some consequences of MA_{ω_1} to illustrate its use:

Theorem 2.17. $\mathsf{ZFC} + \mathsf{MA}_{\omega_1}$ *proves* $\neg\mathsf{CH}$.

Proof. We will apply MA_{ω_1} with the partial order $\mathbb{C} = \mathrm{Add}(\omega, 1)$. Suppose for contradiction that $2^\omega = \omega_1$, and let $\langle x_\alpha \,|\, \alpha < \omega_1\rangle$ enumerate all subsets of ω. Define dense sets D_α for $\alpha < \omega_1$ and D_m for $m < \omega$:

$$D_\alpha = \{p \in \mathbb{C} \,|\, \exists n < \omega, p(n) \neq x_\alpha(n)\},\ D_m = \{p \in \mathbb{C} \,|\, m \subseteq \mathrm{dom}(p)\}.$$

Let G be a filter meeting every D_α and D_m. Let x be the union of conditions in G. It is a function (because G is a filter) from ω into 2 (because G meets every D_m). It further follows $x \neq x_\alpha$ for every $\alpha < \omega_1$ because for every α there is some n the domain of x with $x(n) \neq x_\alpha(n)$ (because G meets every D_α). This contradicts the fact that $\langle x_\alpha \,|\, \alpha < \omega_1\rangle$ enumerates all subsets of ω. □

3. Whitehead conjecture

3.1. The problem

Definition 3.1. Suppose G is an abelian group and $f : G \to H$ is a surjective homomorphism. We say that f *splits* if there exists a homomorphism $f' : H \to G$ such that $f \circ f' = 1_H$.

Note that if $f : G \to H$ is surjective and $\ker(f)$ denotes the kernel of f, then $H \cong G/\ker(f)$ (see Theorem 3.15).

The problems is to characterize free abelian groups H via the criterion of the existence of splitting homomorphisms.

Fact 3.2 (see Theorem 3.24)**.** *H is free iff for every G and every surjective $f : G \to H$, f splits.*

It is easy to see that if H is free, then every $f : G \to H$ splits (see Theorem 3.24). The converse direction is a bit more difficult to prove: it uses the fact that every abelian group H is a quotient of the free group $\mathbb{Z}^{(H)}$ generated by H, i.e. $H \cong \mathbb{Z}^{(H)}/\ker(f)$ for some surjective homomorphism $f : \mathbb{Z}^{(H)} \to H$. The existence of splitting homomorphism ensures that H has an isomorphic copy inside $\mathbb{Z}^{(H)}$, and by Dedekind's theorem (that a subgroup of a free abelian group is always free), H must be free as well.

It follows that to prove the harder direction in Fact 3.2, it suffices to require that every surjective homomorphism $f : \mathbb{Z}^{(H)} \to H$ splits. Whitehead inquired whether it is possible to weaken this criterion still further and demand that only certain f's are split.

To understand this note that if $H \cong \mathbb{Z}^{(H)}/\ker(f)$, then $\ker(f)$ is a normal subgroup of $\mathbb{Z}^{(H)}$ and again by Dedekind's theorem $\ker(f)$ itself must be a free group. All free abelian groups are up to isomorphism of the form $\mathbb{Z}^{(\kappa)}$ for some cardinal κ (finite or infinite), see Section 3.3.[3] Stein proved that if H is countable, then it suffices for the converse direction that every $f : \mathbb{Z}^{(H)} \to H$ such that $\ker(f) \cong \mathbb{Z}$ splits.[4] Whitehead asked whether one can remove the condition of countability in Stein's theorem.

Let us restate the problem now in the modern notation:

Definition 3.3. We say that an abelian group H is a *Whitehead group* or *W-group* if for every G and every surjective homomorphism $f : G \to H$, if $\ker(f) \cong \mathbb{Z}$, then f splits.

Note that by the discussion above we have the following inclusion:

$$\text{Free abelian groups} \subseteq W\text{-groups}.$$

Stein's theorem now reads that every countable H is free iff H is a W-group.

Definition 3.4. We say that *Whitehead's conjecture* holds if there is an abelian group of size ω_1 which is a W-group, but not a free group. We denote this conjecture by WC.

Remark 3.5. Whitehead apparently did not commit strongly to a particular "conjecture", he posed the question as a problem. We write WC to have all the conjectures false in $V = L$ and true under PFA, undescoring the conceptual resemblance of the three problems (Whitehead's, Kaplansky's and Suslin's) which emerged only after some hard work of generations of mathematicians. Note that the conceptual resemblance shows that Stein's theorem

[3] In particular $\mathbb{Z}^{(H)} \cong \mathbb{Z}^{(|H|)}$.

[4] Since H is countable, $\mathbb{Z}^{(H)}$ is countable as well, so all the possibilities for $\ker(f)$ are $\{\mathbb{Z}^{(\kappa)} \,|\, 1 \le \kappa \le \omega\}$. Hence limiting the splitting homomorphism just to the case of $\mathbb{Z}$ is non-trivial.

is specific for the countable case and should not be naively postulated for all cardinals. Compare with König's lemma which asserts that every ω-tree has a cofinal branch, and the fact that König's lemma is false for ω_1 (there exit ω_1-Aronszajn trees).

3.2. Preliminaries on groups

We first review some basic concept. Recall that if G is a group (in general non-commutative) $G = (G, +_G, -_G, 0_G)$. We say that a function $f : G \to H$ between two groups is a *homomorphism* if $f(0_G) = 0_H$, $f(x +_G y) = f(x) +_H f(y)$, and $f(-_G x) = -_H f(x)$. We will omit the subscripts $_G$ and $_H$ in the subsequent text because they can be deduced from the notation.

Assume H is a subgroup, which we denote by $H \leq G$. For every $g \in G$, we call $g + H = \{g + h \,|\, h \in H\}$ the *left coset* (with respect to g) and $H + g = \{h + g \,|\, h \in H\}$ the *right coset* (with respect to g). Note that in general $g + H \neq H + g$ is possible.

As an exercise, convince yourselves that

$$H + a = H + b \leftrightarrow a - b \in H \leftrightarrow b - a \in H \\ \text{and } a + H = b + H \leftrightarrow -a + b \in H \leftrightarrow -b + a \in H. \tag{3.1}$$

Lemma 3.6. *The family of all left cosets and also of all right cosets is a partition of G. The number of elements in both partitions is the same. Also, for every g, $|g + H| = |H + g| = |H|$.*

Proof. Exercise. Hint for the second claim: define a function which maps $H + g$ to $-g + H$ and show that it is a bijection. See [H], Section 4. □

Remark 3.7. Note that we used this argument it the proof of Lagrange's theorem in Introduction to mathematics I: it implies that if G is finite and $H \leq G$, then the number of elements in H divides the number of elements in G.

It follows that the partition into left cosets defines an equivalence relation $\equiv_{H,l}$, and analogously for the right cosets, $\equiv_{H,r}$. By (3.1), a, b are equivalent if their difference is small mod H.

Recall that an equivalence $\equiv$ on G is a *congruence* if $a \equiv b$, then $-a \equiv -b$, and if $a_1 \equiv a_2$ and $b_1 \equiv b_2$, then $a_1 + b_1 \equiv a_2 + b_2$. If $\equiv$ is a congruence of G, then $G/\equiv = \{[g]_\equiv \,|\, g \in G\}$ can be given the group structure by postulating:

$$0 = [0]_\equiv, [a]_\equiv + [b]_\equiv = [a + b]_\equiv, -[a]_\equiv = [-a]_\equiv.$$

Congruences make it possible to define the so called *quotient structures.* In the context of groups, we get:

Lemma 3.8. *$G/\equiv$ is a group (called the* quotient group*) and $\pi : G \to G/\equiv$ is a surjective homomorphism, where $\pi(g) = [g]_\equiv$ for every $g \in G$.*

Proof. The fact that $G/\equiv$ is a group follows easily by the definition of operations in $G/\equiv$; for instance (we omit the subscript $_\equiv$): $[g] + [-g] = [g - g] = [0]$. π is clearly surjective, so it remain to show that it is a homomorphism. $\pi(0) = [0]$, $\pi(-g) = [-g] = -[g]$, and $\pi(g + h) = [g + h] = [g] + [h]$. □

A natural question is whether $\equiv_{H,l}$ and $\equiv_{H,r}$ are congruences. Let us try to check it for $\equiv_{H,r}$ and for the inverse: if $a \equiv_{H,r} b$, then by (3.1) $a-b \in H$; in order to have a congruence, we would like to have $-a \equiv_{H,r} -b \leftrightarrow -a+b \in H$. But $a - b \in H$ does not necessarily imply $-a + b \in H$. However, it does if $H + a = a + H$ and $H + b = b + H$. A similar argument would work for $+$, giving a sufficient condition for being a congruence:

$$\text{if } g + H = H + g \text{ for every } g, \text{ then } \equiv_{H,r} \text{ and } \equiv_{H,l} \text{ are congruences.}$$

But this is actually the same as $\equiv_{H,r}$ being identical to $\equiv_{H,l}$.

This property is very important and can be reformulated in many equivalent ways (where $g + N - g = \{g + n - g \,|\, n \in N\}$):

Lemma 3.9. *The following are equivalent for a subgroup $N \leq G$:*
- *(i)* $\equiv_{N,r} = \equiv_{N,l}$.
- *(ii)* $g + N = N + g$ *for all* $g \in G$.
- *(iii)* *For all* $g \in G$, $g + N - g \subseteq N$.
- *(iv)* *For all* $g \in G$, $g + N - g = N$.

Proof. We prove the less obvious ones.

$(ii) \to (iii)$. Let $g+n-g$ be given. $g+n \in g+N$, and since $g+N = N+g$, there is $n' \in N$ with $g + n = n' + g$. Hence $g + n - g = n' + g - g = n' \in N$.

$(iii) \to (iv)$. Suppose $n \in N$, and let us write it as $g + (-g + n + g) - g$. Since $-g + N + g \subseteq N$ by (iii), there is $n' \in N$ with $n = g + n' - g$, and so $n \in g + N - g$.

$(iv) \to (ii)$. $g + N = g - g + N + g = N + g$. □

Definition 3.10. A subgroup N which satisfies conditions in Lemma 3.9 is called *normal*, and we write $N \lhd G$.

The notions of a normal subgroup, a quotient group and a (surjective) homomorphism are deeply connected as we show next.

Definition 3.11. Suppose $f : G \to H$ is a homomorphism. Then the *kernel* of f, $\ker(f)$, is defined as

$$\ker(f) = \{g \in G \,|\, f(g) = 0\}.$$

As it turns out every normal subgroup is kernel of some homomorphism, and kernels are always normal subgroups.

Theorem 3.12.
- *(i) Suppose $f : G \to H$ is homomorphism. Then* $\ker(f) \lhd G$.
- *(ii) Suppose $N \lhd G$. Then the function π which maps $g \in G$ to $N + g$ is a surjective homomorphism $\pi : G \to G/N$ with* $\ker(\pi) = N$.

Proof. (i). First we need to check that $\ker(f)$ is a subgroup of G. Clearly $0 \in \ker(f)$ because $f(0) = 0$. If $g \in \ker(f)$, then $f(x) = 0$, and so $f(-x) = -f(x) = -0 = 0$, and so $-x \in \ker(f)$. The closure under $+$ is similar. To verify normality, it suffices to show $g + \ker(f) - g \subseteq \ker(f)$ for every $g \in G$; let fix any $n \in N$ and $g + n - g$. Since f is a homomorphism, we get $f(g + n - g) = f(g) + 0 - f(g) = 0$.

(ii). This follows from Lemma 3.8, noting that $N = [0]$. □

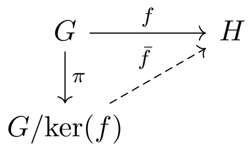
Remark 3.13. Theorem 3.12 implies that if $\equiv$ is a congruence and f is the surjective homomorphism given by $\equiv$, then $[0]_\equiv \lhd G$. Hence $\equiv_{N,r}$ (or $\equiv_{N,l}$) being a congruence is equivalent to all the conditions in Lemma 3.9.

Before we prove the first isomorphism theorem, let us state a small lemma first:

Lemma 3.14. *Suppose $f : G \to H$ is a homomorphism. Then f is injective iff* $\ker(f) = \{0\}$.

Proof. If f is injective, then clearly $\ker(f) = \{0\}$, so let us prove the converse. We notice first that if $g \neq h$ is equivalent to $g - h \neq 0$. Suppose for contradiction that $\ker(f) = \{0\}$ and for some $g \neq h$ we get $f(g) = f(h)$. Then $f(g-h) = f(g)-f(h) = 0$, and so $g-h \neq 0$ is in $\ker(f)$, a contradiction. $\square$

Theorem 3.15 (First isomorphism theorem for groups)**.** *If $f : G \to H$ is a group homomorphism, then there is a unique injective homomorphism $\bar{f} : G/kerf \to H$ such that $\bar{f}(g + \ker(f)) = f(g)$. It follows that $\bar{f}$ is an isomorphism between $G/ker(f)$ and* $\mathrm{im}(f)$*; in particular if f is surjective then $\bar{f} : G/\ker(f) \cong H$. Moreover, denoting $\pi : G \to G/\ker(f)$, the following diagram commutes:*



Proof. By Theorem 3.12, π is a surjective homomorphism. It remains to show that $\bar{f}$ is well-defined and is injective. First we check that $\bar{f}$ is well-defined: Suppose $g + \ker f = g' + \ker f$, we need to show $f(g) = f(g')$; $g + \ker(f) = g' + \ker(f)$ iff $g - g' \in \ker(f)$, and hence $f(g) - f(g') = 0$, and $f(g) = f(g')$. Next we check that $\bar{f}$ is a homomorphism: $\bar{f}(\ker(f)) = f(0) = 0$; $\bar{f}(-[g + \ker(f)]) = \bar{f}(-g + \ker(f)) = f(-g) = -f(g) = -\bar{f}(g + \ker(f))$; $\bar{f}(g+\ker(f)+g'+\ker(f)) = \bar{f}(g+g'+\ker(f)) = f(g+g') = f(g)+f(g') = \bar{f}(g+\ker(f))+\bar{f}(g'+\ker(f))$. By Lemma 3.14, the injectivity of $\bar{f}$ follows if we show $\ker(\bar{f}) = \{\ker(f)\}$. But $\bar{f}(g + \ker(f)) = 0$ is equivalent to $f(g) = 0$ by the definition of $\bar{f}$, and hence $g + \ker(f) = \ker(f)$. $\square$

3.3. Free abelian groups

Recall that if G is any abelian group, we write ng for $x + \cdots + x$ of length $n \in \mathbb{Z}$, and $0g$ for 0_G.[5] Clearly, $ng + mg = (n + m)g$.

Let $F(G)$ be the free abelian group generated by G. It can be represented as the direct sum $\oplus_{g\in G}\mathbb{Z}_g$ of copies of $\mathbb{Z}$ indexed by G, also written as $\mathbb{Z}^{(G)}$, where (G) indicates that only functions with finite support are allowed. That is, an element $x \in \mathbb{Z}^{(G)}$ is a function from G to $\mathbb{Z}$ such that for all but finitely many $g \in G$, $x(g) = 0$. The group operations on $F(G)$ are defined coordinate-wise:

(i) $(x + y)(g) = x(g) + y(g)$, and
(ii) $(-x)(g) = -x(g)$.

[5] This makes every abelian group a module over $\mathbb{Z}$.

(iii) $0_{F(g)}$ is a function which is constantly 0_G.

Define a function $e : G \to F(G)$ by postulating $e(g) := e_g$ where $e_g(g) = 1$, and e_g is 0 everywhere else. The mapping e is injective, so we identify G with the image of this function.[6]

Then the basis of $\mathbb{Z}^{(G)}$ is the set $\{e_g \mid g \in G\}$: every $x \in F(G)$, $x \neq 0_{F(G)}$,[7] can be written uniquely (up to permutation of its members) as

$$x = n_1 e_{g_1} + \cdots + n_k e_{g_k},$$

for some $n_i \neq 0$ and g_i, $1 \leq i \leq k$.

One can easily check that if $|G_1| = |G_2|$, then $F(G_1) \cong F(G_2)$.

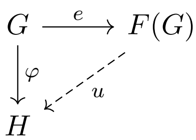
Remark 3.16. If G is an abelian group, then it is free if there is a set $X \subseteq G$ (called a *basis* of G) such that $G \cong \mathbb{Z}^{(X)}$. In particular for every element g of G there exists exactly one expression $n_1 x_1 + \cdots n_k x_k$, $0 \leq k < \omega$, for some some non-zero n_i and x_i from X, such that

$$n_1 x_1 + \cdots n_k x_k = g.$$

For this to be the case, X must *linearly independent*[8] if in the following sense. Whenever $x_1, \ldots, x_k$ are distinct elements of X, then $n_1 x_1 + \cdots n_k x_k = 0$ iff $n_i = 0$ for all $1 \leq i \leq n$. If the equation $n_1 x_1 + \cdots n_k x_k = 0$ had a solution in some non-zero n_i's, then any g could be expressed by more than one equation (because it would be possible to add $n_1 x_1 + \cdots n_k x_k = 0$ to an equation and express the same element). X is a basis if it is a maximal set of linearly independent elements.

The free group $F(G)$ has the following *universal property*:

Theorem 3.17 (Universal property)**.** *Whenever $\varphi : G \to H$ is a homomorphism, then there exists a unique homomorphism $u : F(G) \to H$ such that the diagram below commutes. Briefly stated: every homomorphism $\varphi : G \to H$ extends uniquely to a homomorphism from $F(G)$ to H.*



Proof. Every non-zero element $x \in F(G)$ is a linear (finite) equation of the form $n_1 e_{g_1} + \cdots + n_k e_{g_k}$. Define

$$u(n_1 e_{g_1} + \cdots + n_k e_{g_k}) = n_1 \varphi(g_1) + \cdots + n_k \varphi(g_k). \tag{3.2}$$

[6]However, note that e is not a homomorphism and so we cannot identify G with a subgroup of $F(G)$ by means of e: for all $g \neq h \in G$, $e_{g+h} \neq e_g + e_h$. In general, there cannot be any other embedding of G into $F(G)$ unless G is free by Dedekind's theorem. However, we can always identify e_{g+h} and $e_g + e_h$ via a congruence, obtaining that G is a quotient of $F(G)$, see Corollary 3.20. Note that by Theorem 3.24 a free resolution of a group H splits iff H is embeddable into $F(H)$.

[7]$0_{F(G)}$ is represented as the "empty" sum, and it is the only way how to represent it.

[8]The notion of *linear independence* is usually reserved for vector spaces, i.e. modules over a field: there one can show that every vector space has a basis (a set of linearly independent vectors), and is therefore a free object in the category of modules. This is false for abelian groups in general (not all abelian groups are free). However, a free abelian group is precisely a free module over the ring $\mathbb{Z}$ of integers. The term "linear independence" is sometimes used for abelian groups as well if there is no danger of confusion.

The diagram commutes because for every $g \in G$,

$$\varphi(g) = u(e_g).$$

The mapping u is by definition a homomorphism into H, disregarding whether φ is a homomorphism or not. However, φ being a homomorphism implies that $u \circ e = \varphi$ is a homomorphism. In particular we have

$$u(e_{g+h}) = \varphi(g+h) = \varphi(g) + \varphi(h) = u(e_g) + u(e_h).$$

□

Remark 3.18. The mapping u in the previous theorem is well-defined because all the elements of the basis $\{e_g \,|\, g \in G\}$ of $F(G)$ are "independent" in the sense that for any equation $n_1g_1 + \cdots + n_kg_k$, where g_i are in G, $n_1e_{g_1} + \cdots + n_ke_{g_k} \neq e_h$ for any $h \in G$. For instance, it always holds $e_{g+h} \neq e_g + e_h$ because they "formally different", but $u(e_{g+h}) = u(e_g) + u(e_h)$.

Corollary 3.19 (Extension of functions on basis, universal property)**.** *Suppose $F(B)$ is the free abelian group generated by basis B and let H be an abelian group. Let $u' : F = B \to H$ be any function. Then there is a unique homomorphism $u : F(B) \to H$ such that $u \restriction B = u'$.*

Proof. Define u as in the previous theorem:

$$u(n_1b_1 + \cdots + n_kb_k) = n_1u'(b_1) + \cdots + n_ku'(b_k), \tag{3.3}$$

where the b_i's range over the elements of the basis. □

Corollary 3.20 (Quotients of free groups)**.** *Every abelian group is a quotient of a free group.*

Proof. Apply Theorem 3.17 with $H = G$ and φ the identify function on G. Then $u : F(G) \to G$ is a surjective homomorphism because $\mathrm{im}(\varphi) = G$ which identifies e_{g+h} with $e_g + e_h$. □

3.4. Short exact sequences

Definition 3.21. We say that a sequence of abelian groups together with homomorphisms is a *short exact sequence*,

$$0 \to_{f_3} N \to_{f_2} G \to_{f_1} H \to_{f_0} 0$$

iff $\mathrm{im}(f_{i+1}) = \ker(f_i)$ for all $i > 0$, where 0 denotes the trivial one-element group.

In this case, f_3 maps 0 to 0_N, and by $\{0_N\} = \mathrm{im}(f_3) = \ker(f_2)$, f_2 is an injective homomorphism and N can be identified with a (normal) subgroup of G (see Lemma 3.14). Identifying N with its image, we obtain $\mathrm{im}(f_2) = N = \ker(f_1)$. Since f_0 is surjective and maps the whole H to 0, $H = \ker(f_0) = \mathrm{im}(f_1)$ implies that f_1 is surjective. Thus H is a surjective image of a homomorphism from G onto H with kernel N, by Theorem 3.15 $G/N \cong H$.

Recall that by Corollary 3.20, every abelian group G is a quotient of the free group $F(G)$ generated by G. Let $u : F(G) \to G$ be the surjective homomorphism from Corollary 3.20. The notation for short exact sequences captures the properties of this quotient analysis succinctly as follows:

$$0 \to \ker(u) \to_{1_{\ker(U)}} F(G) \to_u G \cong F(G)/\ker(u) \to 0. \tag{3.4}$$

Definition 3.22. The short exact sequence from (3.4) is called a *free resolution of G*.

Note that by Dedekind's theorem, $\ker(u)$ is a free subgroup of $F(G)$, hence $F(G)$ is equal up to isomorphisms to $\mathbb{Z}^{(\kappa)}$ and $\ker(u)$ to some $\mathbb{Z}^{(\mu)}$ for some finite or infinite cardinals $1 \le \mu \le \kappa$.

Remark 3.23. The fact that $G \cong F(G)/\ker(u)$, with $i : F(G) \cong \mathbb{Z}^{(\kappa)}$ and $j : \ker(u) \cong \mathbb{Z}^{(\mu)}$ isomorphisms for some $\mu \le \kappa$, might lead to the false idea that $G \cong \mathbb{Z}^{(\kappa)}/\mathbb{Z}^{(\mu)}$ which would imply that there are very few non-isomorphic abelian groups (for instance there would be just countably many abelian groups of size $\aleph_n$ for $n < \omega$). The problem with this argument is that to conclude $G \cong \mathbb{Z}^{(\kappa)}/\mathbb{Z}^{(\mu)}$, we would need to assume that $i \restriction \ker(u)$ is an isomorphism between $\ker(u)$ and $\mathbb{Z}^{(\mu)}$, which is not guaranteed by our assumption.[9] In fact, it is known that there are 2^κ many non-isomorphic abelian groups of size κ for all infinite κ. There seems to be no elementary proof in the literature, but it follows from the complicated machinery dealing with stable but not superstable theories developed by Shelah and others.

Let us now return to splitting homomorphisms (see Definition 3.1).

Theorem 3.24 ([9], Thm 2.3)**.** *H is free iff every short exact sequence*

$$0 \to_{f_3} N \to_{f_2} G \to_{f_1} H \cong G/N \to_{f_0} 0$$

splits, i.e. there exists $f_1' : H \to G$ such that $1_H = f_1 \circ f_1'$.

Proof. Suppose first that H is free, and B is a basis of H. For each $x \in B$, define $f_1'(x)$ as an arbitrary element from the preimage of x, $\{g \in G \,|\, f_1(g) = x\}$. By the universal property of H in Corollary 3.19, f_1' extends uniquely to the whole H, and by definition satisfies $1_H = f_1 \circ f_1'$.

Conversely, suppose that every exact short sequence splits and let H be given. Let

$$0 \to \ker(u) \to_{1_{\ker(U)}} F(H) \to_u H \cong F(H)/\ker(u) \to 0. \tag{3.5}$$

be a free resolution of H. Let u' be a splitting homomorphism from H into $F(H)$. Note that u' must be injective because if $x \neq y \in H$, then the preimages of x, y are disjoint, $\{g \in F(h) \,|\, u(g) = x\} \cap \{g \in F(H) \,|\, u(g) = y\} = \emptyset$, and $u'(x) \in \{g \in F(h) \,|\, u(g) = x\}$ and $u'(y) \in \{g \in F(h) \,|\, u(g) = y\}$. Then $\mathrm{im}(u')$ is an isomorphic copy of H in $F(H)$, and hence by Dedekind's theorem H is free. □

Note that for the converse direction (from right to left), it suffices if all *free resolutions of H* split. Thus Whitehead's problem is whether the assumption that all free resolutions of H with $\ker(u) \cong \mathbb{Z}$ split implies that all free resolutions of H split, and hence that H is free.

[9] From the logical perspective, we would need to assume that i is not only an isomorphism between the abelian groups $\langle F(G), +, -, 0\rangle$ and $\langle \mathbb{Z}^{(\kappa)}, +, -, 0\rangle$ but an isomorphism between the richer structures $\langle F(G), +, -, 0, \ker(u)\rangle$ and $\langle \mathbb{Z}^{(\kappa)}, +, -, 0, \mathbb{Z}^{(\mu)}\rangle$, where $\ker(u)$ is viewed as a unary predicate.

Remark 3.25. Theorem 3.24 provides an if and only characterization for being free which works more generally for modules over PIDs ([12], Theorem 5.1 – this gives the full proof for bases of arbitrary size – works for abelian groups as well). See Section **??** for more details on generalizations of being free: while the notion of being “free” requires the notion of “basis” (models over PIDs have bases), the categorical notion of being “projective” is more general (and equivalent to being free if there is a basis).

3.5. More on direct sums and quotients, homology

If A, C are abelian groups we can form the direct sum $A \oplus C = \{(a, c) \,|\, a \in A, c \in C\}$, with operations defined pointwise, and $(0, 0)$ being the neutral element.

Lemma 3.26. *If B is given, and A, C are two subgroups of B with $A \cap C = \{0\}$, then we can identify $A \oplus C$ with $A + C = \{a + c \,|\, a \in A, c \in C\}$, i.e. $A \oplus C \cong A + C$.*

Proof. Set $f : (a, c) \mapsto a + c$. Then the function $f : A \oplus C \to A + C$ is onto by definition. The function f is injective: Let us distinguish two case: (i) if $a \neq a'$ and $c = c'$ (or conversely), then $a + c = a' + c' \leftrightarrow a - a' = 0$ implies $a = a'$ which is a contradiction; (ii) if $a \neq a'$ and $c \neq c'$ and hence $a - a' \neq 0$ and $c - c' \neq 0$, $a - a' = c - c'$ together with $a - a' \in A$ and $c - c' \in C$ imply that the intersection $A \cap C$ contains more than just 0. Finally, f respects the operations: $f((a, c) + (a', c')) = f(a + a', c + c') = a + a' + c + c' = a + c + a' + c' = f(a, c) + f(a', c')$. □

Suppose that A, C are subgroups of an abelian group B, and $A \cap C = \{0\}$ hence $\oplus$ is interpreted as $+$. Then we can use the direct sum to describe an associated quotient: If $B = A \oplus C$, then $\{A + c \,|\, c \in C\}$ forms a partition of B, and $C \cong B/A$, with C containing exactly on element from each coset B/A (and symmetrically, $A \cong B/C$).

Lemma 3.27. *With the assumptions above, $C \cong B/A$.*

Proof. It is easy to check that a mapping π which maps c to $A + c$ is bijective and preserves operations: π is injective by Lemma 3.26 (and surjective by definition) and it preserves operations: $\pi(c + c') = A + (c + c') = (A + c) + (A + c') = \pi(c) + \pi(c')$. □

However, it is not the case that every quotient B/A can be written as a sum $A \oplus C$: if $\{A + b \,|\, b \in B\}$ is the partition B/A, then finding C amounts to finding a set of representatives for the equivalence classes $\{A + b \,|\, b \in B\}$ which together have a group structure, thus giving C. This is possible exactly when the homomorphism onto B/A splits:

Theorem 3.28. *Assume $f : G \to H$ is a surjective homomorphism between abelian groups with $\ker(f) = N$ and $f' : H \to G$ is its splitting homomorphism. Then G contains a subgroup isomorphic to H, and $G = N \oplus H$.*

Proof. We know that f' is injective, so we can identify H with a subgroup of G. Since $H \cap N = \{0\}$, we get $N \oplus H = \{x + f'(y) \,|\, x \in N, y \in H\} = \bigcup\{N + f'(y) \,|\, y \in H\} = G$. Compare also with [12], Lemma 4.6 □

Corollary 3.29. *If $f : G \to H \cong G/ker(f)$ is a surjective homomorphism and H is free, then $G = \ker(f) \oplus H$.*

Proof. This is a consequence of Theorem 3.24 from left to right and of Theorem 3.28. □

Remark 3.30. Thus if f splits, N, H completely determine G because $G = N \oplus H$: this fact is denoted by $\mathrm{Ext}(H, N) = 0$ in the homological notation (more details on homology notation are beyond the scope of this article). In this notation Whitehead's problem is whether $\mathrm{Ext}(H, \mathbb{Z}) = 0$ implies that H is free.

Remark 3.31. Note that there is a canonical example for the kernel to be equal to $\mathbb{Z}$: if $f : G = H \oplus \mathbb{Z} \to H$ is a surjective homomorphism defined by $f(x, n) = x$ (the projection), then $\ker(f) = \mathbb{Z}$ because $f(0, n) = 0$ for all $n \in \mathbb{Z}$.

3.6. Where does (non-trivial) set theory come in?

Before we start, let us recall some theorems which we will use as facts without giving proofs.

An abelian group A is called *torsion-free* if no element except 0 sums up to 0 after added together finitely many times, i.e. $x + \cdots + x \neq 0$ for every $x \neq 0$.[10] If A is torsion-free then a subgroup B of A is called *pure* if A/B is torsion-free.[11] A group A is *finitely generated*[12] if there is a finite set $X \subseteq A$ such that every element of A can be obtained by application of group operations on some members of X. For instance every free abelian group with finite basis is finitely generated.

The following hold:

Theorem 3.32. *(i) All finitely generated torsion-free abelian groups are free.*
(ii) Every Whitehead group is torsion-free. Hence if A is a finitely generated Whitehead group, it is free.
(iii) Every subgroup of a Whitehead group is Whitehead.

These results show that Whitehead groups share some conceptual similarity with free groups. The case of finitely generated abelian groups is well understood, with the concept of being free is equivalent to being torsion-free and to being Whitehead. However, even countable abelian groups which are not finitely generated are very complex and not fully understood (but it is

---

[10] A group A is a *torsion group* if *every* element has finite order, i.e. for every element x there is n such that $nx = 0$. Hence begin torsion is stronger than the negation of being torsion-free.

[11] The primary definition of a pure subgroup is different, but it is equivalent to this one for torsion-free groups A. The primary definition states that being pure is stronger than being just a subgroup because it requires being closed under certain additional equations: B is *pure* in A if for every $b \in B$ and every $n \in \mathbb{Z}$, if there is some $x \in A$ such that $nx = b$, then there is $y \in B$ such that $ny = b$. Compare also with the notions of ω_1-free in Definition 3.41 and of ω_1-pure in Definition 3.42.

[12] Every finitely generated abelian group is uniquely representable as a direct sum of a free group and of a finite abelian group. Thus finitely generated torsion-free abelian groups must be free.

known that in the countable case Whitehead is equivalent to free, see Theorem 3.39). The case of uncountable abelian groups is even more complicated.

Let us define the notion of a smooth chain of groups which is central for understanding the structure of free and Whitehead groups.

Definition 3.33. Let $\eta \geq \omega$ be a limit ordinal. We say that a $\subseteq$-increasings sequence of countable abelian groups $\langle A_\alpha \,|\, \alpha < \eta \rangle$ is *a smooth chain* if for every limit γ, $A_\gamma = \bigcup \{A_\alpha \,|\, \alpha < \gamma\}$. The chain is called *strictly increasing* if $A_\alpha \neq A_{\alpha+1}$ for every $\alpha < \omega_1$. We say that it is *a chain of groups* if A_α is a subgroup of $A_{\alpha+1}$ for every $\alpha < \omega_1$.

It would be tempting so say that the union of a smooth chain of free groups is free, but the problem is that the union of the bases may not be a basis of the union. A stronger condition of $A_{\alpha+1}/A_\alpha$ being free is required which implies that every element of the chain is free, but moreover allows one to extend the bases: if $A_{\alpha+1}/A_\alpha$ is free, then by Theorem 3.24, the surjective homomorphism from $A_{\alpha+1}$ with kernel A_α splits, and hence by Theorem 3.28 and Corollary 3.29, $A_{\alpha+1} = A_\alpha \oplus A_{\alpha+1}/A_\alpha$ and the basis of A_α is disjoint from the basis of $A_{\alpha+1}/A_\alpha$. See also Corollary 2.5 in [9].

Theorem 3.34 ([9], Theorem 2.6)**.** *Let A be an abelian group. Then the following are equal:*

(i) A is free.

(ii) A is the union of a strictly increasing smooth chain of groups $\langle A_\alpha \,|\, \alpha < \eta\rangle$ such that A_0 is free and for every $\alpha < \eta$, the quotient $A_{\alpha+1}/A_\alpha$ is free.

Proof. From (i) to (ii). Let $\langle x_\alpha \,|\, \alpha < \eta\rangle$ be some enumeration of a basis of A. Set A_α to be generated by $\langle x_\xi \,|\, \xi < \alpha\rangle$. This is a strictly increasing smooth chain of groups with $A_{\alpha+1}/A_\alpha$ being free with basis $\{x_\alpha\}$ which can be computed by a direct argument (in particular, $A_{\alpha+1} \cong A_\alpha \oplus \mathbb{Z}$). Note that it also holds that A/A_α is free with basis $\{x_\xi \,|\, \alpha < \xi < \eta\}$.

From (ii) to (i). This is implicit in the previous paragraph as the readers can check for themselves: using $A_{\alpha+1} = A_\alpha \oplus A_{\alpha+1}/A_\alpha$ and continuity of the sequence ("smoothness") it is possibly to glue the basis of A_α's together because they are disjoint, and take unions at limit stages. □

3.6.1. Being free as a compactness property

Recall the notion of compactness of first-order logic: somewhat vaguely stated, it asserts that first-order properties which are true in all its finite substructures reflect up to the whole (infinite) structure. For instance if (G, E) is a non-directed graph and there exists $n < \omega$ such that all its finite subgraphs are n-colorable, then the whole graph (G, E) is n-colorable. This is because being n-colorable for a fixed n can be expressed by a first-order formula. However, it it clearly false to assert that if every finite subgraph of G is finitely-colorable, then the whole G is finitely colorable (because there are infinite G which are not finitely colorable). It follows that being "finitely colorable" is not a first-order property. This leads to the following general question:

> (Q1). Are there some interesting properties of mathematical structures like abelian groups or graphs which are not

> first-order but there is a useful notion of compactness behind them? And subsequently, is the extent of such compactness dependent on the underlying axioms of set theory?

For instance can we assert that the following principle $F(\kappa)$ holds for some infinite κ?

(3.6) $(F(\kappa))$. Suppose A is an abelian group of size $\kappa \geq \omega$ such that every subgroup B of A of size $< \kappa$ is free. Then A is free.

To make $F(\omega)$ meaningful, we understand $F(\omega)$ as saying that if A is a countable abelian group such that every *finitely generated* subgroup of A is free, then A is free.

As it turns out, this is a quite complicated question which heavily depends on the underlying axioms of set theory and the answer moreover dependent of the cardinal κ.

Let us give some examples:

Lemma 3.35. *The principle $F(\omega)$ is false.*

Hints. Let us consider the abelian group $(\mathbb{Q}, +)$ of rationals with addition. This is a countable torsion-free group which is not free. To see that it is non-free realize that if $q_1 \neq q_2$ are any two distinct rationals, then they are linearly dependent in $\mathbb{Q}$, and hence there is no basis of $\mathbb{Q}$ with more than one element. However, $\mathbb{Q}$ is not isomorphic as a group to $\mathbb{Z}$, so $\mathbb{Q}$ does not have a basis of size 1 either. It follows $\mathbb{Q}$ is not free. Note that since finitely generated and torsion-free implies free, it follows that $\mathbb{Q}$ is not finitely generated. To falsify $F(\omega)$ it suffices to show that every finitely generated subgroup of $\mathbb{Q}$ is free: Suppose $r_1/s_1, \dots, r_k/s_k$ are distinct rationals and look at subgroup B generated by them. Little reflection shows that this is an infinite subgroup of a subgroup of $\mathbb{Q}$ generated by the single rational $1/s_1 \cdots s_k$, and being generated by one element and being torsion-free implies it is isomorphic to $\mathbb{Z}$. Since an infinite subgroup of $\mathbb{Z}$ must be isomorphic to $\mathbb{Z}$ again, it follows that B is free. □

We will see below that $F(\omega_1)$ is provably false in ZFC as well. In fact, for every regular $\kappa < \aleph_{\omega^2}$, $F(\kappa)$ is provably false in ZFC. However, surprisingly, there is extension of ZFC which implies that for all $\kappa \geq \aleph_{\omega^2+1}$, $F(\kappa)$ is true.

Remark 3.36. Without going into details, $F(\kappa)$ is always true for sufficiently big large cardinals. For instance if κ is weakly compact, then $F(\kappa)$ is true: this is a straightforward consequence of weak compactness which extends the compactness of first-order logic to a certain infinitary logic (which is strong enough to express the notion of being free). The true challenge of obtaining $F(\kappa)$ for an uncountable κ is the case of successor cardinals μ^+, and typically we are interested in μ^+ as small as possible. The successor cardinal $\aleph_{\omega^2+1}$ is the least cardinal where $F(\kappa)$ can be true.

To return to $F(\omega)$, a weaker version of $F(\omega)$ holds if we include the notion of a *pure subgroup.* Suppose A is countable abelian group. We say that pure finitely-generated subgroups are *dense* in A if for every finitely generated subgroup $B_0 \leq A$, there is some finitely-generated pure $B \leq A$ such that $B_0 \leq B$.

(3.7) $(F(\omega)^*)$. Suppose A a countable torsion-free group such that finitely generated pure subgroups are dense in A. Then A is free.

See Theorem 3.37 for the proof of $F(\omega)^*$.

3.6.2. All countable Whitehead groups are free

The following theorem gives an equivalent condition for a countable abelian group to be free, and one can show that Whitehead groups satisfy it as well.

Theorem 3.37 (Theorem 4.2 in [9], principle $F(\omega)^*$)**.** *Suppose A is a countable torsion-free group such that every finitely-generated subgroup B_0 of A is contained in a finitely generated pure subgroup B of A. Then A is free.*

Hints. The proof proceeds by constructing a strictly increasing chain of groups $\langle A_n \,|\, n < \omega \rangle$ with union A which satisfies the conditions laid out in Theorem 3.34. In some detail, let $A = \{a_n \,|\, n < \omega\}$. Let $A_0 = 0$. If A_n is defined, let A_{n+1} be a finitely generated pure subgroup of A containing $A_n \cup \{a_n\}$. The quotient A_{n+1}/A_n is torsion-free because A_n is pure in A and it is finitely generated because A_{n+1} is finitely generated. Therefore A_{n+1}/A_n is free.

Note that since the chain has length ω, the condition of being "smooth" (continuous) in Definition 3.33 is trivial. □

Remark 3.38. Note that if A is uncountable and satisfies the assumptions of Theorem 3.37, it may fail to be free. This follows from arguments for the consistency of the fact that there may be Whitehead groups which are not free (see Section **??**). Countable and uncountable groups are quite different, which is reflected in many arguments in set theory with respect to many other structures (recall for instance that while every ω-tree has cofinal branches, there are ω_1-trees without cofinal branches).

The main result which motivated Whitehead's question is that for countable groups, the notions of free and Whitehead coincide.

Theorem 3.39 (Stein [23], Theorem 4.1 in [9])**.** *Every countable Whitehead group is free.*

Hints. The proof is by contradiction: assume A is a countable Whitehead groups which is not free, and hence does not satisfy the property in Theorem 3.37. Then there exists a finitely generated subgroup B_0 of A which is not contained in a finitely generated pure subgroup. Let B be the least pure subgroup containing B_0. By our assumption B is not finitely generated. Hence B is a union of a strictly increasing chain of finitely generated Whitehead[13] groups $\langle B_n \,|\, n < \omega \rangle$ such that

$$B_{n+1}/B_n \text{ is a torsion group for all } n < \omega. \tag{3.8}$$

[13] Recall that for finitely generated groups this is equal to being free and also to being torsion-free.

This holds because B is countable and the least torsion-free group extending B_0, and hence B/B_n is torsion-free for each $n < \omega$, and thus B_{n+1}/B_n cannot be torsion-free.[14]

We aim to prove that B is not Whitehead, contradicting Theorem 3.32(iii) because B is a subgroup of A.

The proof proceeds by constructing another strictly increasing chain of groups $\langle C_n \,|\, n < \omega\rangle$, such that for each n, the domain of C_n is equal to $B_n \times \mathbb{Z}$ and for $C = \bigcup_n C_n$, with domain of C being $B \times \mathbb{Z}$, there is a homomorphism $\pi : C \to B$ with kernel $\mathbb{Z}$ which does not split, and thus π is a witness that B is not Whitehead. The proof has two key steps (K1) and (K2) which we have extracted from the usual proof to isolate the analogies and differences between the countable and uncountable cases.

- (K1) The first key ingredient of the proof (which cannot be mimicked for uncountable groups) is that B_{n+1}/B_n being torsion implies that every possible splitting homomorphism ρ for π from B to C is uniquely determined by its restriction to B_0 by an inductive argument: Every $x \in B$ is in some B_n; if $n > 1$, then $x \in B_n \setminus B_{n-1}$, and since B_n/B_{n-1} is torsion, then must be some k_n such that $k_n x \in B_n$. By repeating this argument finitely many times there must be some k such that $kx \in B_0$.
- (K2) The second key ingredient of the proof (which can be in some sense mimicked for the uncountable case and also resolve the problem with missing (K1)) is that since B_0 is finitely generated, there is a finite set S_0 such that every splitting homomorphism $\rho : B \to C$ is uniquely determined by its restriction to S_0. It follows that all such restrictions can be enumerated in countably many stages $\langle g_n \,|\, n < \omega\rangle$, and for each n, C_{n+1} is chosen to prevent g_n from being extendible to a splitting homomorphism from B to C.

The combination of (K1) and (K2) implies that B is not a Whitehead group contradicting the fact that it is a subgroup of Whitehead group A. $\square$

For later reference let us observe that the fact every ρ is determined by its restriction to S_0 is essential for the argument. Suppose this fails and let S_n be a finite basis of B_n for every $n < \omega$ and let F enumerate all countably many functions from S_n to C for $n < \omega$, uniquely extending to homomorphisms $\tilde{f} : B_n \to C$. Note that the S_n's do not need to extend each other, but it still holds that if $\rho : B \to C$ is a homomorphism, then its restriction to B_n is a homomorphism determined by $\rho \restriction S_n$, for all $n < \omega$. Then we have the following weaker property:

$$\forall \rho : B \to C \; \exists n < \omega \; \exists f \in F \; \rho \restriction B_n = \tilde{f}. \tag{3.9}$$

In fact, there are infinitely many such n for every ρ in (3.9). Anticipating the role of $\diamondsuit(S)$ in the proof of Theorem 3.45, we could prove Theorem 3.39 just using (3.9) if we had the following principle $\diamondsuit(\omega)$ which asserts that the finite functions in F can be enumerated in type ω in such a way that the

[14] However, as we discussed, being non-torsion-free is weaker than being torsion so one needs to be more careful here: using the countability of B we can choose inductively B_{n+1} so that B_{n+1}/B_n has the property that every element of the quotient is torsion (not only some of them which is implied by being non-torsion-free).

index n of $g_n \in F$ is greater or equal to the size of the domain S_m which is handled in stage n and every subset ω is captured at least once on a non-zero index:

$$\exists\langle g_n \,|\, g_n : n \to 2, n < \omega\rangle \; \forall f : \omega \to 2 \; \exists n > 0 \; f \restriction n = g_n. \tag{3.10}$$

However, little reflection shows that (3.10) is false: for every $\langle g_n \,|\, n < \omega\rangle$ there are $f : \omega \to 2$ which are never guessed, for instance $h : \omega \to 2$ defined so that $h(n) = 0$ if $g_{n+1}(n) = 1$, and $h(n) = 1$ if $g_{n+1}(n) = 0$, for $n \geq 0$. It is instructive to realize that this falsification of $\diamondsuit(\omega)$ is possible because the domain of g_{n+1} has the greatest element, something which is false for $g_\alpha : \alpha \to 2$ for a limit ordinal α. The fact that $\diamondsuit(\omega_1)$ is consistent[15] and hence an analogue of (3.9) suffices to prove Theorem 3.45 underscores the difference in arguments in the countable and uncountable cases.

Remark 3.40. Note that theorem 3.39 implies that every Whitehead group of any size is ω_1-free.

3.6.3. All Whitehead groups of size ω_1 can be free

Let us analyze Theorem 3.34 in an effort to weaken (ii) substantially. Let us define some notations which will be useful:

Definition 3.41. We say that an abelian group A is ω_1-free if every countable subgroup B of A is free.

Definition 3.42. We say that a subgroup B of A is ω_1-pure if B/A is ω_1-free.

It is easy to see that if A/A_α is ω_1-free, then $A_{\alpha+1}/A_\alpha$ is free since $A_{\alpha+1}/A_\alpha$ is a subgroup of A/A_α (a consequence of the third group isomorphism theorem) and countable because $A_{\alpha+1}$ is countable.

With this setup we can improve Theorem 3.34 by allowing a small set of stages which do not have the property that $A_{\alpha+1}/A_\alpha$ is free. This imbues these algebraic arguments with a set-theoretic notion of a "measure", formulated in terms of the club filter on ω_1, and provides an important improvement of Theorem 3.34.[16]

[15] However, the diamond principle at ω_1 is false for non-stationary sets: The following is false: *There exists a non-stationary set $E \subseteq \omega_1$ and a sequence $\langle g_\alpha \,|\, \alpha \in E\rangle$ such that for every $f : \omega_1 \to 2$ there exists $\alpha \in E$, $\alpha \geq \omega$, such that $f \restriction \alpha = g_\alpha$.* Hint: Assume for contradiction $\langle g_\alpha \,|\, \alpha \in E\rangle$ is a diamond sequence. Let C be a club such that $C \cap E$ is empty and let $\langle c_\alpha \,|\, \alpha < \omega_1\rangle$ be an increasing and continuous enumeration of C, starting above ω. We will define $f : \omega_1 \to 2$ by induction on c_α. First look at c_0; there are 2^ω many subsets of ω, but the set $F_0 = \langle g_\delta \restriction \omega \,|\, \delta < c_0\rangle$ is only countable, so that you can choose f_0 with domain c_0 which is different from all functions in F_0 on ω (and hence no g_α, $\omega \leq \alpha < c_0$, can guess $f_0 \restriction \alpha$ correctly). Continue like this, defining $f_{\beta+1}$ on the segment $[c_\beta, c_{\beta+1})$ and using the interval $[c_\beta, c_\beta + \omega)$ the way we used interval $[0, \omega)$ for the construction of f_0. Set $f_\delta = \bigcup\{f_\gamma \,|\, \gamma < \delta\}$ for a limit ordinal c_δ in C. Since the limit stages are never in E, the resulting function $f = \bigcup\{f_\delta \,|\, \delta < \omega_1\}$ is guessed nowhere at E. Note that if we look at the interval $[\omega, \omega + \omega)$ when constructing f_0, and combine it with the argument for the falsity of (3.10), we can get an f that is not guessed on any element in E, not even on $n < \omega$, $n > 0$.

[16] There is no obvious way how to introduce a similar measure on ω and find an analogue of Theorem 3.43 for ω: if B_{n+1}/B_n is not free, it does not imply that it is torsion and hence an argument from Theorem 3.39 cannot be used in a straightforward way.

Theorem 3.43 (Theorem 5.3 in [9]). *Let A be an abelian group of size ω_1. Then the following are equal:*

(i) A is free.

(ii) A is the union of a strictly increasing smooth chain of groups $\langle A_\alpha \,|\, \alpha < \omega_1\rangle$ such that A_0 is free and

$$C = \{\delta < \omega_1 \,|\, A/A_\delta \text{ is } \omega_1\text{-free}\} \text{ contains a club,} \tag{3.11}$$

or equivalently

$$E = \{\delta < \omega_1 \,|\, A/A_\delta \text{ is not } \omega_1\text{-free}\} \text{ is non-stationary.} \tag{3.12}$$

Proof. Let us give some comments on (ii)→(i). Let $C^* \subseteq C$ is a club and let $\langle \nu(\alpha) \,|\, \alpha < \omega_1\rangle$ be its increasing continuous enumeration. Then $\langle A_{\nu(\alpha)} \,|\, \alpha < \omega_1\rangle$ is a strictly increasing smooth chain of groups such that $A_{\nu(\delta+1)}/A_{\nu(\delta)}$ is free (because $A/A_{\nu(\delta)}$ is ω_1-free and $A_{\nu(\delta+1)}/A_{\nu(\delta)}$ is countable and isomorphic to a subgroup of $A/A_{\nu(\delta)}$). Then the result follows by Theorem 3.34. □

Remark 3.44. Note that we needed to know that A/A_δ is free for $\delta \in C^*$, not only that $A_{\delta+1}/A_\delta$ is free because $\delta+1$ may be different (strictly smaller) than the next element δ^+ of C^* above δ, hence $A_{\delta+1}/A_\delta$ being free is not sufficient to conclude that A_{δ^+}/A_δ is free. For further reference notice that if

$$E_1 = \{\delta < \omega_1 \,|\, A_{\delta+1}/A_\delta \text{ is not free}\} \text{ is stationary,} \tag{3.13}$$

then

$$E_2 = \{\delta < \omega_1 \,|\, A/A_\delta \text{ is not } \omega_1\text{-free}\} \text{ is stationary} \tag{3.14}$$

because $E_1 \subseteq E_2$.

The following Theorem 3.45 is the combinatorial heart of Shelah's original construction from [20], finding a connection between being a Whitehead group and the largeness of E in (3.12) (see Remark 3.44) which leads to the result that consistently all Whitehead groups are free.

Theorem 3.45 (Theorem 6.3 in [9]). *Let A be a union of a strictly increasing smooth chain of groups $\langle A_\alpha \,|\, \alpha < \omega_1\rangle$ such that*

$$E = \{\delta < \omega_1 \,|\, A_{\delta+1}/A_\delta \text{ is not free}\} \tag{3.15}$$

is stationary in ω_1. Then if $\diamondsuit(E)$ holds, then A is not a Whitehead group (and in particular not a free group either).

Hints. The key idea of the proof is to replace the properties (K1) and (K2) in the proof of Theorem 3.39 by $\diamondsuit(E)$ which ensures that we can enumerate all countable functions relevant for the argument in such a way that they capture all possible splitting homomorphisms. As we mentioned in paragraphs discussing (3.10), such an enumeration does not exist for ω.

The rest of the argument is quite similar to Theorem 3.39: Using $\diamondsuit(E)$, one can fix a family of functions $\langle g_\alpha \,|\, \alpha < \omega_1\rangle$,

$$\{g_\alpha \,|\, g_\alpha : A_\alpha \to A_\alpha \times \mathbb{Z}, \alpha \in E\}, \tag{3.16}$$

such that for every $\rho : A \to C$ (where C is the union of a chain $\langle C_\alpha \,|\, \alpha < \omega_1\rangle$ and has domain $A \times \mathbb{Z}$, as in Theorem 3.39) there are stationarily many α

such that $\rho \restriction \alpha = g_\alpha$. At stage α, we prevent all functions $\rho : A \to C$ which extend g_α from being splitting homomorphism from A to C.

Note that the use of diamond cannot be avoided because it is consistent with ZFC that there are non-free Whitehead groups (see Section **??**). □

Finally, we obtain the theorem which shows that consistently every Whitehead group is free:

Theorem 3.46 (Theorem 1.3(i) in [9] proved on page 784)**.** *Assume $\diamondsuit(E)$ holds for every stationary $E \subseteq \omega_1$. Then every Whitehead group is free.*

Proof. Let A be a Whitehead group. It can be shown (we omit the details) that A is a union of a strictly increasing smooth chain of groups $\langle A_\alpha \mid \alpha < \omega_1 \rangle$ such that for each α, $A_{\alpha+1}$ is ω_1-pure in A. Let

(3.17)

$$E = \{\delta < \omega_1 \mid A_\delta \text{ is not } \omega_1\text{-pure in } A\} = \{\delta < \omega_1 \mid A_{\delta+1}/A_\delta \text{ is not free}\}.$$

By Theorem 3.45, E cannot be stationary. It follows that E is non-stationary, and hence A must be free. □