Stable $\aleph_0$-categorical Algebraic Structures

by

Paul Baginski

B.S. (Carnegie Mellon University) 2003
M.S. (Carnegie Mellon University) 2003

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

GRADUATE DIVISION
of the
UNIVERSITY OF CALIFORNIA, BERKELEY

Committee in charge:
Professor Thomas Scanlon, Chair
Professor Leo Harrington
Professor Christos Papadimitriou

Spring 2009

The dissertation of Paul Baginski is approved:

Chair ________________________________ Date __________

________________________________ Date __________

________________________________ Date __________

University of California, Berkeley

Stable $\aleph_0$-categorical Algebraic Structures

Abstract

Stable $\aleph_0$-categorical Algebraic Structures

by

Paul Baginski
Doctor of Philosophy in Mathematics

University of California, Berkeley

Professor Thomas Scanlon, Chair

We examine the algebraic implications of the model-theoretic properties of stability and $\aleph_0$-categoricity when they occur in groups, rings, and other algebraic structures. The known theorems and conjectures in this area fit within a larger class of related results on the coincidence of strong model-theoretic properties in algebraic structures. This dissertation is primarily concerned with the well-known conjecture of Baur, Cherlin, and Macintyre [BCM79] that a stable, $\aleph_0$-categorical group is abelian by finite; a theorem by the same authors guarantees that such a group is at least nilpotent by finite. For rings, there is an analogous conjecture and theorem. Baldwin and Rose [BR77] proved that a stable, $\aleph_0$-categorical ring is nilpotent by finite. It is further conjectured that such a ring will be null by finite, i.e. up to extension by a finite ring, multiplication is trivial.

In this dissertation, we produce an alternate proof of Baldwin and Rose's theorem, using the model-theoretic technique of field interpretation. We also prove that the ring and group conjectures are equivalent. In the remaining sections, we analyze structural properties that would be demanded of a counterexample to the Baur-Cherlin-Macintyre Conjecture. After some reductions, we are able to use the tool of quasiendomorphism rings to place restrictions on the commutator subgroup in certain cases.

Professor Thomas Scanlon
Dissertation Committee Chair

To my husband, Christian,

an endless source of support,

vitality, and love.

Contents

Acknowledgments

This dissertation would not have been possible with the counsel and support of a great number of people.

Without a doubt, my career at Berkeley could not have had its successes nor followed its path without a skilled and talented advisor such as Thomas Scanlon. His wealth of familiarity with model theory, and mathematics in general, has preempted many wrong turns and whirlpools in my research. He educated me both in mathematical knowledge and in navigating the academic world of making connections with potential collaborators. In my time at Berkeley, he has been a friend as well and I am thankful for all that I have learned from him, both mathematical and otherwise. He is a great mathematician, whose effortless accommodation of his students within his research schedule would have you thinking there were 36 hours in a day. I am honored to say that I was his student.

I also owe much of my achievements to the tireless efforts of *mes pères Lyonnais*, Tuna Altınel and Frank Wagner. It was extremely useful to gain some of their intuition for the model theory of groups during my three stays in Lyon. I also cannot cease in my gratitude for their support of my research and endeavors in my graduate career; through their efforts, opportunities have arisen around the world.

A number of other experts of model theory have imparted their knowledge upon me in several encounters: Gregory Cherlin and Alexandre Borovik in Lyon, Dugald Macpherson in Antalya and Manchester, and Ehud Hrushovski in Antalya. The encounters with each refreshed my perspective on the dissertation problem and opened new avenues to pursue. I am also indebted to George Bergman for a conversation on noncommutative ring theory.

In the final and most stressful stretch of my graduate career, I became indebted for the feedback provided by my dissertation committee, Thomas Scanlon, Leo Harrington and Christos Papadimitriou. In the course of my research, I was partially supported by NSF grant # DMS-0450010 and by a Department of Homeland Security Graduate Fellowship.

My fellow Scanlonites, Maryanthe Malliaris, Charlie Smart, Meghan Anderson, Alice Medvedeva, and others, have been an important touchstone while at Berkeley. They helped me prepare for my qualifying exams and ran a vibrant group for seminars. They reminded me that others had faced the same difficulties in dissertation research and that I was not the only one who had trouble wrapping my head around that most troublesome subject, model theory. My officemates, Betsy Stovall, Emily Peters and David Zywina, were also an inspiration in graduate school, for their mathematical industry and our longtime friendship.

I would like to thank my parents and family for supporting me through graduate school, and I thank my husband, Christian, who has made my life wonderful.

Chapter 1

Introduction and History

Throughout the history of modern mathematics, the study of mathematical objects has often been informed by algebraic structures defined on these objects. Examples abound: Galois groups illuminated key questions about field extensions; Picard-Vessiot groups relate to certain differential equations over fields; permutation groups capture symmetries; and the class groups of number rings (or more generally, Krull monoids) extract factorization properties. The presence of such algebraic structures indicates, on an essential level, the underlying symmetry of the objects under study. The study of the associated algebraic structures augments our understanding of the original objects. Galois theory alone testifies to the richness of this idea.

Many advances in model theory were motivated by the question of when a given theory can have associated algebraic structures that in a basic way "come from" the theory. Precisely stated, given a first-order theory T, when can T interpret a group, a field, etc.? This question led to many abstract results, including the general theory of binding groups (cf. [Wag97, Ch 4.8]) and Hrushovski's Group Configuration Theorem [Hru86]. Perhaps the most pointed question in this regard was Zilber's Trichotomy [Zil93] conjecture about algebraic closures in strongly minimal sets:

Conjecture 1.0.1 (Zilber Trichotomy)**.** Let X be a strongly minimal set. Then exactly one of the following holds about the algebraic closure operator, acl, on X:

1. X is **degenerate** (or trivial): for any nonempty set $A \subseteq X$, $\mathrm{acl}(A) = \bigcup_{a \in A} \mathrm{acl}(a)$.

2. X is **modular**: X is bi-interpretable with a group, essentially having the geometry of a vector space

3. X is bi-interpretable with an algebraically closed field.

Hrushovski disproved this conjecture in general ([Hru93]), however the trichotomy does hold for strongly minimal sets in differentially closed fields of characteristic 0 and, more generally, Zariski geometries. The Zilber trichotomy conjecture attempted to classify the simplest infinite definable sets in the theory in terms of what algebraic structures they may interpret. While this conjecture may not be true, its spirit continues in model theory, with the proofs of trichotomy theorems and conjectures in a variety of contexts, such as o-minimal theories [PS98].

Accompanying the question of whether one can interpret algebraic structures, is what algebraic properties these algebraic structures will have. The Zilber trichotomy, for instance, does more than say the structure interprets a group or a field, it says that the group will essentially be a vector space and the field will necessarily be algebraically closed. These are algebraic consequences of the model theoretic hypotheses.

Since algebraic structures are interpretable in a far wider range of structures than the strongly minimal ones, one of the objectives of model theory has been to classify the pure algebraic properties of algebraic structures appearing in such contexts. The context plays a definitive role: when we speak about groups and other algebraic structures, we do not necessarily do so as pure algebraic structures. Rather, they will be groups or other algebraic structures that are interpretable in some ambient theory and this ambient theory induces model theoretic properties on the algebraic structures. Specifically, the algebraic structures (say, groups) would then inherit a theory T in a language $\mathcal{L}$ extending the language of groups, $\mathcal{L}_G$, where we have included predicates for all the subsets of our group that are definable in the original theory. With several model-theoretic properties, we get an automatic transfer of properties of the ambient theory to the enriched theory of the algebraic structure. For example, if the original theory were stable or $\aleph_0$-categorical, then any interpretable groups would also have that property. In particular, since $\aleph_0$-categoricity and stability are both preserved by taking reducts, such groups would also be stable and $\aleph_0$-categorical as pure groups.

Before proceeding with the known results in the area, we must define a common group-theoretic concept.

Definition 1.0.2. Given group theoretic properties P, Q, R, we say that a group G is "P **by** Q" if there is a normal subgroup N of G, such that N has property P and G/N has property Q. This definition schema is right associative, that is to say that G is "P **by** Q **by** R" if and only if there is a normal subgroup N of G with property P such that G/N is Q by R. When property Q is "finite", many authors (including the present one on occasion) will use the phrase "**virtually** P" in place of "P by finite."

The most common usages in this dissertation are "abelian by finite" (or "virtually abelian") and "nilpotent by finite" (or "virtually nilpotent").

We can extend this definition schema to (noncommutative) rings by replacing "normal subgroup" with (two-sided) ideal.

1.1 History

In this dissertation, we will be concerned with groups and rings interpretable in theories with fairly strong model-theoretic assumptions. A number of results have been obtained in this area and we present the following (incomplete) list of known results and conjectures. This list has been compiled by Frank Wagner and communicated [Wag06] to the present author, who has supplemented the list with several of the references. We leave several concepts undefined; interested readers may consult the appropriate references.

1. Theorem ([BCM79] with [CHL85]) $\aleph_0$-categorical superstable groups are virtually abelian of finite Morley rank.

   Theorem ([EW00]) $\aleph_0$-categorical supersimple groups are finite-by-virtually abelian of finite Lascar rank.

   Theorem ([Wag03]) Small profinite m-stable groups are virtually abelian of finite m-rank.

2. Theorem ([Fel78]; [BCM79]) $\aleph_0$-categorical stable groups are virtually nilpotent.

   Conjecture ([BCM79]) $\aleph_0$-categorical stable groups are virtually abelian.

   Theorem ([Mac88]) $\aleph_0$-categorical groups with a simple theory are finite-by-virtually nilpotent.

   Conjecture ([Mac88]) $\aleph_0$-categorical groups with a simple theory are finite-by-virtually abelian.

   Conjecture ([KW06]) Small profinite groups are virtually nilpotent (Newelski [New96, New02] conjectured they are virtually abelian).

3. Theorem ([BCM79] with [CHL85]) $\aleph_0$-categorical superstable rings are virtually null.

   Theorem ([KW06]) $\aleph_0$-categorical supersimple rings are finite-by-virtually null.

   Theorem ([KW06]) Small profinite $\mathcal{M}$-stable rings are virtually null.

4. Theorem ([BR77]) $\aleph_0$-categorical stable rings are virtually nilpotent.

   Conjecture ([BR77]) $\aleph_0$-categorical stable rings are virtually null.

   Theorem ([KW06]) $\aleph_0$-categorical rings with a simple theory are (finite-by-?)virtually nilpotent.

   Conjecture ([KW06]) $\aleph_0$-categorical rings with a simple theory are (finite-by-?)virtually null.

   Theorem ([KW06]) Small profinite rings are virtually nil (every element has power which is zero) of finite nil exponent.

   Conjecture ([KW06]) Small profinite rings are virtually nilpotent

5. Theorem ([CHL85]) $\aleph_0$-categorical superstable theories have finite Morley rank and are one-based

   Theorem ([Hru89]) $\aleph_0$-categorical supersimple theories need not be one-based

   Conjecture ([New96, New02]) small profinite $\mathcal{M}$-stable structures are m-normal (equivalent notion of one-based).

Since this dissertation primarily concerns itself with stable, $\aleph_0$-categorical structures, we isolate those results from the list that are relevant to our discussion.

Theorem (Felgner [Fel78]; Baur, Cherlin, Macintyre [BCM79]). *A stable, $\aleph_0$-categorical group is nilpotent by finite.*

The first step in both Felgner's and BCM's proofs of this theorem is to show that an infinite stable, $\aleph_0$-categorical group cannot be simple (in the sense of group theory). BCM proceed by arguing (using a result of Šunkov [KW73, p. 176]) that a minimal simple counterexample would have to take on the form of $\mathrm{PSL}_2(F)$ for some infinite locally finite field F. This violates $\aleph_0$-categoricity since F is interpretable in $\mathrm{PSL}_2(F)$ and all $\aleph_0$-categorical fields are finite. Felgner eliminates simple groups by a heavily group-theoretic analysis of nilpotent by finite subgroups and centralizers of involutions. Alternately, one can proceed as in Theorem 1.13 of Poizat [Poi01], by exploiting the classification of finite simple groups to know each such group is 2-generated (this was not available to the earlier authors, though Felgner remarked on its utility should it be true).

From there, all authors (Felgner, BCM and Poizat), reduce from the solvable case to the nilpotent case by analyzing the socle, p-Sylow subgroups, and nilpotent subgroups.

Theorem (Baur, Cherlin, Macintyre [BCM79]). *An $\aleph_0$-categorical ω-stable group is abelian by finite.*

This result can be extended to the class of $\aleph_0$-categorical, superstable groups on account of a theorem of Cherlin, Harrington and Lachlan [CHL85] which proves that a superstable, $\aleph_0$-categorical theory is necessarily a theory of finite Morley rank. A major ingredient to the proof in the ω-stable case is the property that an ω-stable group has the descending chain condition on all definable subgroups, i.e. there is no infinite descending chain of definable subgroups. In contrast, in a general stable group we only have the descending chain condition on uniformly definable subgroups. We outline their proof, which is by contradiction. Given a counterexample, BCM reduce to a counterexample of nilpotence class 2 (this reduction, as noted by BCM, works for $\aleph_0$-categorical, stable groups and we have reproduced the details of such an argument in Chapter 3). From there, one sees that the commutator $[\cdot, \cdot]$ can be considered to be a bilinear map from $G/Z(G) \times G/Z(G)$ into the commutator subgroup. Finally, using the descending chain condition on all definable subgroups, the authors are able to minimize the counterexample to have no proper infinite definable subgroups modulo the center and where essentially $G' = \sum_{i=1}^{n} [a_i, G]$ for some finite number $a_i \in G$.[1] BCM then argue directly that such a group must be trivial by finite, by producing quasiendomorphism rings and implicitly using the descending chain condition on all definable groups once again to argue the quasiendomorphism ring is a field, in contradiction to $\aleph_0$-categoricity.

In light of these two theorems, Baur, Cherlin and Macintyre conjectured that the conclusion for stable $\aleph_0$-categorical groups can be strengthened. We shall refer to this theorem throughout the dissertation as the BCM Conjecture.

BCM Conjecture (Baur, Cherlin, Macintyre [BCM79]). *A stable, $\aleph_0$-categorical group is abelian by finite.*

[1] We are being a little loose here in that one needs the correspondences established in Lemma 3.2.2 to know that the vector spaces and bilinear maps in BCM's argument correspond to counterexample groups.

If this conjecture is true, then we know exactly how the countable model of a stable $\aleph_0$-categorical group G will look. There will be a definable normal abelian subgroup A of finite index in G (cf. Section 2.3 on connected components). Since any $\aleph_0$-categorical group has finite exponent, A will necessarily be of the form

$$A \cong \bigoplus_{p \in P} \bigoplus_{n < n_p} \bigoplus_{i < \kappa_{n,p}} \mathbb{Z}/p^n\mathbb{Z}$$

for some finite set P of primes p, with n_p a finite positive integer, and $\kappa_{n,p}$ is either a finite nonnegative integer or ω. As a pure group, A would be totally transcendental since it is an abelian group of finite exponent; and hence A would be ω-stable of finite Morley rank. In fact, using modules, BCM were able to conclude that the original pure group G is ω-stable of finite Morley rank [BCM79, Theorem 63].

As a final historical remark, we draw briefly attention to the corresponding theorems and conjectures for rings possessing stability and $\aleph_0$-categoricity. We shall save the discussion of the results relating to those algebraic structures until Chapter 4.

1.2 Quest for Counterexamples

In the context of stability and $\aleph_0$-categoricity, there was a more central conjecture than Conjecture 1.1 which drove investigations. This was the conjecture of Lachlan:

Conjecture (Lachlan's Conjecture [Lac74])**.** *A stable, $\aleph_0$-categorical theory is ω-stable.*

The discussion in the previous section determined that if the BCM Conjecture were true, then at least as pure groups, any stable, $\aleph_0$-categorical group would be ω-stable. Thus, the truth of the BCM conjecture would lend credence to the truth of Lachlan's Conjecture. Unfortunately, Lachlan's Conjecture was disproved by Hrushovski [Hru89] (discussed in [Wag94]). Hrushovski's disproof of Lachlan's Conjecture cast doubt on the truth of the BCM Conjecture, however all methods based on Hrushovski's ideas have to date failed to produce a counterexample.

Hrushovski's disproof of Lachlan's conjecture hinged upon a generalization of Fraïssé constructions. Rather than including all possible finite structures into the limiting process, one is more selective about which sets and which embeddings between these sets you will allow into the amalgamation process. With a particular selection criterion, one is able to guarantee that the Hrushovski-Fraïssé limit will be stable. Even though Fraïssé limits are a natural way to obtain $\aleph_0$-categorical structures, the amalgamation described by Hrushovski does not easily result in $\aleph_0$-categoricity. By striking a careful balance between the freedom needed for $\aleph_0$-categoricity and the strictness needed for stability, Hrushovski was able to construct his counterexample to Lachlan's conjecture.

Hrushovski's disproof produced a stable, $\aleph_0$-categorical *graph*; it took further groundwork by Baudisch to generalize Hrushovski's limit construction to produce groups. With these generalized methods, Baudisch has constructed multiple $\aleph_1$-categorical groups that have some pathological properties [Bau96b] and [Bau96a]. However, as Baudisch himself noted, there are obstacles to applying these methods to construct $\aleph_0$-categorical groups. In [Bau00], he explains the difficulty in controlling the size of the algebraic closure when performing the counterexample construction. Without good control, the construction results in infinitely many 1-types, clearly ruling out $\aleph_0$-categoricity.

1.3 Summary

In light of the difficulties faced in obtaining a counterexample, it is unclear whether the Baur-Cherlin-Macintyre Conjecture will be disproved as Lachlan's Conjecture was. The current evidence is mixed in its indications. In this dissertation, we provide computations, reductions and theorems which could aide in an eventual positive proof of the BCM Conjecture. Even if the BCM Conjecture proves to be false, these results will be informative about the kinds of counterexamples that are possible.

The chapters are structured as follows.

Chapter 2: Preliminaries. We begin with a short discussion of the basic model theoretic notions of $\aleph_0$-categoricity and stability, especially as applied to groups. The final section provides an extensive discussion of the important notion of connectedness of groups, with several lemmas.

Chapter 3: First Group Reduction. In this chapter we reduce a counterexample to the BCM Conjecture to one which has a number of useful properties, including nilpotence class 2. We reframe the BCM Conjecture in the language of vector spaces over finite fields and bilinear maps between them. We perform two important constructions of nilpotent class 2 groups from vector spaces and bilinear maps.

Chapter 4: Rings. A discussion of stable, $\aleph_0$-categorical rings, including an alternate proof of Baldwin and Rose's theorem that such rings are nilpotent by finite. We also prove the equivalence of the BCM conjecture with the corresponding conjecture for rings.

Chapter 5: Second Group Reduction. Using the vector space constructions from Chapter 3, we break our possible counterexamples into three cases, based on the number of maximal connected abelian subgroups. In each case, we strive to prove results on the structure of the commutator group, primarily how the images $[a, G]$ and $[b, G]$ intersect for distinct elements of G.

Chapter 6: Quasiendomorphism Rings. We provide a detailed introduction to the tool of quasiendomorphism rings. The first application is a fairly simple example of how quasiendomorphism rings may arise in the study of stable, $\aleph_0$-categorical groups. The second application proposes an abstract framework in which one can build a quasiendomorphism ring from a family of definable homomorphisms. We then conclude that such a quasiendomorphism ring is necessarily finite. We argue how this result could be used as the final step in a proof of the BCM Conjecture, and have corollaries that apply to several of the situations described in Chapter 5.

1.4 Notation and Convention

In this dissertation we shall use the phrase $\aleph_0$-categoricity to conform with the usage of cardinals to describe uncountable categoricity. However, we inform the reader that the ordinal phrase ω-categorical is often used in the literature to refer to countable categoricity.

Similarly, when talking about sets definable over a set A, there are two popular notations for dealing with the case when $A = \emptyset$. We shall say the B is **0-definable** when it is definable over $\emptyset$ (other authors use $\emptyset$-definable). However, we will say "type over the empty set" or "$\emptyset$-type" instead of 0-type.

When we say that a group or ring has "nilpotence class k", we mean nilpotence class exactly k. If we simply have k as an upper bound on the nilpotence class, we will say the group has "nilpotence class at most k".

Chapter 2

Preliminaries

This chapter concerns basic notions relating to $\aleph_0$-categoricity and stability in the context of groups and other algebraic structures. The first two sections concern basic notions tied to the model theoretic properties. The third section goes into detail about the concept of connectedness in groups, proving many propositions which will be frequently used in the sequel.

2.1 Countable categoricity

The following theorem, attributed to Ryll-Nardziewski, Engeler and Svenonius, is the springboard for any study of $\aleph_0$-categorical theories. It can be found in any introductory model theory book, such as [Hod97] or [CK90].

Theorem 2.1.1 (Engeler, Ryll-Nardziewski, Svenonius)**.** *Let L be a countable first-order language and let T be a complete theory in L with infinite models. The following are equivalent:*

1. *Any two countable models of T are isomorphic.*
2. *If A is any countable model of T, then $Aut(A)$ is oligomorphic (for every n, the action of $Aut(A)$ on A^n has only finitely many orbits).*
3. *T has a countable model A such that $Aut(A)$ is oligomorphic.*
4. *Some countable model of T realizes only finitely many complete n-types for each $n < \omega$.*

5. *For each $n < \omega$, $|S_n(T)| < \aleph_0$.*

6. *For each arity n, there are only finitely many pairwise non-equivalent formulas $\phi(\overline{x})$ of L modulo T, where $\ell(x) = n$.*

7. *For each $n < \omega$, every type in $S_n(T)$ is principal.*

Any model of an $\aleph_0$-categorical theory is $\aleph_0$-saturated. Indeed, if $A \subseteq M$ is finite, then we may add constants to the language for the elements of A; this does not alter the $\aleph_0$-categoricity. In this extended language, there are only finitely many 1-types in the theory–they must all be principal and hence are realized in all models–in particular in M. In addition to being $\aleph_0$-saturated, the unique countable model of an $\aleph_0$-categorical theory is also strongly $\aleph_0$-homogeneous, meaning that any partial isomorphism between finite sets in the model extends to an automorphism of the model.

Corollary 2.1.2. *Suppose M is the countable model of an $\aleph_0$-categorical theory and $A \subseteq M$ is finite. If $S \subseteq M^n$ is fixed setwise by all automorphisms which fix A pointwise, then S is definable over A. In particular, A has finite algebraic closure. Furthermore, for any k, there is a uniform $f(k)$ such that if $|A| \leq k$, then $|acl(A)| \leq f(k)$.*

Proof. Consider all the types $\text{tp}(\overline{b}/A)$ for $\overline{b} \in S$. Since A is finite, by the Engeler, Ryll-Nardziewski, Svenonius theorem there are only finitely many types over A and each one is principal. Hence for each n-type over A we may choose an isolating formula; pick $\phi_i(\overline{x}; \overline{a}_i)$ for $1 \leq i \leq k$ which isolate the types of elements of S over A. We claim $S = \bigcup_{i=1}^{k} \phi_i(G^n; \overline{a}_i)$. Since automorphisms send elements of the same type to one another, S is certainly contained in the union, since any automorphism which fixes the $\overline{a}_i$ pointwise fixes the union. On the other hand, any $\overline{g} \in G^n$ which satisfies $\phi_i(\overline{x}; \overline{a}_i)$ for some $1 \leq i \leq n$ has the same type over A as some $\overline{b} \in S$. By $\aleph_0$-homogeneity, there is an automorphism of M which fixes A pointwise and sends $\overline{b}$ to $\overline{g}$. Since S is fixed setwise by such automorphisms, $\overline{g} \in S$.

For the second statement of the corollary, it suffices to recall that there are finitely many 1-types over A, and thus finitely many algebraic types, which each have only finitely many realizations. For the uniform bound, note that for a given k, there are only finitely many k-types. If $\phi(x; \overline{y})$ is a formula of $(k+1)$-arity, then consider the formula $\exists^{=n} x \phi(x; \overline{b})$, stating there are exactly n elements which satisfy $\phi(x; \overline{b})$. This formula (or its negation) is in the type of $\overline{b}$, so all $\overline{b}'$ with the same type as $\overline{b}$ must have the same algebraic formulas and same number of realizations to those formulas. In short, they must have isomorphic algebraic closures, in particular, the algebraic closures must have the same size. Since there are only finitely many k-types, there are only finitely many possible sizes of the algebraic closures of k-sets. □

A common use of this corollary is to observe that characteristic subgroups of a countable $\aleph_0$-categorical group are always 0-definable.

We now turn our attention to one important instance of an $\aleph_0$-categorical algebraic structure. The following theorem, attributable to folklore, is often used in arguments by contradiction for $\aleph_0$-categorical theories: one cannot interpret infinite fields in an $\aleph_0$-categorical theory.

Theorem. *An $\aleph_0$-categorical skew field is finite.*

Proof. Let F be an $\aleph_0$-categorical skew field. Since we have only finitely many 1-types, the elements $a, a^2, a^3, \ldots$ cannot all be distinct, so every nonzero element of F has finite multiplicative order. Again, elements that have different multiplicative orders must have different types, so since there are finitely many 1-types, there is an n such that $a^n = 1$ for all nonzero $a \in F$. For any two nonzero elements $a, b \in F$, the subring generated by a, b must be finite by Corollary 2.1.2 since it is contained in the algebraic closure of $\{a, b\}$. By Wedderburn's theorem, finite division rings are finite fields, so a and b commute. Hence F was a field to start with. Any $n+2$ distinct elements of F generate a finite subfield F_0 of size at least $n+2$. The multiplicative group of F_0 is cyclic of order at least $n+1$, a contradiction to the fact that n is a bound on the multiplicative order of any element of F. Hence F has at most $n+1$ elements and thus is finite. □

2.2 Stable groups

The theory of stable groups is very rich and there exist at least two well-written treatises of the subject: [Poi01] and [Wag97]. We excerpt a few important results here; others will appear in later sections as needed.

Lemma 2.2.1 (Poizat [Poi01] Lemma 1.1)**.** *A nonempty stable associative monoid with left and right cancellation, or with left cancellation and right identity, is a group.*

In any stable theory, we have the **Descending Chain Condition (DCC)** on any uniformly definable family of definable sets. However, with definable groups, we get stronger behavior.

Theorem 2.2.2 (Baldwin Saxl [BS76])**.** *In a stable group G, every formula $f(x, \overline{y})$ is associated with a natural number n such that the intersection of an arbitrary family of subgroups H_i defined by formulas $f(x, \overline{a}_i)$ is the intersection of some n among them. Consequently, the groups which are intersections of any number, finite or infinite, of subgroups defined by formulas $f(x, \overline{a}_i)$ form a uniformly definable family.*

Theorem 2.2.2 is so ubiquitous in the literature on stable groups that we shall simply refer to it as the **Baldwin-Saxl condition**. Similarly, the descending chain condition henceforth will be referred to as DCC.

2.3 Connectedness

When working with infinite groups, it is helpful to determine conditions which guarantee that proper subgroups have infinite index. For this task, we import the idea of *connectedness* from topology, where it has been used extensively to study topological groups, algebraic groups and groups occurring in several other fields. In model theory, this idea has played an important role in the study of stable groups, particularly groups of finite Morley rank. Connectedness, as it turns out, shall be a robust concept in our context as well.

Definition 2.3.1. A group G is **connected** if G has no proper definable subgroups of finite index.

A few words about definability: definability will always be in the context of some ambient theory T in which the group is interpretable. This theory will be mentioned explicitly in situations where confusion may arise. Since "definable" refers to "definable with parameters", we must be precise in the previous definition about where we allow such parameters to come from. Generally speaking, we will allow parameters to come from a monster model, $\mathcal{M}$, of our theory, which will be sufficiently saturated for our considerations. We shall comment below on the degree of saturation needed to compute whether a group is connected, but first we need a definition related to connectedness.

Definition 2.3.2. Given a group G, the **connected component** of G, denoted G^0, is the intersection of all definable subgroups of G of finite index.

Clearly if G^0 has finite index in G, then G^0 is connected. In particular, G is connected if and only if $G = G^0$.

Remark 2.3.3. Notation: when we take the connected component of a group with a parenthetical, we shall put the ^{0} to the left of the parenthetical. For example $C^0_G(g)$ instead of $(C_G(g))^0$ and $Z^0(G)$ instead of $(Z(G))^0$.

As before, in the definition of connected component, "definable" means definable with parameters coming from some sufficiently saturated extension of G. The degree of saturation needed for a computation can be determined after a closer examination of the definition of the connected component. In a fixed theory T, the connected component is actually given by a type, which we now describe. Given a formula $\phi(x;\overline{y})$ of our language and parameters $\overline{a}$, it is a definable property whether the realizations of $\phi(x;\overline{a})$ form a subgroup. We shall write $\text{Group}(\phi,\overline{a})$ for the formula that states this property. We define the formulas $\theta_{\phi,n}(x)$, where the indices run through all natural numbers n and all formulas $\phi(x;\overline{y})$ for all arities $\ell(\overline{y})$, as

$$\forall\overline{a}\left(\left[\text{Group}(\phi,\overline{a})\wedge\forall b_1,\ldots b_n\bigvee_{1\leq i<j\leq n}\phi(b_ib_j^{-1},\overline{a})\right]\rightarrow\phi(x,\overline{a})\right)$$

Then the partial type consisting of all $\theta_{\phi,n}(x)$ is clearly the partial type of the connected component, since its realizations are precisely those elements which are in all definable groups of finite index. Call the partial type of the connected component $p^0(x)$; note it is a type over $\emptyset$. However, it is not always a complete type, so that in small models this $\emptyset$-type may coincide with (0-)definable sets, even if G^0 is not definable.

Example 2.3.4. We illustrate why we have brought attention the issues of definability and saturatedness. Consider the additive group $G=(\mathbb{Z},+,0)$ as a pure group. The subgroups nG for $n\in\mathbb{N}$ are all definable and have finite index, thus $G^0=\{0\}$. In this model, the connected component is a 0-definable group, but that is a deceptive happenstance. As we shall see, the type of the connected component is not the $\emptyset$-type isolated by $x=0$. Let G' be an a $\aleph_0$-saturated nonstandard elementary extension of G. Since nG had finite index in G and this is a definable property of the definable set nG, we must have that nG' has finite index (the same index, in fact) in G'. If $H\leq G'$ is some other definable group of finite index, it must be normal since G' is abelian, so for every $g\in G'$ there is an n such that $ng\in H$. Pick a minimal one for each g and call it n_g. If there were a sequence $g_1,g_2,\ldots\in G'$ such that $n_{g_1}<n_{g_2}<\ldots$, then by compactness, the type that says $nx\notin H$ for all $n\in\mathbb{N}$ is consistent. This is a type over the same parameters used to define H, so since G' is

$\aleph_0$-saturated, this type would be realized in G', a contradiction. Hence there is a universal N such that $NG' \subseteq H$. But this means that once again $(G')^0 = \cap_{n\in\mathbb{N}} nG'$. Yet the set on the right is not $\{0\}$. Indeed, the $\emptyset$-type consisting of the formulas $\exists x \forall y \bigwedge_{m<M} x \neq my$ indexed by $M \in \mathbb{N}$ is consistent in $\mathbb{Z}$, so it is realized in G', and all realizations of this type are in $\cap_{n\in\mathbb{N}} nG'$ and hence $(G')^0$. In fact, our analysis has shown that the type $p^0(x)$ of the connected component is simply the partial $\emptyset$-type consisting of the formulas $\exists y\, ny = x$ for all $n \in \mathbb{N}$. It is only a partial $\emptyset$-type, since for example, it contains neither of the formulas $x = 0$ and $x \neq 0$.

Generally, the number of definable subgroups of finite index in G is bounded above by $\kappa = |T| + 2^{|G|} + \aleph_0$, so to compute the connected component in a group in an arbitrary theory, we may take $\mathcal{M}$ to be a κ^+-saturated elementary extension of the model in which we have interpreted G. In stable theories, however, we require far less saturation. Moreover, G^0 is connected to the extent observable in the theory.

Lemma 2.3.5. *If G is a stable group, then G^0 is an intersection of at most $|T|$ definable subgroups of finite index. Hence G^0 can be computed in any $|T|^+$-saturated elementary extension of G. Furthermore if G is $|T|^+$-saturated, then G^0 has no proper relatively definable subgroups of finite index. Thus, from the perspective of our ambient theory, G^0 is connected.*

Proof. Reexamine the type $p^0(x)$ of G^0. For every formula $\phi(x;\overline{y})$, consider the subgroups of the form $\phi(G;\overline{a})$ which are finite index in G. They are a uniformly definable family, so by Baldwin-Saxl, their intersection equals an intersection of only finitely many of them. So G^0 is an intersection of $|T|$ many definable groups of finite index: each formula $\phi(x;\overline{y})$ only needs to be considered for finitely many choices of parameters $\overline{y}$. Since we can elementarily embed the $|T|$ many parameters into an $|T|^+$-saturated extension of G, this model can accurately compute the intersection of the subgroups $\phi(x;\overline{a})$ which have finite index, for each formula $\phi(x;\overline{y})$ of the language. Thus such a model has the correct computation of G^0.

Now suppose G is $|T|^+$-saturated and suppose G^0 has a relatively definable subgroup H of finite index, i.e. there is a definable subset S of G such that $S \cap G^0 = H$ and H has finite index in G^0. Say $S = \phi(G;\overline{a})$ for some parameters $\overline{a}$ in our monster model. But then H is the set of realizations to the $\overline{a}$-type $p^0(x) \cup \{\phi(x;\overline{a})\}$. By [Poi81] (or alternately Theorem 5.17 of [Poi01]), any type definable subgroup is equal to an intersection of $|T|$ many definable groups. So $H = \cap_{i<\kappa} F_i$, where each $F_i = f_i(G;\overline{a}_i)$ is a definable subgroup of G. We shall show that each $F_i \supseteq G^0$; for contradiction, choose such an F with $G^0 \cap F$ a proper (finite index) subgroup of G^0.

Enumerate the formulas of the language as $(\phi_i \mid i < \kappa)$. For each formula $\phi_i(x;\overline{y})$ of the language, we can consider the intersection of G with all finite index subgroups of G of the form $\phi_i(x;\overline{b})$. As mentioned in the first paragraph, this is equal to a finite intersection and hence is a definable, normal subgroup K_i of finite index. We claim that $F \cap K_i$ has finite index in K_i for some $i < \kappa$. If we can do this, then $F \cap K_i$ has finite index in G and hence so does F. But then $F \cap G^0 = G^0$ by definition of G^0.

Assume, therefore that $F \cap K_i$ has infinite index in each K_i. Since each K_i is definable (with parameters), we may let $\psi_i(x;\overline{a}_i)$ define K_i and let $\theta(x;\overline{b})$ define F. For any finite $I \subseteq \kappa$, we have infinitely many elements $\{c_n\}_{n<\omega}$ of $\bigcap_{i\in I} K_i$ which are pairwise inequivalent modulo $F \cap \bigcap_{i\in I} K_i$. In other words, for every $N < \omega$, the c_n satisfy the formula $\Phi_{I,N}(x_1, \ldots, x_N)$

$$\bigwedge_{n<N} \bigwedge_{i\in I} \phi_i(x;\overline{a}_i) \wedge \bigwedge_{i<j<N} \neg\theta(x_i x_j^{-1};\overline{b})$$

Therefore $\Phi = \{\Phi_{I,N} \mid I \subseteq_{\text{fin}} \kappa,\, N < \omega\}$ is consistent; by compactness, in some elementary extension $G' \succeq G$, we can find distinct $\{c_n\}_{n<\omega}$ such that for all $n < m < \omega$ and all $i < \kappa$, $G' \models \phi_i(c_n;\overline{a}_i)$ and $G' \models \neg\theta(c_n c_m^{-1};\overline{b})$. Since the $\{c_n\}_{n<\omega}$ are countable in number, the $|T|^+$-saturatedness of G lets us take $G' = G$. Hence we get $G^0 = \bigcap_{i<\kappa} \phi_i(G;\overline{a}_i) \supseteq \{c_n \mid n < \omega\}$. Thus $F = \theta(G;\overline{b})$ has infinite index in G^0, a contradiction to the assumption on F. So G^0 is connected (in terms of relatively definable subgroups of finite index). □

In the case of $\aleph_0$-categoricity, we have a weaker conclusion about the connected component.

Proposition 2.3.6. *If G is an $\aleph_0$-categorical group, G^0 is a 0-definable subgroup.*

Proof. The automorphic image of a definable group of finite index is another definable group of finite index. Hence G^0 is characteristic. By Corollary 2.1.2, G^0 is 0-definable. □

The combination of stability and $\aleph_0$-categoricity will force the connected component to be easily computable (see Proposition 2.3.14 below). Before proceeding to that restricted model theoretic setting, we provide a number of general properties of connected groups.

Proposition 2.3.7. *If H is a (definable) subgroup of G, then $H^0 \leq G^0$.*

Proof. For any definable subgroup I of finite index in G, we have that $I \cap H$ has finite index in H, and it is (relatively) definable in H with the same parameters used to define I. Hence $H \cap G^0 = H \cap \bigcap_{I \in \mathcal{D}} I \supseteq H^0$, where $\mathcal{D}$ is the collection of definable subgroups of G of finite index. □

Proposition 2.3.8. *If G is a connected group and $f : G \to H$ is a definable homomorphism, then $f(G)$ is connected. In particular, if G is connected and N is a definable normal subgroup of G, then G/N is connected.*

Proof. If I is a definable finite index subgroup of $f(G)$, then $f^{-1}(I)$ is a definable finite index subgroup of G. Hence $f^{-1}(I) = G$ and $I = f(G)$. □

We have a partial converse:

Proposition 2.3.9. *If G is a group with a connected definable normal subgroup N such that G/N is also connected, then G is connected.*

Proof. If $K \leq G$ is a definable subgroup of finite index, then KN is also definable and of finite index. Since N is a normal subgroup, we may pass to the quotient KN/N. This is a finite index, definable subgroup of G/N, so by connectedness it equals G/N. Hence $KN = G$. But K is a finite index, definable subgroup of G, so by the Second Isomorphism Theorem, $K \cap N$ is a finite index, definable subgroup of N. By connectedness of N, $K \cap N = N$. Hence $G = KN = K$ and G is connected. □

Proposition 2.3.10. *If A and B are connected groups, then $A \times B$ is also connected.*

If $A, B \leq G$, A is normal and A and B are connected, then the group product AB is connected.

Proof. Cross product: Since A and B are connected and $(A \times B)/A \cong B$, Proposition 2.3.9 tells us that $A \times B$ is connected.

Group product: $AB/A \cong B/(A \cap B)$ by the Second Isomorphism Theorem. Since $B/(A \cap B)$ is connected by Proposition 2.3.8 and A is connected, we know AB is connected by Proposition 2.3.9. □

Under model theoretic assumptions, we obtain greater information about connected components. For example, under stability we discover that connected groups generate connected groups:

Proposition 2.3.11. *Assume our ambient theory is stable. If $(A_i \mid i \in I)$ are connected groups and $A = \langle \bigcup_{i \in I} A_i \rangle$ is definable, then A is connected.*

Proof. Suppose B is a proper, definable, finite index subgroup of the definable group A. Then all the conjugates B^a form uniformly definable family of finite index subgroups of A; by Baldwin-Saxl, their intersection equals a finite intersection. So without loss of generality, we may assume B is normal.

B cannot contain every A_i, so choose one it does not contain. Then $A_i \cap B$ is a finite index subgroup of A_i by the Second Isomorphism Theorem, so $A_i \subseteq B$, a contradiction. □

Proposition 2.3.12 (Proposition 1.10 [Poi01])**.** *If G is a connected stable group and $Z(G)$ is finite, then $Z(G) = Z_2(G) = 0$; an infinite nilpotent connected stable group has infinite center.*

Proposition 2.3.13 (Cherlin [Che79])**.** *In a group G of finite Morley rank, G^0 is 0-definable and has finite index.*

In the context of $\aleph_0$-categoricity and stability, we have an analogous result.

Proposition 2.3.14. *Every $\aleph_0$-categorical stable group has a connected component G^0 which is 0-definable and has finite index.*

Proof. Proposition 2.3.6 gives us that G^0 is 0-definable. We revisit the proof of Lemma 2.3.5 to get that G^0 has finite index.

For each formula $\phi(x; \overline{y})$, we may consider those subgroups $G_{\phi,\overline{a}}$ which are defined by $\phi(G; \overline{a})$ and have finite index in G. By the Baldwin-Saxl condition, the intersection of this collection, G_ϕ, is equal to a finite subintersection; thus G_ϕ has finite index as well. Note that G_ϕ is fixed under all automorphisms of G, and hence is 0-definable by $\aleph_0$-categoricity (Lemma 2.1.2). By $\aleph_0$-categoricity, there are only finitely many 0-definable subgroups; in particular there are only finitely many G_ϕ. Thus G^0, which is the intersection of all these G_ϕ, has finite index. □

Proposition 2.3.15. *Let G be a stable group which is nilpotent by finite. Then G^0 is nilpotent. Furthermore, any nilpotent subgroup of G of finite index has nilpotency class at least as great as the nilpotency class of G^0.*

Proof. By Theorem 3.17 of Poizat [Poi01], if H is a nilpotent subgroup of class n, then it is contained in a definable nilpotent subgroup $\tilde{H}$ of class n. If H has finite index, then so does $\tilde{H}$ and hence $G^0 \leq \tilde{H}$ and G^0 is nilpotent. Clearly the nilpotency class of G^0 is at most the nilpotency class of $\tilde{H}$. □

Chapter 3

First Group Reduction

In this section, we shall suppose that the BCM Conjecture (Conjecture 1.1) is not true. Given this, we shall infer that counterexamples with certain strong group-theoretic properties must exist.

3.1 Nilpotence

By Proposition 2.3.14, any stable, $\aleph_0$-categorical group G has a connected component G^0 which is of finite index and 0-definable in G. Therefore, we may already assume our example is connected. By the Theorem 1.1, G must be nilpotent by finite and since G is connected, by Proposition 2.3.15 it is nilpotent.

An $\aleph_0$-categorical group must have finite exponent, so let $\exp(G) = e$. Since G is a nilpotent group, its torsion subgroup is equal to the direct sum of its Sylow subgroups G_p, all of which are normal (and thus unique by the infinite Sylow theorem). Since G has finite exponent e, $G = \prod_{p|e\, prime} G_p$. All the G_p are 0-definable, so since G is connected, they are all infinite. In fact, they must also be connected, since if $G_p^0 \neq G_p$, then $H = G_p^0 \times \prod_{q|e\, prime,\, q\neq p} G_q$ is a finite index definable subgroup of G. Consequently, we obtain the following observation.

Proposition 3.1.1. *If there is a stable, $\aleph_0$-categorical group G of exponent e which is not abelian, then for some prime $p|e$, there is a connected, stable, $\aleph_0$-categorical group of exponent $\mathsf{v}_p(e)$ which is not abelian (where $\mathsf{v}_p(e)$ is the p-adic valuation of e).*

Proof. If all the G_p are abelian, then so is G since it is a direct product of them. Hence at least one of them is not abelian. □

So now we have reduced our example to being a connected, p-group for some p. We may continue by restricting the nilpotence class.

Proposition 3.1.2. *If G is a connected, $\aleph_0$-categorical, stable group of nilpotence class $k \geq 2$, then there is a 0-definable, connected, $\aleph_0$-categorical, stable quotient of G of nilpotence class 2.*

Proof. If $k = 2$ we are done. Otherwise, let $Z_{k-2}(G)$ be the $(k-2)$th center of G (here $Z_{i+1}(G)$ is the preimage of the center of $G/Z_i(G)$ in G). Then G/Z_{k-2} has nilpotence class 2 by the definition of nilpotence class. Furthermore, since Z_{k-2} is 0-definable, this quotient group is 0-definable and must be connected by Proposition 2.3.8. □

To prove several other properties, we first need to recall some properties of nilpotent groups of class 2.

Proposition 3.1.3. *Suppose H is nilpotent of class 2. Then all of the following hold:*

1. *The map $[\cdot,\cdot] : H \times H \to Z(H)$ given by $[g_1, g_2] = g_1^{-1}g_2^{-1}g_1g_2$ induces a bilinear map $[\cdot,\cdot] : H/Z(H) \times H/Z(H) \to Z(H)$.*
2. *For all $g_1, g_2 \in H$, $ord([g_1, g_2]) \mid \gcd(ord(g_1), ord(g_2))$.*
3. *For all $g \in H$, $C_H(g)$ is normal.*
4. *For all $g, h \in H$, for all $n \geq 1$, we have $(gh)^n = g^n h^n [g, h]^{n(n-1)/2}$.*
5. *For every odd n, the set $\Omega_n(H) = \{x \in H \mid ord(x)|n\}$ forms a subgroup.*
6. *For every odd prime p, the set $S_p(G)$ of all p-power-elements forms a subgroup, known as the p-Sylow subgroup.*

Proof. These are all standard results which can be found in most references on group theory (see [Hal59], for example). The bilinearity immediately implies (2). For all $g \in H$, $\ker([g,\cdot]) = C_H(g)$ and so for all $g \in H$, $C_H(g) \trianglelefteq H$. (4) is the well-known Collection Formula, which can be found in [Hal59]. Finally, (5) and (6) follow immediately from (2) and (4). □

Under the assumption of connectedness, we get an additional, important property of nilpotent class 2 groups.

Lemma 3.1.4. *If G is a connected group of nilpotence class 2, then G', the commutator subgroup, is also connected.*

Proof. Suppose G' has a proper definable subgroup H of finite index. Since G' is generated by $\bigcup_{g\in G}[g,G]$, it must be that H does not contain one of these groups, say $[g,G]$. By class two nilpotence, $[g,G]$ is a subgroup and $x \mapsto [g,x]$ is a definable homomorphism from G onto $[g,G]$. By Proposition 2.3.8, $[g,G]$ is connected. Since $H \cap [g,G]$ is a definable finite index subgroup, it must be equal to $[g,G]$ and hence $[g,G] \subseteq H$, a contradiction. □

Lastly, under the assumptions of stability and $\aleph_0$-categoricity, we may perform manipulations on centralizers to achieve particular properties.

Proposition 3.1.5. *Suppose G is a stable $\aleph_0$-categorical group which is not abelian. Then there is a definable connected subgroup $H \leq G$ which is not abelian such that for all $x \in H\backslash Z(H)$, $C_H^0(x)$ is abelian. Also, $H \cap Z(G) \supseteq Z^0(G)$.*

Proof. Assume that $C(g)$ is not already abelian by finite for every $g \notin Z(G)$. Consider the collection of $\bigcap_{g\in S} C(g)$ as S varies over all the finite subsets of G. This is a uniformly definable family by Baldwin-Saxl, so by the DCC we may choose an H in the family that is minimal and not abelian by finite. Let S be a corresponding finite subset of G yielding H. For every $h \in H$, $C_H(h)$ is just $C_G(h) \cap \bigcap_{g\in S} C_G(g)$. By minimality, $C_H(h)$ is abelian by finite, or else $H \subseteq C_G(h)$, in which case $h \in Z(H)$. Thus H has the desired property, save perhaps connectedness. But by Proposition 2.3.7, we will have $C^0_{H^0}(h) \leq C^0_H(h) \leq H^0$ for every $h \in H$, so the connected group H^0 will have the desired property as well. The statement about $Z^0(G)$ follows from the fact that $Z(G) \subseteq C_G(g)$ for all $g \in G$, so $Z(G) \subseteq H$ and by Proposition 2.3.7 $Z^0(G) \subseteq H^0$. □

We now group all the results into one full statement.

Proposition 3.1.6. *If there is an $\aleph_0$-categorical stable group which is not abelian by finite, then there is a group G which is:*

1. *stable,*

2. *$\aleph_0$-categorical,*

3. *connected,*

4. *nilpotent of class* 2*,*

5. *a p-group of finite exponent, where*

6. $G/Z^0(G)$ *is an elementary p-group,*

7. G' *is an elementary p-group,*

8. G' *is connected,*

9. *for odd primes p,* $x \mapsto x^p$ *is a homomorphism from* G *into* $Z(G)$*,*

10. *for* $p = 2$*,* $x \mapsto x^4$ *is a homomorphism from* G *into* $Z(G)$*, and*

11. *for all* $g \in G \backslash Z(G)$*,* $C(g)$ *is abelian by finite.*

Proof. A combination of Propositions 3.1.1 and 3.1.2 gives us a connected, stable, $\aleph_0$-categorical p-group G of nilpotence class 2.

Next we reduce to the case where $x^p = 1$ for every $x \in G' = [G, G]$. For each $k \geq 0$, let $\Omega_{p^k}(Z(G)) = \{x \in Z(G) \,|\, \mathrm{ord}(x) \leq p^k\}$, which is a subgroup of the center since $Z(G)$ abelian. Pick the largest $k \geq 0$ for which $[G, G] \not\subseteq \Omega_{p^k}(Z(G))$. If we then quotient G by $\Omega_{p^k}(Z(G))$, we preserve all the properties of G obtained so far, but gain that $[G, G] \subseteq \Omega_p(Z(G))$. Also, by bilinearity, for every $x, y \in G$ we have $[x^p, y] = [x, y]^p = 1$, so $x^p \in Z(G)$ for all $x \in G$. Hence $G/Z(G)$ has exponent p, and since it is abelian, it is an $\mathbb{F}_p$ vector space. The connectedness of G' comes from Lemma 3.1.4.

Lastly, for odd primes p, $x \mapsto x^p$ is a homomorphism from G into $Z(G)$ by (4) in Proposition 3.1.3. This same result proves the statement for $p = 2$ that $x \mapsto x^4$ is a homomorphism under the already proven hypothesis that $\exp(G') = 2$ when $p = 2$. Since G is connected, the image I of G under the appropriate homomorphisms for p, is a connected group by Proposition 2.3.8. Hence it must be a subgroup of $Z^0(G)$ by Proposition 2.3.7. So $G/Z^0(G)$ has exponent p; but since G' a connected subgroup of $Z(G)$, by Proposition 2.3.7, G' must be a subgroup of $Z^0(G)$. Hence $G/Z^0(G)$ is abelian and thus must be an $\mathbb{F}_p$-vector space.

Finally, an application of Proposition 3.1.5 gives us a group where all centralizers of noncentral elements are abelian by finite. This Proposition may reduce the commutator subgroup, which is not a problem, but it also may vary the center. However we know that this new group H contains $Z^0(G)$ and so $H/Z^0(H)$ must still be an $\mathbb{F}_p$-vector space and all our properties are preserved. $\square$

These properties will be present throughout the rest of the text, since they are conveniently preserved under (definable) subgroups and all but the final property are preserved under (definable) quotients.

3.2 Vector spaces and bilinear maps

By Proposition 3.1.6, we have reduced to a counterexample G where $G/Z(G)$ and G' are both $\mathbb{F}_p$ vector spaces (if $G/Z^0(G)$ is an $\mathbb{F}_p$-vector space, then clearly so is $G/Z(G)$). Also $[\cdot,\cdot]$ can be interpreted as a skew symmetric bilinear map from $G/Z(G) \times G/Z(G)$ to G'. Furthermore $G/Z(G)$ is a connected vector space and $[\overline{g}, G/Z(G)] = 0$ if and only if $\overline{g} = 0$, i.e. $g \in Z(G)$. Following this line, we observe that the BCM Conjecture (Conjecture 1.1) can be framed entirely in the language of vector spaces and bilinear maps over a finite field. Indeed, Baur, Cherlin, and Macintyre ([BCM79]) performed exactly such a translation of Theorem 1.1 on ω-stable, $\aleph_0$-categorical groups to the language of vector spaces.

Theorem 3.2.1. *There is a counterexample to the BCM Conjecture if and only if there are $\mathbb{F}_p$-vector spaces A, B, C and a bilinear map $f : A \times B \to C$ such that*

- *(A, B, C, f) is stable and $\aleph_0$-categorical*
- *A and B are connected in this theory*
- *$f(a, B) = 0$ if and only if $a = 0$*
- *$f(A, b) = 0$ if and only if $b = 0$, and*
- *the image of f generates C.*

Proof. We have already argued that the BCM Conjecture implies this statement about vector spaces. For the converse, we use the construction of a nilpotent class two groups from vector spaces which will be described in Lemma 3.2.2. Since the constructions are definable, they will produce a stable, $\aleph_0$-categorical connected group which is not abelian. $\square$

We note that for $p \neq 2$, we could have alternately proved this theorem with the construction in Lemma 3.2.3, provided we revise the statement of the theorem to require the bilinear form to be skew-symmetric in the statement of the theorem.

Lemma 3.2.2. *Let A, B, C be $\mathbb{F}_p$ vector spaces for some prime p, and suppose that $f : A \times B \to C$ is a bilinear form whose image generates C. Suppose further that $f(a, B) = 0$ iff $a = 0$ and $f(A, b) = 0$ iff $b = 0$. Then we can construct a group H with underlying set $A \times B \times C$ and multiplication defined as:*

$$(a, b, c) \otimes (a', b', c') := (a + a', b + b', c + c' - f(a', b))$$

H has the properties:

1. $\exp(H) = p$ *if p odd,* $\exp(H) = 4$ *if $p = 2$,*
2. *nilpotent of class* 2,
3. $[(a, b, c), (d, e, g)] = (0, 0, f(a, e) - f(d, b))$
4. $Z(H) = H' = 0 \times 0 \times C$
5. $A \times \ker(f(a, \cdot)) \times C$ *is the centralizer of any* $(a, 0, c)$
6. $\ker(f(\cdot, b)) \times B \times C$ *is the centralizer of any* $(0, b, c)$
7. $H = (A \times \{0\} \times C)(\{0\} \times B \times C)$
8. *if A and B are connected and either C is connected or the ambient theory is stable, then*
   - *H is connected*
   - *H' is connected*

Proof. We first verify that H is indeed a group with this operation. Clearly $(0, 0, 0)$ is the identity and the inverse of (a, b, c) is $(-a, -b, -c - f(a, b))$. Lastly, associativity is verified:

$$\begin{aligned}((a, b, c) \otimes (d, e, g)) \otimes (h, i, j) &= (a + d, b + e, c + g - f(d, b)) \otimes (h, i, j) \\ &= (a + d + h, b + e + i, c + g + j - f(d, b) - f(h, b + e)) \\ &= (a + d + h, b + e + i, c + g + j - f(d + h, b) - f(h, e)) \\ &= (a, b, c) \otimes (d + h, e + i, g + j - f(h, e)) \\ &= (a, b, c) \otimes ((d, e, g) \otimes (h, i, j))\end{aligned}$$

Since we are already performing calculations, let us compute the commutator of (a, b, c) and (d, e, g).

$$\begin{aligned}[(a,b,c),(d,e,g)] &= (a,b,c)^{-1}(d,e,g)^{-1}(a,b,c)(d,e,g)\\ &= (-a,-b,-c-f(a,b))(-d,-e,-g-f(d,e))(a,b,c)(d,e,g)\\ &= (-a-d,-b-e,-c-f(a,b)-g-f(d,e)-f(d,b))(a,b,c)(d,e,g)\\ &= (-d,-e,-f(a,b)-g-f(d,e)-f(d,b)-f(a,-b-e))(d,e,g)\\ &= (0,0,-f(a,b)-f(d,e)-f(d,b)-f(a,-b-e)-f(d,-e))\\ &= (0,0,f(a,e)-f(d,b))\end{aligned}$$

We are now ready to calculate the center of H, which is the set of all (a, b, c) such that $f(a,e)-f(d,b) = 0$ for all $(d, e, f) \in H$. Taking $d = 0$, we find that $f(a, e) = 0$ for all $e \in B$, so $a = 0$. Similarly, we conclude $b = 0$. Hence $Z(H) = 0 \times 0 \times C$. This is the commutator subgroup of H since the image of f generates C and $[(a, 0, 0), (0, b, 0)] = (0, 0, f(a, b))$ for all $a \in A$ and $b \in B$.

Knowing the center lets us see that $H/Z(H) \cong A \times B$, which is abelian, so H has nilpotence class 2. This also allows us to immediately conclude the connectedness results. If A and B are connected, then so is $A \times B$ (Proposition 2.3.10). If the ambient theory is stable, then by Proposition 2.3.11, we find that C is also connected, being generated by the union of the uniformly definable connected groups $f(a, B)$ for $a \in A$ (these are connected by Proposition 2.3.8). Hence H is the extension of a connected group $A \times B$ by another connected group $0 \times 0 \times C$, so H is connected by Proposition 2.3.9. $H' = 0 \times 0 \times C$ is obviously connected since C is.

The centralizer of $(a, 0, c)$ is the set of (d, e, f) such that $f(a, e) - f(d, 0) = 0$, which is $A \times \ker(f(a, \cdot)) \times C$. Similarly the centralizer of $(0, b, c)$ is $\ker(f(\cdot, b)) \times B \times C$.

For any $(a, b, c) \in H$, consider that $(a, 0, c)(0, b, 0) = (a, b, c - f(0, 0)) = (a, b, c)$, so indeed $H = (A \times \{0\} \times C)(\{0\} \times B \times C)$.

Lastly we determine the exponent of H:

$$\begin{aligned}(a,b,c)^p &= (pa, pb, pc - f(a,b) - f(a,2b) - \ldots - f(a,(p-1)b))\\ &= (0,0,-f(a,\sum_{i=1}^{p-1} ib))\end{aligned}$$

If p is odd, then this last term becomes $-f(a, 0) = 0$. If $p = 2$, then this term is $f(a, b)$, which is generally nonzero. However $(a,b,c)^4 = (0,0,f(a,b))^2 = 0$, so H has exponent 4. $\square$

Note that one of the properties of Proposition 3.1.6 is missing from the list: we are not *a priori* guaranteed that centralizers of noncentral elements are abelian by finite. Using the formula for the commutator, we see that for a general element (a,b,c), its centralizer is the set of elements (d,e,g) such that $f(a,e) = f(d,b)$. In general, if $f(a,e') = f(d',b)$ as well, there is no reason for $f(d,e') = f(d',e)$, i.e. no reason why $(d,e,g),(d',e',g') \in C(a,b,c)$ should commute. Even when we assume that we are working with a counterexample G from Proposition 3.1.6 where centralizers *are* abelian by finite, and use Lemma 3.2.2 on $A = B = G/Z(G), C = G'$ and $f = [\cdot,\cdot]$, we still have no guarantee that even specialized elements like $(a,0,c)$ have abelian centralizer connected components in H. Nonetheless, this lemma will be useful for constructing new counterexamples from "pieces" of existing counterexamples.

For the second vector space construction that can be used in the proof of Theorem 3.2.1, we need slightly more restrictive conditions. We assume that $p \neq 2$ and that our bilinear map goes from the cross product of a vector space with itself. These are natural conditions, however, when we consider a counterexample of odd exponent obtained by Proposition 3.1.6: our bilinear map goes from $G/Z(G) \times G/Z(G)$ to G'. A natural choice for vector spaces is $A = B = G/Z(G)$. In such a case we have a slight variation on the construction, assuming $p \neq 2$. This is the second construction that can be used in the proof of Theorem 3.2.1.

Lemma 3.2.3. *Let $p \neq 2$ be prime. Assume A, B are $\mathbb{F}_p$-vector spaces and $f : A \times A \to B$ is a skew-symmetric bilinear map. Assume $f(a,A) = 0$ if an only if $a = 0$ and that the image of f generates B. Then we can define a group H on $A \times B$ with multiplication given by:*

$$(a,b) \times (a',b') := (a+a', b+b'+f(a,a'))$$

H has the properties:

1. $\exp(H) = p$,

2. *nilpotent of class exactly* 2,

3. $[(a,b),(c,d)] = (0, 2f(a,c))$

4. $Z(H) = H' = 0 \times B$

5. $\ker(f(a,\cdot)) \times B$ *is the centralizer of any* (a,b)

6. if A *is connected and either* B *is connected or the ambient theory is stable, then*

- H *is connected*
- H' *is connected*

Proof. The identity of H is found to be $(0,0)$ and the inverse of (a,b) is $(-a,-b)$. Lastly, associativity follows from the bilinearity of f:

$$\begin{aligned}((a,b)\times(a',b'))\times(a'',b'') &= (a+a', b+b'+f(a,a'))\times(a'',b'')\\ &= (a+a'+a'', b+b'+f(a,a')+b''+f(a+a',a''))\\ &= (a+a'+a'', b+b'+b''+f(a,a'+a'')+f(a',a''))\\ &= (a,b)\times(a'+a'', b'+b''+f(a',a''))\\ &= (a,b)\times((a',b')\times(a'',b''))\end{aligned}$$

Therefore H as defined in the statement of the theorem is indeed a group. Furthermore, H clearly has exponent p, since both A and B do and $f(a,a) = 0$ by skew-symmetry.

By definition of multiplication, (a,b) and (a',b') commute if and only if $f(a,a') = f(a',a)$. Since $p \neq 2$, skew symmetry of f implies $f(a,a') = 0$. Hence $C_H(a,b) = \ker(f(a,\cdot)) \times B$. If $(a,b) \in Z(H)$, then $\ker(f(a,\cdot)) = A$, so $a = 0$. Hence $Z(H) = 0 \times B$. Now if A is connected and the ambient theory is stable, then since B is generated by the connected groups $f(a,A)$, it must be that B is connected by Proposition 2.3.11. If A and B are connected, then H is connected by Proposition 2.3.9, since $H/Z(H) \cong A$ is connected and $Z(H) \cong B$ is connected. Also $H/Z(H) \cong A$ is abelian, so H has nilpotence class exactly 2.

The desired form of the commutator $[(a,b),(c,d)]$ is easily verified from the skew-symmetry and bilinearity of f. Clearly $Z(H) = H'$ since the image of f generates B and $p \neq 2$. □

The advantage over this vector space construction over the one in Lemma 3.2.2 is that we do preserve the property that centralizers of noncentral elements are abelian by finite. In fact, most of the original group structure is preserved, except that we remove all the elements of the center that are not in the commutator subgroup (and correspondingly trim the noncentral elements of the group). For example, if G were a counterexample produced by Proposition 3.1.6 of exponent p prime and X were a connected infinite $\mathbb{F}_p$-vector space, then $G \times X$ has all the same properties listed in Proposition 3.1.6. But in a very clear way, X is extraneous and only increases the center. We will use the following lemma liberally in Chapter 5 in order to trim the excess central elements and be left with only the commutator.

Lemma 3.2.4 (Trimming Lemma). *Assume $p \neq 2$ prime. Suppose G is a stable, $\aleph_0$-categorical, connected group of nilpotence class 2, so that $G/Z(G)$ is an $\mathbb{F}_p$-vector space. Then we can define a group H and an injection $\iota : G/Z(G) \to H$ with the properties:*

1. *H stable, $\aleph_0$-categorical,*
2. $\exp(H) = p$,
3. *H has nilpotence class 2,*
4. *H is connected,*
5. *H' is connected,*
6. $\iota(G/Z(G)) \cap H' = 0$,
7. $H = \iota(G/Z(G))H'$,
8. $\langle[\iota(G/Z(G)), \iota(G/Z(G)))]\rangle = Z(H) = H'$,
9. *$C_H(\iota(\overline{g})) = \iota(C_G(g)/Z(G))H'$ for any representative $g \in G$ of $\overline{g}$.*
10. *For any $g \in G$, $C_G(g)$ is abelian by finite if and only if $C_H(\iota(\overline{g}))$ is.*

Proof. In Lemma 3.2.3, take $A = G/Z(G)$, $B = G'$, and $f = [\cdot, \cdot] : G/Z(G) \times G/Z(G) \to G'$ and construct our H. The items not involving ι follow immediately from the conclusions of that lemma.

Set $\iota(\overline{g}) = (\overline{g}, 0)$ for all $\overline{g} \in G/Z(G)$. Clearly $\iota(G/Z(G)) \cap H' = 0$, $H = \iota(G/Z(G))H'$, and $\langle[\iota(G/Z(G)), \iota(G/Z(G)))]\rangle = H' = Z(H)$. Lastly,

$$\begin{aligned} C_H(\overline{g}, 0) &= \{(x, y) \mid f(\overline{g}, x) = 0, y \in H'\} \\ &= \{(x, 0) \mid [\overline{g}, x] = 0\}\{(0, y) \mid y \in H'\} \\ &= \iota(C_G(g)/Z(G))H' \end{aligned}$$

for any representative $g \in G$ of $\overline{g}$. If $C_G(g)$ were abelian by finite, then since $\iota(G/Z(G)) \cap H' = 0$, we know $\iota(C_G^0(g)/Z(G))H' = (\iota(C_G(g))H')^0 = C_H^0(\iota(\overline{g}))$ by Proposition 2.3.10. The converse follows from the same line of equalities. □

For any $x \in H \backslash H'$, there is a unique $y \in H'$ such that $xy \in \iota(G/Z(G))$, and we have $C_H(x) = C_H(xy)$. Considering the unique $\overline{g} \in G/Z(G)$ corresponding to xy by ι, we may extend the final item in the above lemma to all of $H \backslash H'$, and thus we know the centralizers of H entirely in terms of the centralizers in G.

Chapter 4

Rings

4.1 Preliminaries and Notation

We adopt the convention that a ring need not have a multiplicative identity, nor will it necessarily be commutative. Rings with identity will be called **unital rings**. Throughout this chapter, **ideal** shall mean two-sided ideal; left and right ideals will be denoted as such. An advantage of our convention on multiplicative identity is that ideals themselves are rings.

Definition 4.1.1. A ring R is:

1. **nil** if for each $x \in R$, there is an integer $n \geq 1$ such that $x^n = 0$.

2. **nilpotent** if there is an integer $n \geq 1$ such that $x_1 \cdots x_n = 0$ for all $x_1, \ldots, x_n \in R$.

3. **null** if $xy = 0$ for all $x, y \in R$.

As with groups, it will be important to have an appropriate notion of connectedness.

Definition 4.1.2. A ring R is **connected** if it contains no proper definable ideals I such that R/I is finite. The **connected component** of R is the intersection of all its definable ideals of finite index.

One easily obtains proofs of propositions analogous to those in Section 2.3, simply by replacing "group" with "ring" and "normal subgroup" with "ideal". In particular, if R is connected and I is a definable ideal, R/I is connected.

Our ring-theoretic definition of connectedness invokes ideals, since they are the natural analogue to normal subgroups for making quotients in the category of rings. However, a ring is also an additive group, so we hope that there is a close connection between the concepts of ring-connectedness and group-connectedness. This is indeed the case under the assumptions of stability and $\aleph_0$-categoricity.

Proposition 4.1.3. *Let R be a stable, $\aleph_0$-categorical ring. Then the connected component R^0 is 0-definable and has finite index in R. Furthermore R is connected as a ring if and only if it is connected as an additive group.*

Proof. We may show that each $\aleph_0$-categorical, stable ring R contains a unique definable connected ideal R^0 of finite index. Analogous to the group theory argument (see Proposition 2.3.14), this is done by using Baldwin-Saxl to intersect families of uniformly definable ideals of finite index, and then using $\aleph_0$-categoricity to show these intersections are 0-definable and finite in number. So the connected component is indeed 0-definable and finite index.

Now suppose R is connected as a ring. Let R_g^0 be the connected component of R considered as an additive group, which is 0-definable and finite index (as a group) by Proposition 2.3.14. Let $a \in R$ be given. Multiplication on the left by a is a group homomorphism, so by Proposition 2.3.8, aR_g^0 is a connected group. Since R_g^0 has finite index in R, $R_g^0 \cap aR_g^0$ has finite index in aR_g^0. By connectedness, $aR_g^0 = R_g^0 \cap aR_g^0$, so $aR_g^0 \leq R_g^0$. Similarly, $R_g^0 a \subseteq R_g^0$, so R_g^0 is an ideal of R, and it must have finite index. Thus $R_g^0 \supseteq R^0$. Yet R^0 is a subgroup of R of finite index, so clearly $R_g^0 = R^0 = R$ and R is connected as a group. The converse follows immediately by noting that every ideal of finite index is an additive group of finite index. □

Remark 4.1.4. The previous proposition implies that for each $r \in R$, if R is connected as a ring then the rings rR and Rr are as well.

As with groups, the connected component in stable, $\aleph_0$-categorical rings strips away the finitary portion of "P by finite" properties:

Proposition 4.1.5. *If R is a stable, $\aleph_0$-categorical ring that is null by finite, and I is a finite index null ideal, then R^0 is null as well.*

Proof. Suppose I is a finite index null ideal; by intersecting with R^0 we may without loss assume it is contained in R^0. Pick any element $x \in I$. Then $xR \supseteq xR^0 \supseteq xI = 0$.

Since multiplication by x is an additive group homomorphism with kernel containing I, we conclude xR^0 is finite. But xR^0 is connected by Proposition 4.1.3, so $xR^0 = 0$. Similarly $R^0x = 0$ and thus $I \subseteq \mathrm{Ann}(R^0)$. Now take $y \in R^0$. Again, multiplication by y is a group homomorphism with I contained in the kernel. Thus yR^0 is finite and therefore equals 0 by connectedness. Since $y \in R^0$ arbitrary, $(R^0)^2 = 0$ and thus R^0 is null. □

4.2 Nilpotent Rings

The main result of this section is a proof of:

Theorem. *A stable, $\aleph_0$-categorical ring is nilpotent by finite.*

This theorem first appeared in a paper by Baldwin and Rose [BR77]. However, in the years surrounding that publication, Felgner [Fel75] had already proved the result with the hypothesis of ω-stability in place of stability, and Cherlin and Reineke [CR76] and Sabbagh [Sab75a] [Sab75b] had observed that Felgner's argument could be extended to stability without too much additional computation. Both Felgner's proof and Baldwin and Rose's proof have at their heart the proof that if R is semisimple (i.e. its Jacobson radical is 0), then R satisfies the descending chain condition (DCC) on all left ideals. They then proceed with ring theoretic structural results to get the final conclusion.

We summarize Baldwin and Rose's argument to indicate where ring theoretic ideas come into play. First Baldwin and Rose show that in any stable ring R, the Jacobson radical $J(R)$ must be nilpotent. In a noncommutative ring without identity, the Jacobson radical is defined as $\{x \in R \mid \forall y \exists z (yx + z + zyx = 0)\}$, which is 0-definable in the language of rings (Lam [Lam01] performs an alternate definition involving intersections of quasi-regular ideals; this turns out to be equivalent). The authors argue that if $J(R)$ is not nilpotent, then by the Compactness Theorem, there are infinitely many $\{c_i\}_{i<\omega}$ in (an elementary extension of) the ring, the product of any number of them being nonzero. Stability assures that increasing products do not form a definable linear order, and then quasi-invertibility of elements of the Jacobson radical finishes the contradiction.

In the second component of Baldwin and Rose's argument, they show that any semisimple stable ring has the full descending chain condition on all left ideals. They follow the proof of Wedderburn's structure theorem for semisimple rings with the full DCC on left ideals [Her68], but using DCC on uniformly definable ideals instead (Wedderburn's proof does not use the full power of the full DCC at any point in the proof). With these arguments, Baldwin and Rose are able to prove that every left ideal is in fact a principal left ideal; from this, stability gives that any semisimple stable ring has the full DCC on left ideals, which (by compactness) is equivalent to having full ACC on left ideals. Using the easy conclusion from $\aleph_0$-categoricity that there are $n > m$ such that $x^n = x^m$ for all $x \in R$, the authors then use a number of ring theoretic characterizations of rings with ACC from [Her68] and [Her69] to conclude that the an $\aleph_0$-categorical stable semisimple ring is finite. Since $J(R)$ is definable and $R/J(R)$ is semisimple, the two components complete the proof.

In contrast, the proof presented below uses far less ring theoretic machinery. We still utilize basic notions such as the Jacobson radical and basic lemmas about rings equal to their Jacobson radical (a real possibility when we do not proscribe a multiplicative identity to our rings). However, our proof generally takes a more model-theoretic approach, by first using the notion of connectedness, and then working to interpreting an infinite field. Such a line of proof was suggested in a private communication by Frank Wagner [Wag06] and we have pursued these ideas to a full argument below.

Theorem 4.2.1. *Let R be a stable, $\aleph_0$-categorical ring. Then R is nilpotent by finite. In particular, R^0 is nilpotent.*

Proof. By $\aleph_0$-categoricity, R contains only finitely many 0-definable sets; in particular it contains only finitely many infinite, connected, 0-definable ideals.

We claim that if R is connected, then R is nilpotent. This shall be proven by induction on the number of 0-definable infinite subsets of R. However, for the base case we shall argue a more general statement: any ring R with no proper infinite 0-definable connected ideals is nilpotent.

Assuming this stronger form of the base case, let us first argue the induction step. If R has no proper, infinite, 0-definable, connected ideals, then R is nilpotent by the base case. Otherwise, let I be a proper, infinite, 0-definable, connected ideal of R. Any 0-definable subset of I must also be an 0-definable subset of R, thus I has strictly fewer 0-definable subsets. By induction, I is nilpotent, say $I^n = 0$. Similarly, R/I is nilpotent as well, say $(R/I)^m = 0$. Thus $R^{nm} = 0$ and R is nilpotent.

Base Case: If R is a connected $\aleph_0$-categorical, stable ring with no proper infinite 0-definable connected ideals, then R is nilpotent.

Proof of Base Case: Assume R is not nilpotent; by connectedness, it must be infinite. Note that if R has a proper infinite 0-definable ideal I, then it has a connected one, I^0; hence R has no proper infinite 0-definable ideals.

The annihilator of R, $\mathrm{Ann}(R) = \{x \mid \forall y \in R\, xy = 0 = yx\}$ is an 0-definable ideal; since R is not nilpotent, it must be proper and hence finite. We may, in fact, assume that $\mathrm{Ann}(R) = 0$. Indeed, $\mathrm{Ann}(R)$, the preimage in R of $\mathrm{Ann}(R/\mathrm{Ann}(R))$, etc. are all 0-definable ideals of R, so after finitely many steps they must stabilize by $\aleph_0$-categoricity. They are also all nilpotent, so quotienting out R by the largest one will not affect our conclusion.

Suppose I is a finite left ideal of R. For each $a \in I$, $Ra \subseteq I$, yet by Remark 4.1.4, Ra is a connected ring. Therefore $Ra = 0$ and $a \in \mathrm{Ann}_r(R)$, the right annihilator of R. Analogously, if I is a finite right ideal of R, then $I \subseteq \mathrm{Ann}_l(R)$, the left annihilator of R. Consequently, any finite two-sided ideal I must be contained in $\mathrm{Ann}_r(R) \cap \mathrm{Ann}_l(R) = \mathrm{Ann}(R) = 0$, so R has no nontrivial finite ideals. In particular, $\mathrm{Ann}_l(R)$ and $\mathrm{Ann}_r(R)$ are both proper 0-definable ideals and thus must be 0.

Exercise 4.4 of Lam [Lam01] gives one way to construct of the Jacobson radical J for noncommutative rings without identity. By this construction, J is an ideal that is fixed by all automorphisms and so by $\aleph_0$-categoricity, J is 0-definable. Hence $J = 0$ or $J = R$.

By stability, we have the chain condition on sets of the form rR for $r \in R$. Let $r \in R$ be such that rR is minimal nonzero (such an r exists since $\mathrm{ann}_l(R) = 0$). By Exercise 4.7 of Lam [Lam01], $J = R$ iff R has no simple left (resp. right) modules. In particular, if $J = R$ then rR is not a simple right R-module, so either $rR \cdot R = 0$ or rR contains a proper nontrivial right R-submodule M. The former is not possible for then $rR \subseteq \mathrm{ann}_l(R) = 0$, and so M exists. In particular, $M \not\subseteq \mathrm{ann}_l(R) = 0$, so $M \cdot R \neq 0$. Thus we may choose $s \in M$ such that $sR \neq 0$; then $sR \subseteq M \subsetneq rR$, a contradiction to the minimality of rR. Hence $J = 0$.

Set $V = \{x \in R \mid \forall y \in R,\, xyx = 0\}$. This an 0-definable set which is closed under multiplication by R on either side. However, it need not be additively closed; thus, let (V) be the ideal generated by V. Note that $0 \in V$ and $x \in V$ iff $-x \in V$, thus (V) is the union of the sets $V + \ldots + V$ as the number of summands goes to infinity. Yet, by $\aleph_0$-categoricity, these 0-definable sets must stabilize in finitely many steps, so $(V) = V + \ldots + V$, the sum of n copies of V. This is a 0-definable ideal, so either $(V) = 0$ or $(V) = R$. Let $x_1, \ldots, x_n \in V$ be given and consider $(x_1 + \ldots + x_n)^{2n+1}$. By Pigeonhole Principle, for each term in the multinomial expansion, there exists a $j \in \{1, \ldots, n\}$ such that x_j appears at least thrice in this term. Thus $x_j y x_j$ appears in this term for some $y \in R$ and so the term is 0. Thus, we have shown that (V) is a nil ideal, which must be contained in J by Exercise 4.4 of Lam [Lam01]. Thus $V = 0$.

Recall that we have chosen an $r \in R$ such that rR is minimal nonzero. Set $A = \mathrm{ann}_l(r) \cap rR$, which is an ideal in rR. Since $r \notin V$, there exists $z \in R$ such that $rzr \neq 0$. Since $\mathrm{ann}_l(R) = 0$, this implies $rzrR \neq 0$. By minimality, $rzrR = rR = rR \cdot rR$ and thus $A \neq rR$. But rR is connected (by Lemma 4.1.3) and nonzero, so the ring $F := rR/A$ is infinite.

Let nonzero $b \in F$ be given and choose a representative $r\tilde{b}$ of b in rR. Since $b \neq 0$, $r\tilde{b} \notin \mathrm{ann}_l(r)$, so $r\tilde{b}r \neq 0$. Since $\mathrm{ann}_l(R) = 0$ and by minimality, $r\tilde{b}rR = rR$. Thus, for every $a, b \in F$, the equation $bX = a$ has a solution in F. For each $b \in F$, let e_b denote a solution to $bX = b$.

Let $b, c \in F$ nonzero such that $bc = 0$. Then $b = r\tilde{b} + A$ and $c = r\tilde{c} + A$ for some $\tilde{b}, \tilde{c} \in R$. Since $bc = 0$, we see that $r\tilde{b}r\tilde{c} \in A$, i.e. $r\tilde{b}r\tilde{c}r = 0$. But since b and c both nonzero, we have $r\tilde{b}rR = rR$ and $r\tilde{c}rR = rR$. Thus $0 = r\tilde{b}r\tilde{c}rR = r\tilde{b}rR = rR$, a contradiction. Thus F has no zero divisors. In particular, for each nonzero $b \in F$ and each $a \in F$, the solution to the equation $bX = a$ is unique.

Let $a, b, x \in F$ nonzero be given. Then $be_b x = bx$ and $ae_a x = ax$, so by cancellation, $e_b x = x = e_a x$, and so $e_a = e_b$. Since $ae_a = a$ for all $a \in F$, we have a two-sided multiplicative identity.

In summary, F is an infinite, stable, $\aleph_0$-categorical domain; stability demands that F is a skew field by Lemma 2.2.1. Yet there are no infinite $\aleph_0$-categorical skew fields by Theorem 2.1, so we have our contradiction. □

4.3 Ring reduction

As with groups, we have a stronger conjecture for $\aleph_0$-categorical stable rings.

Conjecture 4.3.1. If R is an $\aleph_0$-categorical stable ring, then R is null by finite.

This counterexample is also borne from a stronger theorem in ring theory.

Theorem 4.3.2 (Baur, Cherlin, Macintyre [BCM79] with Cherlin, Harrington, Lachlan [CHL85])**.** *A superstable, $\aleph_0$-categorical ring is null by finite.*

This theorem was first proven for ω-stable, $\aleph_0$-categorical rings by BCM. It can be extended to superstable $\aleph_0$-categorical rings on account of Cherlin, Harrington and Lachlan's theorem that an $\aleph_0$-categorical, superstable theory has finite Morley rank.

As with groups, if there is a counterexample to the conjecture, then we also have a specialized counterexample.

Proposition 4.3.3. *If there is an $\aleph_0$-categorical stable ring which is not null by finite, then there is a ring R which is:*

1. *$\aleph_0$-categorical,*
2. *stable,*
3. *connected,*
4. *for all $r_1, r_2, r_3 \in R$ we have $r_1 r_2 r_3 = 0$, and*
5. *there exist $r_1, r_2 \in R$ such that $r_1 r_2 \neq 0$.*

Proof. By Theorem 4.2.1, any connected stable $\aleph_0$-categorical ring R is nilpotent; we may choose a connected R of the least nilpotency class $n > 2$.

We define an increasing collection of ideals A_i inductively as follows: $A_0 = 0$ and A_{i+1} is the preimage in R of $\mathrm{Ann}_l(R/A_i)$. Note that $A_1 \subsetneq R$ since $R^2 \neq 0$. Each A_i is 0-definable, so by $\aleph_0$-categoricity, the A_i stabilize. Let $N > 0$ be the least positive integer such that A_N is maximal but proper. Then R/A_N is a connected, $\aleph_0$-categorical, stable ring. By minimality, the nilpotency class of R/A_N is either n or 2.

We claim that $S = R/A_N$ cannot have nilpotency class n. By the choice of N, either $\mathrm{Ann}_l(S) = S$ or $\mathrm{Ann}_l(S) = 0$. The first option is easily eliminated since $S^2 \neq 0$ because $n > 2$. Because S is nilpotent, it is contained in its Jacobson radical J by Exercise 4.4 of [Lam01]. But by Exercise 4.7 of [Lam01], $S = J$ iff S has no simple right S-modules. In particular, S is not simple, and thus $S \cdot S = 0$ (not possible) or there is a proper, nontrivial right S-module $M_1 \subsetneq S$. Yet $M_1 \cdot S \neq 0$ because $\mathrm{Ann}_l(S) = 0$, so there exists $a_1 \in M_1$ such that $0 \subsetneq a_1 S \subseteq M_1 \subsetneq S$. Proceeding recursively, if we are given $a_k S$, a proper, nontrivial right S-submodule of S, then $a_k S$ cannot be simple, and since $a_k S \cdot S \neq 0$ because $\mathrm{Ann}_l(S) = 0$, we may choose a proper nontrivial right S-submodule M_{k+1} of $a_k S$. Again, $M_{k+1} \cdot S \neq 0$, so we may choose $a_{k+1} \in M_{k+1}$ such that $a_{k+1} S \neq 0$. This induction yields a strictly descending chain $S \supsetneq a_1S \supsetneq a_2S \supsetneq \ldots$, contradiction the chain condition on uniformly definable sets.

Thus, we have shown that $S = R/A_N$ has nilpotency class 2 and thus $R^2 \subseteq A_N$. Since $N > 0$, we may consider the ring R/A_{N-1}. This is a connected, $\aleph_0$-categorical, stable ring. By construction of the A_i, we see that $\mathrm{Ann}_l(R/A_{N-1}) = A_N/A_{N-1}$ and thus $(R/A_{N-1})/\mathrm{Ann}_l(R/A_{N-1}) \cong S$ and has nilpotency class 2. Yet $R^2 \subseteq A_N$, so $(R/A_{N-1})^3 = 0$. By the choice of N, $(R/A_{N-1})^2 \neq 0$. So the ring R/A_{N-1} shows that $n = 3$. □

4.4 Equivalence of conjectures

Conjecture 4.3.1, if true, essentially says that stable, $\aleph_0$-categorical rings are rings in name only. That is to say, potentially excepting a finite extension, the ring has no nontrivial multiplication operation and constitutes no more than an additive abelian group. It is no surprise then, that in the stable, $\aleph_0$-categorical context, groups and rings amount to the same question.

Theorem 4.4.1. *Conjectures 1.1 and 4.3.1 are equivalent.*

Proof. Suppose Conjecture 4.3.1 is false and Conjecture 1.1 is true. We obtain a minimal counterexample ring R by Proposition 4.3.3. Consider the group G whose set is $R \times R$ with the operation $(a, b) \cdot (x, y) = (a + x + ay, b + y)$. We verify that this is a group. The identity is $(0, 0)$ and the inverse of (a, b) is $(ab - a, -b)$. Lastly, associativity follows from the fact that threefold products are zero in R:

$$\begin{aligned}
[(a,b)(c,d)](e,f) &= (a+c+ad, b+d)(e,f) \\
&= (a+c+ad+e+(a+c+ad)f, b+d+f) \\
&= (a+c+e+ad+af+cf, b+d+f) \\
&= (a,b)(c+e+cf, d+f) \\
&= (a,b)[(c,d)(e,f)]
\end{aligned}$$

Note that π_2, the projection of G onto the second coordinate, is a group homomorphism onto $(R, +)$. By Lemma 4.1.3, R is connected as a ring if and only if it is connected as an additive group, so $(R, +)$ is connected. The kernel of π_2 is the subgroup consisting of $(a, 0)$, with $a \in R$, which is again isomorphic to $(R, +)$. Hence G is an extension of a connected group by a connected group. Since G is interpretable in R, we may consider it in light of the theory it inherits from R. In this theory the kernel of π_2 becomes a definable subgroup of G, so by Proposition 2.3.9 G is connected. Furthermore, interpretability gives that G is stable and $\aleph_0$-categorical, so it is abelian. This in turn implies $(a,b)(x,y) = (x,y)(a,b)$, so $a + x + ay = a + x + xb$ and $ay = xb$. Since y, a arbitrary, we can choose them such that $ay = 0$. Then $xb = 0$ for all $b, x \in R$ and so R is null.

For the converse, suppose Conjecture 1.1 is false and Conjecture 4.3.1 is true. We obtain a minimal counterexample group by Proposition 3.1.6, which is a connected, nilpotent class two group G. Write the operations on $Z(G)$ and $G/Z(G)$ additively. Let R be the abelian group $G/Z(G) \times Z(G)$, equipped with the multiplication operation: $(a,x) \otimes (b,y) = (0,[a,b])$. This multiplication is associative (because applying it twice yields 0) and distributes over addition. So by Conjecture 4.3.1, this ring is null by finite. By Proposition 4.1.5, R^0 is null. Set $H = \{g \in G/Z(G) \,|\, \exists x \in Z(G)\,(g,x) \in R^0\}$, which is a definable subgroup since R^0 is a definable subring. Since R/R^0 is a finite group, H has finite index in $G/Z(G)$. By the connectedness of $G/Z(G)$ (see Proposition 2.3.8), $G/Z(G) = H$. Thus for every $a, b \in G/Z(G)$, there are $x, y \in Z(G)$ such that $(a,x), (b,y) \in R^0$ and hence $[a,b] = 0$. $\square$

Chapter 5

Second Analysis of the Groups

5.1 Peaks

In Chapter 3, we reduced to a counterexample of the BCM Conjecture that satisfies Proposition 3.1.6. We also were able to describe two group constructions out of vector spaces in Section 3.2. We now use these in conjunction to gain control over the exponent of our counterexample.

Proposition 5.1.1. *If there is a counterexample to the BCM Conjecture, then for some prime p there is a counterexample G which is:*

1. *stable,*
2. *$\aleph_0$-categorical,*
3. *connected,*
4. *nilpotent of class* 2*,*
5. $\exp(G) = p$ *if p odd,* $\exp(G) = 4$ *if $p = 2$,*
6. *$Z(G) = G'$ if p odd,*
7. *G' is a connected $\mathbb{F}_p$-vector space,*
8. *$G/Z^0(G)$ is a connected $\mathbb{F}_p$-vector space,*
9. *for all $g \in G \backslash Z(G)$, $C(g)$ is abelian by finite.*

Proof. Let G be a counterexample given by Proposition 3.1.6. If p is odd, apply the Trimming Lemma (Lemma 3.2.4) to produce a group H that satisfies all the criteria. If $p = 2$, we apply Lemma 3.2.2 with $A = B = G/Z(G)$, $C = G'$ and $f = [\cdot, \cdot]$ to obtain a counterexample that meets all the conditions, save perhaps the final one. Now use Proposition 3.1.5 on this counterexample to attain the final condition; all the others are preserved by Lemma 3.1.4 and the fact that every group of exponent 2 is abelian. □

In this chapter, it is the last of these properties that our investigations will hinge upon. Throughout this chapter, we will assume the group G has the above properties, unless we utilize Lemma 3.2.2, where the outcome may lack this final property. However, with the condition on centralizers in hand, we may proceed with the following definition.

Definition 5.1.2. A **peak** of G is a maximal connected abelian subgroup of G which properly extends $Z^0(G)$.

It may very well be that G has no peaks, i.e. $Z^0(G)$ is the sole maximal connected abelian subgroup of G. This will be one of the more fruitful possibilities that we will consider.

If P is a peak and $g \in P \backslash Z(G)$, then $C(g) \supseteq P$. Since centralizers of noncentral elements are abelian, $C^0(g)$ is a connected abelian group extending P by Proposition 2.3.7. By maximality, $C^0(g) = P$. So in fact, peaks are the maximal connected centralizer connected components of elements $g \in G \backslash Z(G)$ such that $C^0(g) \neq Z(G)$. Since connected components of a uniformly definable family of groups are once again a uniformly definable family of groups, we know that $\mathcal{P}$, the collection of all peaks, is a uniformly definable family (which may be empty!).

If $a \in P \in \mathcal{P}$ and $g \in G$, then $g^{-1}ag = aa^{-1}g^{-1}ag \in aG' \subseteq P$ and so P is normal. If P_1, P_2 are two distinct peaks and $x \in P_1 \cap P_2$, then $C(x) \supseteq P_1 \cup P_2$. By maximality, this means $C(x) = G$ so that $x \in Z(G)$. Hence the intersection of two distinct peaks is central. This allows us to define an equivalence relation $\sim$ on G:

Definition 5.1.3. The peak equivalence relation $\sim$ is given as follows: $x \sim y$ iff

1. $x, y \in Z(G)$,

2. $x, y \in T_G := \{x \in G \,|\, C^0(x) = Z^0(G)\}$,

3. $x, y \notin Z(G) \cup T_G$ and there is a peak $P \in \mathcal{P}$ such that $C^0(x) \cup C^0(y) \subseteq P$.

There are three possibilities for the equivalence classes of $\sim$: G has no peaks (i.e. $G = Z(G) \cup T_G$), G has one peak, or G has two or more (possibly infinitely many) peaks. Each one poses alternate situations with a different flavor, so we have devoted separate sections to the analysis of each possibility.

5.2 Multiple Peaks

Suppose G has multiple peaks (possibly infinitely many) and choose two distinct ones, say A, B. Since A and B are both connected, we conclude that AB is a connected group by Proposition 2.3.10. Furthermore, AB is not abelian since no noncentral element of A commutes with all of B. Thus AB must be nilpotent of class 2 by Proposition 2.3.15 and $Z(AB) = Z(G) \cap AB \supseteq Z^0(G)$. So we have a connected group, AB, which contains two peaks A and B (of G, but also of AB) whose group product equals the whole group AB. Fixing A, we wish to extend this property to all other peaks of AB.

If C is any peak of G, we may define $\pi_B(C) = \{b \in B \,|\, \exists a \in A, ab \in C\}$, which is a "projection" of $C \cap AB$ into B (it need not be surjective, but the image of an element in $C \cap AB$ is well-defined up to $Z(AB)$-equivalence). Each $\pi_B(C) \supseteq Z^0(G)$ and so we may consider the uniform family of these sets, ranging over $C \in \mathcal{P}$. By Baldwin-Saxl, the groups $\bigcap_{C \in S} \pi_B(C)$, running over all nonempty subsets $S \subseteq \mathcal{P}$, form a uniformly definable family of groups. By the DCC, we may choose a minimal $\bigcap_{C \in S} \pi_B(C)$ that is infinite modulo $Z^0(G)$. This intersection equals the intersection of finitely may $\pi_B(C_i)$ for some $1 \leq i \leq n$. Since $\pi_B(A) = B \cap Z(G)$, we know A is not among the C_i; since $\pi_B(B) = B$, we may without loss assume $B = C_n$. Call the connected component of this intersection $\tilde{B}$ and consider the connected group $A\tilde{B}$. It is connected for the same reasons AB was and the connected component of its center is still $Z^0(G)$.

For any peak $C \in \mathcal{P}$ with $C \neq A$, we have $C \cap A\tilde{B}$ is an abelian subgroup, $\tilde{C}$. In fact, if $\tilde{C}$ is not a finite extension of $Z^0(G)$, then $(\tilde{C})^0$ must be a peak of $A\tilde{B}$. Indeed, if $\tilde{D}$ were a definable connected abelian subgroup of $A\tilde{B}$ properly extending $(\tilde{C})^0$, then we could choose some peak D of G such that $D \supseteq \tilde{D}$. Since $D \cap AB \supseteq \tilde{D}$ but $C \cap A\tilde{B} = \tilde{C} \leq \tilde{D}$, C and D are distinct peaks, so $C \cap D \subseteq Z(G)$. Yet $\tilde{C}$ is in this intersection, a contradiction. Hence, the peaks of $A\tilde{B}$ are precisely $(P \cap A\tilde{B})^0$ for $P \in \mathcal{P}$, provided $(P \cap A\tilde{B})^0 \supsetneq Z^0(A\tilde{B}) = Z^0(G)$.

Return to considering $C \in \mathcal{P}$ with $\tilde{C} = C \cap A\tilde{B}$. Any $c \in \tilde{C}$ is expressible as $c = ab$ for some $a \in A$ and $b \in \tilde{B}$. But then $b \in \pi_B(C)$ by definition, so $\tilde{C} \subseteq A(\pi_B(C) \cap \tilde{B})$.

We know by minimality that $\pi_B(C) \cap \bigcap_{i=1}^n \pi_B(C_i)$ is either finite modulo $Z^0(G)$ or else $\pi_B(C) \supseteq \bigcap_{i=1}^n \pi_B(C_i) \supseteq \tilde{B}$. In the first case, $\pi_B(C) \cap \tilde{B}$ is finite modulo $Z^0(G)$, so $\tilde{C}$ is a subgroup of a finite extension of A; hence $(\tilde{C})^0 \subseteq A$ by Proposition 2.3.7. Since $C \neq A$ by assumption, $C \cap A = Z(G)$ and thus $(\tilde{C})^0 \subseteq Z(G)$, i.e. $(C \cap A\tilde{B})^0$ is not a peak of $A\tilde{B}$.

In the latter case, $\pi_B(C) \supseteq \tilde{B}$, so for every $b \in \tilde{B}$, there is an $a \in A$ such that $ab \in C$. But then $ab \in C \cap AB = \tilde{C}$, so $A\tilde{C} \supseteq A \cup \tilde{B}$ and thus $A\tilde{C} = A\tilde{B}$. Since $A(\tilde{C})^0$ is connected by Proposition 2.3.10 and it has finite index in the connected group $A\tilde{C} = A\tilde{B}$, by the normality of A and the Second Isomorphism Theorem we conclude that $A(\tilde{C})^0 = A\tilde{B}$. So for any arbitrary peak P of $A\tilde{B}$, if $P \neq A$, then $AP = A\tilde{B}$.

Lastly, if $x \in A\tilde{B}$ and $C^0_{A\tilde{B}}(x) \supsetneq Z^0(A\tilde{B})$, we claim $x \in CZ(A\tilde{B})$ for some peak C of $A\tilde{B}$. Indeed, $C^0_{A\tilde{B}}(x) \subseteq C$ for some peak C of $A\tilde{B}$. If $C \neq A$, then since $AC = A\tilde{B}$, we can write x as ac for some $a \in A$, $c \in C$. Assume $a \notin Z(A\tilde{B})$. For any $c' \in C^0_{A\tilde{B}}(x) \subseteq C$, we necessarily have $ac' = c'a$, i.e. $c' \in C_{A\tilde{B}}(a)$. So by Proposition 2.3.7 we have $C^0_{A\tilde{B}}(x) \subseteq C^0_{A\tilde{B}}(a) = A$, contradicting that $C \cap A \subseteq Z(A\tilde{B})$. So $a \in Z(G)$ and $x \in CZ(G)$ for a peak of $A\tilde{B}$. If, on the other hand, $C = A$, i.e. $C^0_{A\tilde{B}}(x) \subseteq A$, then since $x \in A\tilde{B}$ we may write $x = ab$ for some $b \in \tilde{B}$. If $b \notin Z(A\tilde{B})$, then a similar argument shows $C^0_{A\tilde{B}}(x) \subseteq \tilde{B}$, leading to the same contradiction.

We have shown the following:

Theorem 5.2.1. *If there is a counterexample H satisfying Proposition 5.1.1 which has 2 or more peaks, then there is a definable subgroup G of H which has all the properties of Proposition 5.1.1 and moreover:*

- $Z(G) = G \cap Z(H)$
- *G has at least two peaks*
- *there is a peak A of G (called a* **pivot peak***) such that for any other peak B of G, $AB = G$.*
- *for any $x \in G$, if $Z^0(G) \subsetneq C^0(x) \subseteq P$ for some peak P, then $x \in PZ(G)$.*

Proof. The arguments preceding the lemma has shown such a definable connected subgroup G can be obtained satisfying these four conditions. Since G is a subgroup of a group where all centralizers are abelian by finite and $Z(G) = G \cap Z(H)$, the abelian-by-finiteness of centralizers carries over to G as well. All the remaining conditions follow from the fact that G is a subgroup or is connected. □

We now assume G possesses the above properties. Fix our special pivot peak A and let B be any other peak. Since $AB = G$, every element of G can be written uniquely (up to elements of $Z(G)$) as ab for some $a \in A$ and $b \in B$. If C is a third peak of G, then in particular, every noncentral element of C can be written uniquely (up to elements of $Z(G)$) as ab for some noncentral $a \in A$ and noncentral $b \in B$. This gives us homomorphisms between the peaks other than A, which we now describe precisely.

Suppose B and C are peaks of G distinct from A. Then there is a homomorphism $\sigma_{B,C} : B/Z(G) \to C/Z(G)$ given by: for any $\bar{b} \in B/Z(G)$, pick a representative $b \in B$. If $b \notin Z(G)$, choose a noncentral $a \in A$ and a noncentral $c \in C$ such that $b = ac$; if $b \in Z(G)$, then take $a = c = 1$. Set $\sigma_{B,C}(\bar{b}) = \bar{c}$. Since c is unique up to equivalence modulo $A \cap C \subseteq Z(G)$, any other representative of $\bar{b}$ would just differ by an element of $Z(G)$ and so the image $\bar{c}$ is well-defined. That it is a homomorphism follows from the fact that A is normal: if $b = ac$ and $b' = a'c'$, then $bb' = aca'c' = (aca'c^{-1})cc'$, so $\sigma_{B,C}(\overline{bb'}) = cc' = \sigma_{B,C}(\bar{b})\sigma_{B,C}(\bar{c})$. If $c \in C \backslash Z(G)$, then there is some $a \in A$ and $b \in B$, both noncentral, so that $ab = c$. But then $b = a^{-1}c$, so that $\bar{c} = \sigma_{B,C}(\bar{b})$ and $\sigma_{B,C}$ is surjective.

Lemma 5.2.2. *Let G be a counterexample given by Theorem 5.2.1 and let A be a pivot peak, i.e. a peak such that $AB = G$ for any peak $B \neq A$. Then we have a uniformly definable family of isomorphisms $\sigma_{B,C} : B/Z(G) \to C/Z(G)$ for all pairs of peaks B, C distinct from A. Moreover, $\sigma_{B,B}$ is the identity automorphism on $B/Z(G)$ and $\sigma_{C,D} \circ \sigma_{B,C} = \sigma_{B,D}$ for all B, C, D distinct from A, so $\sigma_{C,B}$ is the inverse of $\sigma_{B,C}$.*

Proof. The $\sigma_{B,C}$ are defined preceding the paragraph and verified to be surjective homomorphisms. From the definition it is clear that $\sigma_{B,B}$ is the identity automorphism on $B/Z(G)$. Given B, C, D peaks distinct from A and $\bar{b} \in B/Z(G)$, pick a representative b of $\bar{b}$ in B. Pick $a \in A, c \in C$ such that $b = ac$. Pick $a' \in A, d \in D$ such that $c = a'd$. Then $b = aa'd$, so by definition we have $\sigma_{B,C}(\bar{b}) = \bar{c}$, $\sigma_{C,D}(\bar{c}) = \bar{d}$, and $\sigma_{B,D}(\bar{b}) = \bar{d}$. Hence $\sigma_{C,D} \circ \sigma_{B,C} = \sigma_{B,D}$. Taking $B = D$ and using the fact that $\sigma_{B,B}$ is an automorphism, we conclude that $\sigma_{B,C}$ is injective for any peaks B, C distinct from A. Hence these maps are isomorphisms. □

Lemma 5.2.3. *Let G be a counterexample given by Theorem 5.2.1 and let A be a pivot peak. Let B and C be two (not necessarily distinct) peaks which are distinct from A. Then for all $a \in A$, $b \in B$ and $c \in C$ such that $b = ac$, we have $[a, G] \subseteq [b, G] = [c, G]$. More generally, this is the case when $\sigma_{B,C}(\bar{b}) = (\bar{c})$.*

Proof. If $a \in A$ and $P \neq A$ is a peak, then $G = AP$ so $[a, G] = [a, P]$. For any $b \in P$

$$\begin{aligned} [ab, G] &= \{[ab, a'b'] \mid a' \in A, b' \in P\} \\ &= \{[a, b'] + [b, a'] \mid a' \in A, b' \in P\} \\ &= [a, P] + [b, A] = [a, G] + [b, G] \end{aligned}$$

So if $a \in A$, $b \in B$, $c \in C$ and $b = ac$, then using the fact that $AB = G = AC$ we have

$$[b, A] = [b, G] = [ac, G] = [a, G] + [c, G] = [a, C] + [c, A]$$

so $[c, A] \subseteq [b, A]$ and $[c, G] \subseteq [b, G]$. Symmetrically, since $c = a^{-1}b$, we get $[b, A] \subseteq [c, A]$ and $[b, G] \subseteq [c, G]$. So $[b, A] = [b, G] = [c, G] = [c, A]$ and since $[b, A] = [a, C] + [c, A]$, we get $[a, G] \subseteq [b, G] = [c, G]$. By definition, we have $\sigma_{B,C}(\bar{b}) = \bar{c}$ and for any such $\bar{b}$ and $\bar{c}$, there are representatives b and c of $\bar{b}$ and $\bar{c}$, respectively, and an $a \in A$, such that $b = ac$. □

We now calculate how these peaks arise. Fix our pivot peak A and choose another peak $B \neq A$. Let $x = ab$ for $a \in A \backslash Z(G)$ and $b \in B \backslash Z(G)$, i.e. $x \notin A \cup B$. Given any other element $cd \in AB$ with $c \in A$ and $d \in B$, we have $[x, cd] = [a, d] + [b, c]$. So $cd \in C(x)$ if and only if $[a, d] = [b, c^{-1}]$. Therefore $C(x)$ is infinite modulo $Z(G)$ if and only if $[a, G] \cap [b, G]$ is infinite. In particular, if $C(x)$ is infinite modulo $Z(G)$, then $C^0(x)$ is contained in some peak C which is distinct from A and B. Indeed, if x commuted with infinitely many elements of B distinct modulo $Z(G)$, then a would commute with those same elements, so $C(a) \cap B$ is infinite modulo $Z(G)$. This contradicts that $C^0(a) = A$, whose intersection with B is central. So $C \neq B$ and similarly $C \neq A$.

By Theorem 5.2.1, $x = zc$ for some $c \in C$ and $z \in Z(G)$. Since $c = (z^{-1}a)b$, we may apply Lemma 5.2.3, and see $[a, G] = [za, G] \subseteq [b, G]$. So in summary, $x \in AB \backslash (A \cup B)$ has infinite centralizer modulo $Z(G)$ if and only if $x = ab$ for $a \in A$, $b \in B$ and $[a, G] \subseteq [b, G]$.

5.3 No Peaks

Suppose $G = T_G$, i.e. no noncentral element has an infinite centralizer modulo the center. There is a way to attain a situation similar to the multiple peaks case: apply Lemma 3.2.2 with $A = B = G/Z(G)$, $C = G'$ and f the natural reduction of $[\cdot, \cdot]$ to $G/Z(G) \times G/Z(G) \to G'$. The resulting group would have two abelian subgroups $A \times \{0\} \times C$ and $\{0\} \times B \times C$ whose product is the whole group. However, as noted in Section 5.1, in so doing, we may have lost the guarantee that all other centralizers of noncentral elements are abelian by finite.

Staying with the original no peaks group, let us consider its structure. Note that for any subgroup H of G properly containing $Z(G)$, we have $C_H(h) \subseteq C_G(h)$ for all $h \in H$, so H must have no peaks as well.

Theorem 5.3.1. *There is a definable connected subgroup $Z(G) \leq U \leq G$ which is not abelian and which satisfies the property:*

$$\text{For all } x_1, x_2 \in U,\ [x_1, U] = [x_2, U] \text{ or } [x_1, U] \cap [x_2, U] \text{ is finite.}$$

in addition to all the properties of Proposition 5.1.1. U will also have no peaks.

Proof. Let H be the outcome of using Lemma 3.2.2 with $A = B = G/Z(G)$ and $C = G'$ and $f = [\cdot, \cdot]$. Since H is symmetric in the first two coordinates, we can define a conjugation map $\overline{(x_1, x_2, x_3)} = (x_2, x_1, x_3)$. This map unfortunately is not a homomorphism, however we still have $C_H(\overline{x}) = \overline{C_H(x)}$. The analogous statement holds for centralizer connected components.

An element $x = (x_1, x_2, x_3)$ of H has infinite centralizer modulo $Z(H)$ if and only if there are $y = (y_1, y_2, y_3) \in H$ for infinitely many y_1 and y_2 such that:

$$[x_1, y_2] = [y_1, x_2]$$

Thus if x_1 and x_2 are nontrivial, (x_1, x_2, x_3) has infinite centralizer modulo $Z(H)$ if and only if $[x_1, G] \cap [x_2, G]$ is infinite.

Let $A = G/Z(G) \times 1 \times G'$. Then A is connected and abelian and for any $a \in A$, $C_H^0(a) = A$. For any $x \notin A$, $C_H(x) \cap A$ is finite modulo $Z(H)$.

Consider the collection of all products $AC_H^0(x)$ for $x \notin A$ with $C_H^0(x)$ infinite modulo $Z(H)$. There is at least one such product, namely $A\overline{A}$. By Baldwin-Saxl and DCC, we may choose a minimal intersection of the $AC_H^0(x)$ which is not abelian by finite; label its connected component as I.

Since A connected, we know by Proposition 2.3.7 that $A \subseteq I$. So given any $(x_1, x_2, x_3) \in I$ and any $y \in G'$, we have

$$(1, x_2, y) = (x_1^{-1}, 1, x_3^{-1}y)(x_1, x_2, x_3) \in I$$

so that I has underlying set $G/Z(G) \times U/Z(G) \times G'$ for some subgroup $U \leq G$. Because I is an infinite extension of A, it must be that $U/Z(G)$ is infinite. Since projection onto the second coordinate is a homomorphism, $\pi_2(I) = U/Z(G)$ is connected by Proposition 2.3.8. U cannot be abelian by finite since G has no peaks and U infinitely extends $Z(G)$. In fact, since U is infinite modulo $Z(G)$ and centralizers are abelian by finite in G, we know $Z(U) = Z(H)$. One consequence of this is that $Z(I) = 1 \times 1 \times G' = Z(H)$.

Let $U' = \langle [U, U] \rangle$ and consider $J = U/Z(G) \times U/Z(G) \times U'$. By Lemma 3.2.2, J is a connected subgroup of I which is not abelian (by finite) and has $Z(J) = 1 \times 1 \times U'$. Let nontrivial $x_1, x_2 \in U/Z(G)$ be given and set $x = (x_1, x_2, 1)$. Since $Z(U) = Z(G)$, the same argument as before gives us that $C^0_J(x)$ is infinite modulo $Z(J)$ iff $[x_1, U] \cap [x_2, U]$ is infinite. Let us assume $C^0_J(x)$ is indeed infinite modulo $Z(J)$. Then $C^0_I(x)$ is infinite modulo $Z(I) = Z(H)$ as well, so by the minimality of I, we must have $AC^0_H(x) \supseteq I$. But since $A \subseteq I$, we must have $I = A(C^0_H(x) \cap I) \subseteq AC_I(x)$. By connectedness (via Proposition 2.3.10), $AC^0_I(x) = I$. Thus $\pi_2(C^0_I(x)) = U/Z(G)$.

On the other hand, if $C^0_J(x)$ is infinite modulo $Z(J)$, then by symmetry so is $C^0_J(\overline{x})$. By the argument above, $AC^0_I(\overline{x}) = I$ and thus $U/Z(G) = \pi_2(C^0_I(\overline{x})) = \pi_1(C^0_I(x))$. Thus $C^0_I(x) \subseteq U/Z(G) \times U/Z(G) \times G'$ and $C^0_I(x) = Z(I)C^0_J(x)$. This gives us that $I = AC^0_I(x) = AZ(I)C^0_J(x) = AC^0_J(x)$. Letting $A_J = A \cap J = U/Z(G) \times 1 \times U'$, we see by intersection that $J = A_J C^0_J(x)$. Analogously $J = A_J C^0_J(\overline{x})$.

These conditions combine to give us $\pi_1(C^0_J(x)) = \pi_2(C^0_J(x)) = U/Z(G)$. Thus, for every $u \in U/Z(G)$, there exists a $v \in U/Z(G)$ such that $(u, v, 1) \in C^0_J(x)$, i.e. so that $[x_1, u][x_2, v] = 1$. So $[x_1, U] \subseteq [x_2, U]$. Conversely, we have for every $u \in U$ the existence of $v \in U$ such that $(v, u, 1) \in C^0_J(x)$, which gives $[x_2, U] \subseteq [x_1, U]$ and thus the images are equal.

Thus we have shown that U is a definable subgroup of G which is not abelian by finite such that for every $x_1, x_2 \in U$, $[x_1, U] \cap [x_2, U]$ is either finite or equal. If $p \neq 2$ then $Z(G) = G'$ is connected and $U/Z(G)$ is connected, so by Proposition 2.3.9, U is connected. If $p = 2$, then if $[x_1, U^0] \cap [x_2, U^0]$ is infinite, then $[x_1, U] = [x_2, U]$. Since $[x_1, U^0]$ and $[x_2, U]$ are connected subgroups of finite index by Proposition 2.3.8, it must be that $[x_1, U^0] = [x_2, U^0]$. So U^0 is our connected definable subgroup with the desired property. In either case, once we have this connected definable subgroup (call it U), we clearly see it has no peaks, since any peak of U would be contained in a peak of G. All the remaining properties are inherited immediately, except that $Z(U) = Z(G) = G'$, which is not necessarily U'. A simple application of the Trimming Lemma when $p \neq 2$ takes care of this final concern and does not disrupt any of the other properties. $\square$

5.4 One Peak

Suppose there is exactly one peak P. There is a way to attain a situation similar to the multiple peaks case: apply Lemma 3.2.2 with $A = G/P$, $B = P$, $C = G'$ and f the natural reduction of $[\cdot, \cdot]$ to $G/P \times P \to G'$. The resulting group would have two abelian subgroups $A \times \{0\} \times C$ and $\{0\} \times B \times C$ whose product is the whole group. However, as noted in Section 5.1, in so doing, we may have lost that all other centralizers of noncentral elements are abelian by finite.

Chapter 6

Quasiendomorphism Rings

6.1 Endomorphism and Quasiendomorphism Rings

For ease of definition, we shall identify functions with their graphs and have our groups be additive. Unless otherwise mentioned (such as in the examples), we shall assume our groups to be abelian in this chapter.

Definition 6.1.1. Let G be an additive abelian group.
An **additive relation** of G is a subset $\sigma \subseteq G \times G$ such that

1. σ is a subgroup

2. the projection, $\pi_1(\sigma)$, of σ onto the first coordinate equals G

A **quasiendomorphism** of G is an additive relation which furthermore satisfies:

3. for all $x \in G$, $\sigma(x) := \{y \in G \mid (x, y) \in \sigma\}$ is finite.

An **endomorphism** of G is a quasiendomorphism which is a function.

The definition of quasiendomorphism varies in the literature, depending on convenience. The present exposition builds upon the exposition in Baur-Cherlin-Macintyre [BCM79], but our definitions differ. For example, BCM's definition of "additive relation" is more general than our definition, which coincides with their definition of "quasiendomorphism". The shift in definitions causes our definition of "quasiendomorphism" to be more restrictive as well. In order to avoid any confusion, we proceed in full detail with self-contained proofs of some of the basic lemmas in that paper.

Quasiendomorphisms have been used as a tool in several other papers, which have varied treatments as well. Wagner [Wag97, Ch. 4.4] uses a generalized version of quasiendomorphisms in order to study stable groups. Quasiendomorphisms also appear in the proof of Theorem 1.14 in Poizat [Poi01], for example. The general idea behind using quasiendomorphism rings is to create a rich algebraic object out of definable relations on our structure that approximate invertible maps. Then, using model theoretic methods, one hopes to derive an infinite field from this object or conclude, contrary to expectations, that the quasiendomorphism ring is finite. Section 6.3 illustrates this philosophy in application.

From the definitions, it follows that if σ is an additive relation, then $\sigma(0)$ is a group. In the case that σ is a quasiendomorphism, then $\sigma(0)$ is finite. As the next two propositions show, the converse is true as well and $\sigma(0)$ captures how additive relations lie within each other.

Lemma 6.1.2. *If σ is an additive relation on G and $(x, y) \in \sigma$, then $\sigma(x) = y + \sigma(0)$. Hence σ is a quasiendomorphism if and only if $\sigma(0)$ is finite.*

Proof. If $y, y' \in \sigma(x)$, then since σ a group, $(0, y - y') \in \sigma$, so $y \equiv y' \mod \sigma(0)$. By definition, σ is a quasiendomorphism if and only if $\sigma(x)$ is finite for all $x \in G$. The equivalence follows immediately. □

Lemma 6.1.3. *Suppose $\sigma \subseteq \tau$ are additive relations on G. Then $\tau = \sigma + (\{0\} \times \tau(0))$ (where $+$ denotes group addition). Furthermore, $[\tau : \sigma] = [\tau(0) : \sigma(0)]$, so if $\sigma(0)$ has finite index in $\tau(0)$, then σ has finite index in τ. In particular, if τ is a quasiendomorphism, then σ has finite index in τ.*

Proof. For any $(g, h) \in \tau$, there is some x such that $(g, x) \in \sigma \subseteq \tau$. Then $(g, h) - (g, x) = (0, h - x) \in \tau$ so $h - x \in \tau(0)$. Hence $\tau = \sigma + (\{0\} \times \tau(0))$. By the Second Isomorphism Theorem, $\tau/\sigma \cong (\{0\} \times \tau(0))/(\{0\} \times \sigma(0)) \cong \tau(0)/\sigma(0)$. If $\sigma(0)$ has finite index in $\tau(0)$, then the right hand side is a finite group; such is the case if τ is a quasiendomorphism since $\tau(0)$ is finite by definition. □

Given an additive relation σ on G and a subgroup A of G, we may define the restriction of σ to A, denoted $\sigma\,|_A$, as:

$$\sigma\,|_A := \{(a, a') \in A \times A \,|\, (a, a') \in \sigma\}.$$

This differs from the usual relation restriction in that we are restricting the codomain as well. With that consideration, we note that the group $\sigma\mid_A$ is an additive relation if and only if for every $a \in A$ there is an $a' \in A$ such that $(a, a') \in \sigma$. If σ was a (quasi)-endomorphism and $\sigma\mid_A$ is an additive relation, then it must in particular be an (quasi)-endomorphism.

If A is a (necessarily) normal subgroup of G of finite index n, then $\sigma\mid_A$ is a finite index subgroup of σ of index dividing n^2. Indeed, $A \times A$ has index n^2 in $G \times G$ and $\sigma\mid_A = \sigma \cap A \times A$, so we have our bound by the Second Isomorphism Theorem.

Given two additive relations σ_1 and σ_2 on G, we can define three algebraic operations, negation, addition and multiplication, on σ_1 and σ_2 to produce additive relations. When applied to (quasi)-endomorphisms, these operations yield (quasi)-endomorphisms. To avoid confusion with Cartesian products of additive relations, we will use $*$ to denote multiplication.

Definition 6.1.4. Given two additive relations σ_1 and σ_2 on G, set

$$\begin{aligned} -\sigma_1 &:= \{(x, -y) \in G \times G \mid (x, y) \in \sigma_1\} \\ \sigma_1 + \sigma_2 &:= \{(x, y) \in G \times G \mid \exists u, w \in G,\ y = u + w,\ (x, u) \in \sigma_1,\ (x, w) \in \sigma_2\} \\ \sigma_1 * \sigma_2 &:= \{(x, y) \in G \times G \mid \exists z \in G,\ (x, z) \in \sigma_2,\ (z, y) \in \sigma_1\} \end{aligned}$$

In other words, $-$ corresponds to inverting the second coordinate, $+$ corresponds to function addition, and $*$ corresponds to composition. It is easy to verify that the sets defined above are additive relations (resp. (quasi)-endomorphisms) if σ_1 and σ_2 are. As shorthand, we write $\sigma - \tau$ in place of $\sigma + (-\tau)$. As one would expect, many natural ring properties hold. However, there are a few ring properties which will require more assumptions to guarantee.

Proposition 6.1.5. *The operations $-$, $+$, and $*$ have the following algebraic properties on additive relations on G:*

- *$+$ and $*$ are associative.*
- *$0 = G \times \{0\}$ is an additive identity.*
- *$1 := \{(g, g) \mid g \in G\}$, the identity automorphism of G, is a multiplicative identity.*
- *$-$ is an involutory operator.*
- *$-$ distributes over $+$.*

- *for all* σ, τ, $-(\sigma * \tau) = (-\sigma) * \tau = \sigma * (-\tau)$
- *for all* σ, $\sigma - \sigma = G \times \sigma(0)$
- $+$ *is commutative*
- *for all* σ, $0 * \sigma = 0$ *but* $\sigma * 0 = G \times \sigma(0)$.
- *for all* $\sigma_1, \sigma_2, \sigma_3$ *additive relations on* G,

$$\sigma_1 * (\sigma_2 + \sigma_3) = \sigma_1 * \sigma_2 + \sigma_1 * \sigma_3$$

but

$$(\sigma_1 + \sigma_2) * \sigma_3 \subseteq \sigma_1 * \sigma_3 + \sigma_2 * \sigma_3$$

The index is bounded above by $|\sigma_3(0)|$, *so if* σ_3 *is a quasiendomorphism, then* $(\sigma_1 + \sigma_2) * \sigma_3$ *has finite index in* $\sigma_1 * \sigma_3 + \sigma_2 * \sigma_3$. *If* σ_3 *is an endomorphism, they are equal.*

Proof. Most of these properties follow immediately from the definitions, or the corresponding properties of G, or general facts such as associativity of the composition of relations. However, we have provided arguments for claims that require more care.

We shall show distributivity on the left:

$$\begin{aligned}
\sigma_1 * (\sigma_2 + \sigma_3) &= \{(g, g') \,|\, \exists h\, (g, h) \in (\sigma_2 + \sigma_3),\, (h, g') \in \sigma_1\} \\
&= \{(g, g') \,|\, \exists h_1, h_2,\ (g, h_1) \in \sigma_2,\, (g, h_2) \in \sigma_3,\, (h_1 + h_2, g') \in \sigma_1\} \\
&= \{(g, g') \,|\, \exists h_1, h_2, h_3\ (g, h_1) \in \sigma_2,\, (g, h_2) \in \sigma_3, \\
&\qquad\qquad (h_1, h_3) \in \sigma_1, (h_2, g' - h_3) \in \sigma_1\} \\
&= \{(g, g') \,|\, \exists h_2, h_3\ (g, h_3) \in \sigma_1 * \sigma_2,\, (g, h_2) \in \sigma_3,\, (h_2, g' - h_3) \in \sigma_1\} \\
&= \{(g, g') \,|\, \exists h_3\ (g, h_3) \in \sigma_1 * \sigma_2,\, (g, g' - h_3) \in \sigma_1 * \sigma_3\} \\
&= \sigma_1 * \sigma_2 + \sigma_1 * \sigma_3
\end{aligned}$$

Near distributivity on the right:

$$\begin{aligned}
(\sigma_1 + \sigma_2) * \sigma_3 &= \{(g, g') \,|\, \exists h_1\, (g, h_1) \in \sigma_3,\, (h_1, g') \in (\sigma_1 + \sigma_2)\} \\
&= \{(g, g') \,|\, \exists h_1, h_2\, (g, h_1) \in \sigma_3,\, (h_1, h_2) \in \sigma_1,\, (h_1, g' - h_2) \in \sigma_2\} \\
&\subseteq \{(g, g') \,|\, \exists h_2\, (g, h_2) \in \sigma_1 * \sigma_3,\, (g, g' - h_2) \in \sigma_2 * \sigma_3\} \\
&= \sigma_1 * \sigma_3 + \sigma_2 * \sigma_3
\end{aligned}$$

By Lemma 6.1.3, the index of $(\sigma_1 + \sigma_2) * \sigma_3$ in $\sigma_1 * \sigma_3 + \sigma_2 * \sigma_3$ equals the index of $((\sigma_1 + \sigma_2) * \sigma_3)(0)$ in $(\sigma_1 * \sigma_3 + \sigma_2 * \sigma_3)(0) = (\sigma_1 * \sigma_3)(0) + (\sigma_2 * \sigma_3)(0)$. We wish to bound this index.

Suppose we are given $g_1 \in (\sigma_1 * \sigma_3)(0)$ and $g_2 \in (\sigma_2 * \sigma_3)(0)$ and we find $h, h' \in \sigma_3(0)$ such that

$$(h, g_1) \in \sigma_1 \qquad\qquad (h', g_2) \in \sigma_2$$

If $z \in \sigma_3(0)$ and $g_1' \in (\sigma_1 * \sigma_3)(0)$ and $g_2' \in (\sigma_2 * \sigma_3)(0)$ such that

$$(h - z, g_1') \in \sigma_1 \qquad\qquad (h' - z, g_2') \in \sigma_2$$

Then $(z, g_1 - g_1') \in \sigma_1$ and $(z, g_2 - g_2') \in \sigma_2$, so $(z, g_1 - g_1' + g_2 - g_2') \in \sigma_1 + \sigma_2$. Since $z \in \sigma_3(0)$, $g_1 - g_1' + g_2 - g_2' \in ((\sigma_1 + \sigma_2) * \sigma_3)(0)$ and the elements $g_1 + g_2$ and $g_1' + g_2'$ of $(\sigma_1 * \sigma_3 + \sigma_2 * \sigma_3)(0)$ are equivalent modulo $((\sigma_1 + \sigma_2) * \sigma_3)(0)$. Therefore the number of distinct classes of $(\sigma_1 * \sigma_3 + \sigma_2 * \sigma_3)(0)$ modulo $((\sigma_1 + \sigma_2) * \sigma_3)(0)$ is bounded above by the number of pairs of elements $\sigma_3(0)$ distinct up to translation by the same element of $\sigma_3(0)$. This value is clearly equal to $|\sigma_3(0)|$.

We now show that $-$ commutes with $*$. By definition:

$$\begin{aligned} -(\sigma * \tau) &= \{(g, -g') \,|\, (g, g') \in \sigma * \tau\} \\ &= \{(g, -g') \,|\, \exists h\, (g, h) \in \tau,\, (h, g') \in \sigma\} \\ &= \{(g, -g') \,|\, \exists h\, (g, h) \in \tau,\, (h, -g') \in -\sigma\} \\ &= (-\sigma) * \tau \end{aligned}$$

On the other hand, if $(h, g') \in \sigma$, then by Lemma 6.1.2 and the fact that σ is a group, we know $(-h, -g') \in \sigma$ as well. So we alternately derive:

$$\begin{aligned} -(\sigma * \tau) &= \{(g, -g') \,|\, (g, g') \in \sigma * \tau\} \\ &= \{(g, -g') \,|\, \exists h\, (g, h) \in \tau,\, (h, g') \in \sigma\} \\ &= \{(g, -g') \,|\, \exists h\, (g, -h) \in -\tau,\, (h, g') \in \sigma\} \\ &= \{(g, -g') \,|\, \exists h\, (g, -h) \in -\tau,\, (-h, -g') \in \sigma\} \\ &= \sigma * (-\tau) \end{aligned}$$

Lastly, we show that $\sigma - \sigma = G \times \sigma(0)$. For this we use Lemma 6.1.2: if $\sigma(x) = y + \sigma(0)$, then $(-\sigma)(x) = -y - \sigma(0) = -y + \sigma(0)$. Hence $(\sigma - \sigma)(x) = \sigma(0)$ and thus $\sigma - \sigma = G \times \sigma(0)$, which is an additive relation extending 0. □

Even though we are missing a few ring properties (such as: the distributivity of multiplication on the right over addition; additive inverses; multiplication by 0 on the right producing 0), we shall work to a situation where these properties will hold and we have a genuine ring. Since our eventual goal is to produce rings, we would like to pay special attention to algebraic structures closed under $-$, $+$ and $*$. In light of the properties listed in Proposition 6.1.5, any such algebraic structure must be a near semiring. For the reader not abreast of the nomenclature of algebraic structures with few axioms, we remind them of the definition now.

Definition 6.1.6. A **near semiring** is a set S equipped with two binary operations $+$ and $*$ satisfying:

- $(S, +)$ is a semigroup with identity 0.
- $(S, *)$ is a semigroup
- $a * (b + c) = a * b + a * c$ for all $a, b, c \in S$
- $0 * a = 0$ for all $a \in S$

This definition can be equivalently stated with $*$ being right distributive and 0 being right absorptive.

In the context of additive relations on G, we have a third operation $-$, which approximates the notion of additive inverse. Since near semirings do not need to be closed under $-$ (or even have an operator like $-$), we give such near semirings of additive relations special status.

Definition 6.1.7. A near semiring R of additive relations on G is called **symmetric** if $-r \in R$ whenever $r \in R$.

A simple example of a symmetric near semiring of additive relations on G is $\mathrm{Mor}(G)$, the near semiring of all additive relations on G. $\mathrm{Mor}(G)$ is simply the near semiring structure present on the family of all subgroups of $G \times G$ which project surjectively onto the first coordinate; this near semiring is clearly closed under $-$.

Now that we have at our disposal $-$, $+$ and $*$, three algebraic operations on additive relations, we would like to consider closures of sets under such operations.

Definition 6.1.8. Given a set H of additive relations on G, we define the **symmetric near semiring of additive relations** on H, denoted $E[H]$, to be the intersection of all symmetric sub-near-semirings R of $\mathrm{Mor}(G)$ which contain H. We define the **symmetric near semiring of quasiendomorphisms** and the **symmetric near semiring of endomorphisms** analogously, replacing "additive relation" with "(quasi)-endomorphism" throughout the definition.

Remark 6.1.9. Recall that we do not require near semirings to have multiplicative identity, so the definition of $E[H]$ does not necessitate that 1 be a member. However, should we want to ensure that our symmetric near semiring of additive relations has a multiplicative identity, we may always include 1 in our seed set H.

As we shall see, $E[H]$ can be built recursively from below. Given a set H of additive relations on G, we define a near semiring of morphisms recursively as follows:

1. Set $H_0 = H \cup \{0\}$.
2. Given H_i, set

$$H_{i+1} = \{\sigma_1 - \sigma_2 \,|\, \sigma_1, \sigma_2 \in H_i\} \cup \{\sigma_1 * \sigma_2 \,|\, \sigma_1, \sigma_2 \in H_i\}$$

Proposition 6.1.10. *Given a set H of additive relations on G, we define the H_i as above. Then $E[H] = \bigcup_{i<\omega} H_i$.*

Proof. Since any $r, s \in \bigcup_{i<\omega} H_i$ belongs to some H_i, then $(0 - r) = -r \in H_{i+1}$ and $s - (-r) = s + r \in H_{i+2}$, so we see that $\bigcup_{i<\omega} H_i$ is symmetric and closed under $+$. Hence $\bigcup_{i<\omega} H_i$ is clearly a symmetric near semiring since it is also closed under $*$ and it contains the additive identity 0, which is left absorptive by Proposition 6.1.5. By definition, $E[H]$ must be a sub-near-semiring, but the reverse inclusion is clear. □

If G is $\aleph_0$-categorical and stable and an additive relation σ is definable, then we may take its connected component σ^0, which will have finite index in σ. Note that both $\pi_1(\sigma^0)$ and $\pi_2(\sigma^0)$ are definable, connected (by Proposition 2.3.8) subgroups of G, so they are contained in G^0 (by Proposition 2.3.7). Furthermore, $\pi_1(\sigma^0)$ has finite index in $\pi_1(\sigma) = G$, so $\pi_1(\sigma^0) = G^0$. Thus σ^0 is an additive relation on G^0, and if σ was a (quasi)-endomorphism, then σ^0 will be too. From earlier discussions it follows that since G^0 has finite index in G, then $\sigma\restriction_{G^0}$ has finite index in σ, and thus $\sigma^0 = (\sigma\restriction_{G^0})^0$. Also, if σ was an endomorphism, then necessarily $\sigma^0 = \sigma\restriction_{G^0}$.

By Lemma 6.1.3, we know $[\sigma\restriction_{G^0}: \sigma^0] = [\sigma\restriction_{G^0}(0) : \sigma^0(0)]$. However, we can push this result up to σ.

Lemma 6.1.11. *Let σ be an additive relation on G. Suppose G^0 and σ^0 are finite index in their respective groups. Then $[\sigma : \sigma^0] = [G : G^0][\sigma(0) : \sigma^0(0)]$.*

Proof. We know $[\sigma : \sigma^0] = [\sigma : \sigma\restriction_{G^0}][\sigma\restriction_{G^0}: \sigma^0]$, and that $[\sigma\restriction_{G^0}: \sigma^0] = [\sigma\restriction_{G^0}(0) : \sigma^0(0)]$. The Second Isomorphism Theorem gives us that $[\sigma\restriction_{G^0} +(\{0\} \times \sigma(0)) : \sigma\restriction_{G^0}] = [\sigma(0) : \sigma\restriction_{G^0}(0)]$. Combined, they yield:

$$[\sigma : \sigma^0] = [\sigma : \sigma\restriction_{G^0} +(\{0\} \times \sigma(0))][\sigma(0) : \sigma^0(0)]$$

It remains to show that $[\sigma : \sigma\restriction_{G^0} +(\{0\} \times \sigma(0))] = [G : G^0]$. Since $\pi_1(\sigma) = G$, we know $(G^0 \times G) + \sigma = G \times G$. On the other hand, $\sigma \cap (G^0 \times G) = \sigma\restriction_{G^0} +(\{0\} \times \sigma(0))$. Indeed, if $(g, h) \in \sigma \cap (G^0 \times G)$, then there is a $(g, h') \in \sigma\restriction_{G^0}$ for some $h' \in G^0$. But then $(0, h - h') \in \sigma(0)$, so we obtain the desired equality of groups. Now a final application of the Second Isomorphism theorem gives us that $[\sigma : \sigma_{G^0} + (\{0\} \times \sigma(0))] = [G : G^0]$. □

When our additive relations are definable and we are in a context where connected components have finite index (e.g. in a stable, $\aleph_0$-categorical context), then we have an alternate choice for creating a symmetric near semiring out of a set of additive relations. Given H, a set of additive relations, we perform the same recursive construction as for $E[H]$, except we take connected components at each stage. Specifically:

1. Set $H^*_0 = \{0^0\} \cup \{\sigma^0 \mid \sigma \in H\}$.

2. Given H^*_i, set

$$H^*_{i+1} = \{(\sigma_1 - \sigma_2)^0 \mid \sigma_1, \sigma_2 \in H^*_i\} \cup \{(\sigma_1 * \sigma_2)^0 \mid \sigma_1, \sigma_2 \in H^*_i\}$$

3. $E^0[H] = \bigcup_{i<\omega} H^*_i$.

With the following set of lemmas, we will verify that $E^0[H]$ is indeed a symmetric near semiring, albeit with slightly different algebraic operations. We will establish several properties of $E^0[H]$, and relate it to $E[H]$.

Lemma 6.1.12. *Suppose connected components have finite index. If σ is an additive relation on G, then $-(\sigma^0) = (-\sigma)^0$. Furthermore, if σ is a quasiendomorphism, $(\sigma - \sigma)^0 = 0^0$.*

Proof. Clearly since $\sigma^0 \subseteq \sigma$, we have $-(\sigma^0) \subseteq -\sigma$. If $(x, y), (x', y') \in \sigma$ are equivalent modulo σ^0, then $(x - x', y - y') \in \sigma^0$. But then $(x, -y), (x', -y') \in -\sigma$ and $(x - x', -y - (-y')) \in -(\sigma^0)$ so $[-\sigma : -(\sigma^0)]$ is bounded above by $[\sigma : \sigma^0]$ and $(-\sigma)^0 = (-(\sigma^0))^0$. Conversely, if $(x, y), (x', y') \in -\sigma$ are equivalent modulo $-(\sigma^0)$ then $(x-x', y-y') \in -(\sigma^0)$. But then $(x, -y), (x', -y') \in -(-\sigma) = \sigma$ and $(x - x', -y - (-y')) \in -(-(\sigma^0)) = \sigma^0$. So $[\sigma : \sigma^0]$ is bounded above by $[-\sigma : -(\sigma^0)]$, and thus $[\sigma : \sigma^0] = [-\sigma : -(\sigma^0)]$. Substitute $-\sigma$ for σ in this formula, and we obtain

$$[-\sigma : (-\sigma)^0] = [\sigma : -((-\sigma)^0)]$$

Hence $-((-\sigma)^0)$ is a definable subgroup of finite index in σ; this implies $-((-\sigma)^0) \supseteq \sigma^0$ and thus $(-\sigma)^0 \supseteq -(\sigma^0)$. Yet we knew that $(-\sigma)^0 = (-(\sigma^0))^0$, so $(-\sigma)^0 = -(\sigma^0)$.

The statement about quasiendomorphisms follows by Proposition 6.1.5: since $\sigma - \sigma = G \times \sigma(0)$ and $\sigma(0)$ is finite for quasiendomorphisms, the connected component of $G \times \sigma(0)$ is $G^0 \times \{0\} = 0^0$ (using Proposition 2.3.10). □

Lemma 6.1.13. *Suppose connected components have finite index. If σ and τ are two additive relations on G, then*

$$(\sigma + \tau)^0 = (\sigma^0 + \tau^0)^0$$

Proof. Since $\sigma \supseteq \sigma^0$ and $\tau \supseteq \tau^0$, we easily see from the definition of $+$ that $\sigma + \tau \supseteq \sigma^0 + \tau^0$ as groups in $G \times G$. By Proposition 2.3.7, this means $(\sigma + \tau)^0 \supseteq (\sigma^0 + \tau^0)^0$. Both of these are additive relations on G^0, so by Lemma 6.1.3 we know that

$$[(\sigma + \tau)^0 : (\sigma^0 + \tau^0)^0] = [(\sigma + \tau)^0(0) : (\sigma^0 + \tau^0)^0(0)]$$

If we show this index is finite, then by connectedness $(\sigma + \tau)^0$ equals $(\sigma^0 + \tau^0)^0$.

We know by Lemma 6.1.11 that $(\sigma + \tau)^0(0)$ has finite index in $(\sigma + \tau)(0)$. Yet from the definition of $+$ on morphisms, it is clear that $(\sigma + \tau)(0)$ is the sum of groups $\sigma(0)$ and $\tau(0)$. Since $\sigma^0(0)$ and $\tau^0(0)$ have finite index in $\sigma(0)$ and $\tau(0)$, respectively, by Lemma 6.1.11 it must be that $(\sigma^0 + \tau^0)(0) = \sigma^0(0) + \tau^0(0)$ has finite index in $(\sigma + \tau)(0)$. Again by Lemma 6.1.11, $(\sigma^0 + \tau^0)^0(0)$ has finite index in $(\sigma^0 + \tau^0)(0)$. Since $(\sigma + \tau)^0(0)$ contains $(\sigma^0 + \tau^0)^0(0)$, the latter has finite index in the former, which is precisely the result sought to finish the proof. □

Lemma 6.1.14. *Suppose connected components have finite index. If σ and τ are two additive relations on G, then*

$$(\sigma * \tau)^0 = (\sigma^0 * \tau^0)^0$$

Proof. Since $\sigma \supseteq \sigma^0$ and $\tau \supseteq \tau^0$, we easily see from the definition of $*$ that $\sigma * \tau \supseteq \sigma^0 * \tau^0$ as groups in $G \times G$. By Proposition 2.3.7, this means $(\sigma * \tau)^0 \supseteq (\sigma^0 * \tau^0)^0$. Both of these are additive relations on G^0, so by Lemma 6.1.3 we know that

$$[(\sigma * \tau)^0 : (\sigma^0 * \tau^0)^0] = [(\sigma * \tau)^0(0) : (\sigma^0 * \tau^0)^0(0)]$$

If we can show the index on the right is finite, then by connectedness, $(\sigma * \tau)^0$ and $(\sigma^0 * \tau^0)^0$ must be equal.

Consider $(\sigma * \tau)(0) = \{g \in G \,|\, \exists h \in \tau(0),\, (h, g) \in \sigma\}$ and set

$$T := \{x \in G \,|\, \exists y \in \tau^0(0),\, (y, x) \in \sigma\}$$

Since σ and $\tau^0(0)$ are groups, it is clear that T is a group as well. Moreover, $(\sigma * \tau)(0) \supseteq T \supseteq (\sigma^0 * \tau^0)(0)$. On the one hand, if two elements $g, g' \in (\sigma * \tau)(0)$ have corresponding $h, h' \in \tau(0)$ with $h \equiv h' \mod \tau^0(0)$ and $(h, g), (h', g') \in \sigma$, then $h - h' \in \tau^0(0)$ and $(h - h', g - g') \in \sigma$. So $g - g' \in T$ and thus $[(\sigma * \tau)(0) : T] \leq [\tau(0) : \tau^0(0)]$, which is finite. On the other hand, we claim $T = \sigma(0) + (\sigma^0 * \tau^0)(0)$, where the $+$ denotes a group sum. Indeed, since $0 \in \tau^0(0)$, we know T contains both groups on the right, thus their sum. Conversely, given some $x \in T$, we choose some $y \in \tau^0(0)$ such that $(y, x) \in \sigma$. Since $y \in \tau^0(0) \subseteq G^0$, there is some $z \in G^0$ such that $(y, z) \in \sigma^0$. But then $z \in (\sigma^0 * \tau^0)(0)$ by definition and $x - z \in \sigma(0)$. Hence T equals the sum of the two groups. A quick inspection shows that $\sigma(0) \cap (\sigma^0 * \tau^0)(0) \supseteq \sigma^0(0)$ since $0 \in \tau^0(0)$. The Second Isomorphism Theorem thus implies that T is a finite extension of $(\sigma^0 * \tau^0)(0)$, and so we have shown that $(\sigma * \tau)(0)$ finitely extends $(\sigma^0 * \tau^0)(0)$. Yet by Lemma 6.1.11, $(\sigma * \tau)^0(0)$ has finite index in $(\sigma * \tau)(0)$ and $(\sigma^0 * \tau^0)^0(0)$ has finite index in $(\sigma^0 * \tau^0)(0)$. Since $(\sigma * \tau)^0(0)$ extends $(\sigma^0 * \tau^0)^0(0)$, the latter must have finite index in the former. By the conclusion of the previous paragraph, $(\sigma * \tau)^0 = (\sigma^0 * \tau^0)^0$. □

Corollary 6.1.15. *Suppose connected components have finite index. Let H be a set of morphisms and define:*

$$R = \{\sigma^0 \,|\, \sigma \in E[H]\}$$

Then $R = E^0[H]$ and R is a symmetric near semiring, with the operations

$$\begin{aligned} -^0(\sigma^0) &:= (-\sigma)^0 \\ \sigma^0 +^0 \tau^0 &:= (\sigma + \tau)^0 \\ \sigma^0 *^0 \tau^0 &:= (\sigma * \tau)^0 \end{aligned}$$

Proof. We shall prove the equality $R = E^0[H]$ by showing inductively that $H_n^* = \{\sigma^0 \mid \sigma \in H_n\}$ for all $n < \omega$. Clearly $H_0^* = \{\sigma^0 \mid \sigma \in H_0\}$. Assuming H_n^* has the desired form, consider H_{n+1}^*. Using Lemmas 6.1.12, 6.1.13 and 6.1.14, we obtain:

$$\begin{aligned} H_{n+1}^* &= \{(\sigma_1 - \sigma_2)^0 \mid \sigma_1, \sigma_2 \in H_n^*\} \cup \{(\sigma_1 * \sigma_2)^0 \mid \sigma_1, \sigma_2 \in H_n^*\} \\ &= \{(\tau_1^0 - \tau_2^0)^0 \mid \tau_1, \tau_2 \in H_n\} \cup \{(\tau_1^0 * \tau_2^0)^0 \mid \tau_1, \tau_2 \in H_n\} \\ &= \{(\tau_1^0 + (-\tau_2)^0)^0 \mid \tau_1, \tau_2 \in H_n\} \cup \{(\tau_1^0 * \tau_2^0)^0 \mid \tau_1, \tau_2 \in H_n\} \\ &= \{(\tau_1 + (-\tau_2))^0 \mid \tau_1, \tau_2 \in H_n\} \cup \{(\tau_1 * \tau_2)^0 \mid \tau_1, \tau_2 \in H_n\} \\ &= \{\sigma^0 \mid \sigma \in H_{n+1}\} \end{aligned}$$

Since $E[H] = \bigcup_{n<\omega} H_n$ by Proposition 6.1.10 and $E^0[H] = \bigcup_{n<\omega} H_n^*$, the induction proves $R = E^0[H]$.

Defining $-^0$, $+^0$ and $*^0$ on R as in the statement of the theorem, we immediately conclude that R is a symmetric near semiring using Lemmas 6.1.12, 6.1.13, 6.1.14 to understand the operations of R in terms of those on $E[H]$, which is a symmetric near semiring by Lemma 6.1.5. For example, left distributivity:

$$\begin{aligned} \sigma^0 *^0 (\tau^0 +^0 \lambda^0) &= \sigma^0 *^0 (\tau + \lambda)^0 \\ &= (\sigma * (\tau + \lambda))^0 \\ &= (\sigma * \tau + \sigma * \lambda)^0 \\ &= (\sigma * \tau)^0 +^0 (\sigma * \lambda)^0 \\ &= (\sigma^0 *^0 \tau^0) +^0 (\sigma^0 *^0 \lambda^0) \end{aligned}$$

□

In the special cases of quasiendomorphisms and endomorphisms, $E^0[H]$ produces actual rings.

Corollary 6.1.16. *If H consists of only quasiendomorphisms, then $E^0[H]$ is a ring and $-^0$ takes elements to their additive inverses.*
If H consists of only endomorphisms, then $E[H]$ is a ring and $-^0$ takes elements to their additive inverses. If the group G is connected, then $E[H] = E^0[H]$.

Proof. Since being a quasiendomorphism is preserved under $-$, $+$, $*$, and connected components, the previous corollary gives us that all of $E^0[H]$ consists of solely quasiendomorphisms. By Lemmas 6.1.12 and 6.1.13, $(\sigma +^0 (-^0\sigma)) = (\sigma - \sigma)^0 = (G \times \sigma(0))^0 = 0^0$. Thus $-^0\sigma$ is the additive inverse under $+^0$ of $\sigma \in E^0[H]$. Similarly, since σ_3 has finite kernel, Lemma 6.1.5 gives us

$$\begin{aligned}(\sigma_1 +^0 \sigma_2) *^0 \sigma_3 &= ((\sigma_1 + \sigma_2) * \sigma_3)^0 \\ &= (\sigma_1 * \sigma_3 + \sigma_2 * \sigma_3)^0 \\ &= \sigma_1 *^0 \sigma_3 +^0 \sigma_2 *^0 \sigma_3\end{aligned}$$

and $\sigma_3 *^0 0 = 0^0$.

Similarly, the negation, sum, and product of endomorphisms is an endomorphism, so if H consists solely of endomorphisms, so does $E[H]$. Lemma 6.1.5 implies that if $\ker(\sigma_3) = \{0\}$, then $\sigma_3 * 0 = 0$, multiplication by σ_3 on the right distributes over addition, and $\sigma_3 - \sigma_3 = 0$. Hence $E[H]$ is a ring. If G is connected, then any endomorphism on G equals its connected component; by Corollary 6.1.15, $E[H] = E^0[H]$. □

Corollary 6.1.17. *If H consists solely of quasiendomorphisms, then $E^0[H]$ is the quotient of $E[H]$ by the ideal $I = \{\sigma \in E[H] \mid \sigma^0 = 0^0\}$.*

Proof. Let $R = E^0[H]$ and consider the map $f : E[H] \to R$ where $\sigma \mapsto \sigma^0$. By the way addition and multiplication are defined on R in Corollary 6.1.15, we have ensured that f is a ring homomorphism. Its kernel clearly must be I. □

When H consists solely of (quasi)-endomorphisms, we shall refer to $E^0[H]$ as the **ring of (quasi)-endomorphisms** on G generated by H. There are several advantages to the ring of quasiendomorphisms $E^0[H]$ over the symmetric near semiring of morphisms $E[H]$, not least of which is that we are dealing with a *ring* rather than a symmetric near semiring. In general, $E^0[H]$ removes the finite noise caused by addition and multiplication. Another example occurs when we multiply two additive relations σ and τ which may be near inverses of each other, i.e. $\sigma * \tau$ is a finite extension of 1. By taking connected components, we force σ^0 to be the a left inverse of τ^0 in $E^0[H]$.

We analyze several symmetric near semirings of additive relations which may arise in the context of stable, $\aleph_0$-categorical groups. In all cases, we will push to obtain quasiendomorphisms, or even endomorphisms, so that our near semirings will be actual rings. However we have conducted the preparations in this section in greater generality to permit certain manipulations later on that do not always produce rings.

The near semirings constructed in the following sections will usually arise under additional hypotheses than the two model theoretic ones. Our goal will be to utilize the $\aleph_0$-categoricity and stability to force the associated rings to be finite.

6.2 First application

In this application, we use automorphic actions on a subgroup to define an endomorphism ring. This situation arises in the reduced counterexample to the BCM Conjecture that we have obtained in Proposition 5.1.1. Although that group arises in a stable, $\aleph_0$-categorical context, the endomorphism ring construction below follows solely from a few group-theoretic hypotheses. Nonetheless, the example in this section illustrates how quasiendomorphism rings arise naturally in counterexamples to the BCM Conjecture. For this example, we shall write the original group, G, multiplicatively to avoid confusion.

Theorem 6.2.1. *Let G be a group of nilpotency class at most 2. Suppose N is a proper normal abelian subgroup of G of finite exponent, n. Then consider the action of G on N by conjugation, which yields a group $H \cong G/C_G(N)$ of definable automorphisms of N. The resulting ring of endomorphisms, $E[H]$, is nilpotent by finite. If, furthermore, N is a vector space, then $E[H]$ is null by finite.*

Proof. Since N is finite exponent and abelian, for each prime p, it has only one Sylow p-subgroup S_p and N is clearly the direct product all of them. For each p, the p-Sylow subgroup S_p of N is characteristic and thus normal in G as well (and definable if N is definable).

Since N is normal, conjugation defines an automorphic action of G on N. The kernel of the resulting map from G to $\mathrm{Aut}(N)$ is precisely $C_G(N)$. Hence, for every $\overline{g} \in G/C_G(N)$, we get an automorphism $\sigma_{\overline{g}}$ of N given by $\sigma_{\overline{g}}(n) = g^{-1}ng$. Set $H = \{0, 1\} \cup$

$\{\sigma_{\overline{g}} \,|\, \overline{g} \in G/C_G(N)\}$. Note that

$$\begin{aligned}(\sigma_{\overline{g}} * \sigma_{\overline{h}})(n) &= \sigma_{\overline{g}}(h^{-1}nh) \\ &= g^{-1}h^{-1}nhg = \sigma_{\overline{gh}}\end{aligned}$$

Since $Z(G) \leq C_G(N)$ and G has nilpotency class 2, the group $G/C_G(N)$ is abelian, and thus $\sigma_{\overline{g}} * \sigma_{\overline{h}} = \sigma_{\overline{h}} * \sigma_{\overline{g}}$ for all $\overline{g}, \overline{h} \in G/C_G(N)$. Therefore multiplication in $R = E[H]$ is commutative, and R is a ring since H consists solely of endomorphisms (Corollary 6.1.16).

Let $\sigma_1, \sigma_2 \in H$ be given and choose representatives $g_1, g_2 \in G$ of the corresponding classes in $G/C_G(N)$. Let $a \in N$ be given. Since $g_1 a g_1^{-1} a^{-1} \in Z(G)$, we have that:

$$\begin{aligned}(\sigma_{\overline{g_1}} + \sigma_{\overline{g_2}})(a) &= g_1 a g_1^{-1} g_2 a g_2^{-1} \\ &= (g_1 a g_1^{-1} a^{-1}) a g_2 a g_2^{-1} \\ &= a g_2 g_1 a g_1^{-1} a^{-1} a g_2^{-1} \\ &= a g_2 g_1 a g_1^{-1} g_2^{-1} \\ &= (1 + \sigma_{\overline{g_2 g_1}})(a)\end{aligned}$$

This equation holds independent of the choice of representatives g_1 and g_2, hence we obtain that $\sigma_1 + \sigma_2 = 1 + \sigma_2 * \sigma_1$. By induction, this means that every element of R is of the form $1 + \ldots + 1 + \sigma$, for some $\sigma \in H$ and finite sum of 1s. But since N has exponent n, $n \cdot 1 = 0$ in R and n is the least positive integer with this property. In other words, R has characteristic n. To obtain R, we only need to construct elements of the form $k + \sigma$ for $\sigma \in H$ and $0 \leq k < n$ and therefore R is naturally seen as a subset of $\{0, \ldots, n-1\} \times H$.

Let I be the nilradical of R, that is, the ideal consisting of all nilpotent elements of R. Equivalently, I is the radical of the zero ideal. Immediately, we see that $m\mathbb{Z} \subseteq I$, where m is the product of all distinct primes dividing n. Furthermore, the equation $\sigma_1 + \sigma_2 = 1 + \sigma_1 * \sigma_2$ for $\sigma_1, \sigma_2 \in H$ yields that $(H-1)^2 = 0$ and thus $H - 1 \subseteq I$. Consider the projection $\pi : R \to R/I$. Since every element of R can be written as $k + \sigma$ for some $\sigma \in H$ and $0 \leq k < n$, we find that $\pi(k + \sigma) = \pi(k + 1)$. This shows that the restricted map $\pi : \mathbb{Z}/n\mathbb{Z} \to R/I$ is a surjection, so R is nilpotent by finite and $I \supseteq H - 1 + m\mathbb{Z}$. But the reverse inclusion is obvious since $k \notin I$ for integer $k \notin m\mathbb{Z}$. In the special case when $n = p$ a prime, then R has characteristic p and $m = p$, so $I = H - 1$. Since $(H-1)^2 = 0$, I is null and R is null by finite. $\square$

6.3 Second application

Our setting for this example involves three additive abelian groups A, G, H interpretable in our theory. We assume that G and H are connected and that we have a definable subset $\Sigma \subseteq A \times G \times H$ satisfying:

1. $\pi_1(\Sigma) = A$
2. For all $a \in A$, $\sigma_a := \{(g, h) \in G \times H \,|\, (a, g, h) \in \Sigma\}$ is a homomorphism from all of G to H. We shall write σ_a functionally as $\sigma_a(g) = h$.
3. σ_0 is the zero map $0 : x \mapsto 0$,
4. For all $a, b \in A$ and $g \in G$, $\sigma_{a+b}(g) = \sigma_a(g) + \sigma_b(g)$ (i.e. $\sigma : A \times G \to B$ given by $(a, g) \mapsto \sigma_a(g)$ is a bilinear function.)

There will be two properties that will frequently fall under our concern for a nonzero $a \in A$: (i) whether σ_a is surjective, and (ii) whether $\ker(\sigma_a)$ is finite. Both these properties will have significant advantages; the former in producing invertible elements and the latter in producing quasiendomorphisms. Hence, we will pay special attention to these properties in the sequel. Also, since we are dealing with connected groups, the endomorphisms 0^0 and 1^0 equal 0 and 1, respectively, so we will drop the exponent ^{0}.

Under our assumptions, the σ_a are a uniformly definable family of homomorphisms from G to H. In the initial setting, we have to worry about $\sigma_a \equiv 0$, but with the following proposition, we can eliminate that concern.

Proposition 6.3.1. *Given A, G, H, Σ as above, the set of all indices corresponding to trivial homomorphisms, $B = \{a \in A \,|\, \sigma_a \equiv 0\}$ is a definable subgroup. We may then consider $\Sigma' := \{(a + B, g, h) \,|\, (a, g, h) \in \Sigma\}$. This is a well-defined set which has the same properties (1)-(4) as Σ. Furthermore $\ker(\sigma_a)$ is finite if and only if $\ker(\sigma_{a+B})$ is finite and the analogous statement holds for surjectivity of σ_a versus σ_{a+b}. Lastly, $\sigma_{a+B} \equiv 0$ if and only if $a \in B$ if and only if $a + B = 0$ in A/B.*

Proof. If $a, b \in B$, then for any $g \in G$ we have $\sigma_{a+b}(g) = \sigma_a(g) + \sigma_b(g) = 0 + 0$, so $a + b \in B$. If $a \in B$ then $\sigma_{-a} \equiv \sigma_{-a} + \sigma_a \equiv \sigma_{a-a} = \sigma_0 \equiv 0$. So $-a \in B$ and B is a group. B is clearly definable.

Given $a, a' \in A$, if $a = a' + b$ for some $b \in B$ then for all $g \in G$,

$$\sigma_a(g) = \sigma_{a'+b}(g) = \sigma_{a'}(g) + \sigma_b(g) = \sigma_{a'}(g)$$

so $\sigma_a \equiv \sigma_{a'}$. Therefore, it makes sense to define Σ' and the σ_{a+B} as in the statement of the proposition. Other than the indexing set, nothing else has changed about our homomorphisms, and it is clear that $\sigma_{a+B} \equiv 0$ if and only if $a + B = B$. □

From now on, we shall assume that our A, G, H, Σ also satisfy:

5. For all $a \in A$, $\sigma_a \equiv 0$ if and only if $a = 0$.

Given this setting, we can construct a large uniformly-defined family of additive relations on G. For each $a, b \in A$, where $b \neq 0$, define $\Gamma_{a,b}$ to be:

$$\Gamma_{a,b} = \{(g, g') \in G \times G \mid \sigma_a(g) = \sigma_b(g')\}$$

We see that $\Gamma_{a,b}$ is an additive relation if and only if $\mathrm{im}(\sigma_b)$, the image of σ_b, contains $\mathrm{im}(\sigma_a)$, the image of σ_a. Set $0 = G \times 0$ and $1 = \Delta = \{(g, g) \mid g \in G\}$.

Proposition 6.3.2. *$\Gamma_{a,b}$ is a quasiendomorphism if and only if $\mathrm{im}(\sigma_b) \supseteq \mathrm{im}(\sigma_a)$ and $\ker(\sigma_b)$ is finite.*

Proof. By Lemma 6.1.2, $\Gamma_{a,b}$ is a quasiendomorphism if and only if $\Gamma_{a,b}(0)$ is finite. But $\Gamma_{a,b}(0) = \ker(\sigma_b)$, so we have our result. □

Set

$$\begin{aligned} \mathcal{A} &= \{0, 1\} \cup \{\Gamma_{a,b} \mid a, b \in A,\ b \neq 0,\ \mathrm{im}(\sigma_b) \supseteq \mathrm{im}(\sigma_a)\} \\ \mathcal{F} &= \{0, 1\} \cup \{\Gamma_{a,b} \mid a, b \in A,\ b \neq 0,\ \mathrm{im}(\sigma_b) \supseteq \mathrm{im}(\sigma_a),\ \ker(\sigma_b) \text{ finite}\}. \end{aligned}$$

Then $\mathcal{A}$ consists of 0, 1, and the $\Gamma_{a,b}$ which are additive relations; this is a uniformly definable family. Similarly, the uniformly definable family $\mathcal{F}$ consists of 0, 1 and the $\Gamma_{a,b}$ which are quasiendomorphisms. Since, in our application to stable, $\aleph_0$-categorical structures connected components have finite index, we will proceed with an analysis of the semiring $E^0[\mathcal{A}]$, and more importantly, the sub(semi)ring $R = E^0[\mathcal{F}]$. Note that every element of $E^0[\mathcal{A}]$ is a definable group since each element of $\mathcal{A}$ is definable. By Corollary 6.1.16, R is a ring whose additive and multiplicative identities are clearly 0 and 1, respectively. We immediately obtain identities in R and $E^0[\mathcal{A}]$, which are just restatements of the general properties developed in Section 6.1.

Proposition 6.3.3. *Let $a, b \in A$ with $a \neq 0$ and $\mathrm{im}(\sigma_a) \supseteq \mathrm{im}(\sigma_b)$.*

1. *If $\ker(\sigma_a)$ finite, $\Gamma^0_{0,a} = 0$,*

2. *If $\ker(\sigma_a)$ finite, $\Gamma^0_{a,a} = 1$,*

3. *If $\ker(\sigma_a)$ finite, $\Gamma^0_{b,a} -^0 \Gamma^0_{b,a} = 0$,*

4. *$-\Gamma_{b,a} = \Gamma_{-b,a} = \Gamma_{b,-a}$ and so $-^0\Gamma^0_{b,a} = \Gamma^0_{-b,a} = \Gamma^0_{b,-a}$.*

Proof. By the initial hypotheses, all the Γ which appear in the statements are additive relations. Since $\sigma_0(g) = 0$ for all $g \in G$ and $\sigma_a(g) = 0$ if and only if $g \in \ker(\sigma_a)$, we know $\Gamma_{0,a} = G \times \ker(\sigma_a)$. Since $\ker(\sigma_a)$ is finite by assumption, $\Gamma^0_{0,a}$ is clearly 0.

The second claim is another immediate consequence of the definitions, the finiteness of $\ker(\sigma_a)$, and Lemma 6.1.11.

The third claim just says that $-^0$ takes elements to their additive inverses; this is true in R by Corollary 6.1.16.

For the last claim, we know by definition

$$\begin{aligned} -\Gamma_{b,a} &= \{(g, -g') \in G \times G \mid (g, g') \in \Gamma_{b,a}\} \\ &= \{(g, -g') \in G \times G \mid \sigma_b(g) = \sigma_a(g')\} \\ &= \{(g, g') \in G \times G \mid \sigma_b(g) = \sigma_a(-g')\} \\ &= \{(g, g') \in G \times G \mid \sigma_b(g) = -\sigma_a(g')\} \end{aligned}$$

Yet since $\sigma_x(h) + \sigma_{-x}(h) = \sigma_{x-x}(h) = 0$ for all $h \in G$ and $x \in A$, we know that the set above is equal to both $\Gamma_{-b,a}$ and $\Gamma_{b,-a}$. By Lemma 6.1.12, taking connected components gives us the second part of the result. □

Due to properties (1)-(5) proscribed upon A, G, H, and Σ, we obtain several other identities involving the elements of $\mathcal{F}$. We remark that analogue of the previous and the following propositions both hold for $\Gamma_{a,b}$ without the restriction on finite kernels, but appropriate care must be taken when finite kernels are necessary.

Proposition 6.3.4. *Let $a, b, c \in A$ with $a \neq 0$. The following properties hold:*

1. *If $b \neq 0$ and $\mathrm{im}(\sigma_b) \supseteq \mathrm{im}(\sigma_a) \supseteq \mathrm{im}(\sigma_c)$, then $\Gamma_{a,b}, \Gamma_{c,a}, \Gamma_{c,b} \in \mathcal{A}$ and they satisfy the identity $\Gamma_{c,b} = \Gamma_{a,b} * \Gamma_{c,a}$. So $\Gamma^0_{c,b} = \Gamma^0_{a,b} *^0 \Gamma^0_{c,a}$.*

2. *If* $b \neq 0$, $\mathrm{im}(\sigma_a) = \mathrm{im}(\sigma_b)$, *and* $\ker(\sigma_b)$ *is finite, then* $\Gamma^0_{b,a}$ *has* $\Gamma^0_{a,b}$ *as a left inverse. Symmetrically, if* $b \neq 0$, $\mathrm{im}(\sigma_a) = \mathrm{im}(\sigma_b)$, *and* $\ker(\sigma_a)$ *is finite, then* $\Gamma^0_{b,a}$ *has* $\Gamma^0_{a,b}$ *as a right inverse.*

3. *If* $\mathrm{im}(\sigma_a) \supseteq \mathrm{im}(\sigma_b)$ *or* $\mathrm{im}(\sigma_a) \supseteq \mathrm{im}(\sigma_c)$, *then* $\Gamma_{b,a} + \Gamma_{c,a} = \Gamma_{b+c,a}$. *If* $\Gamma_{b,a}, \Gamma_{c,a} \in \mathcal{F}$ *then* $\Gamma_{b+c,a} \in \mathcal{F}$. *The converse holds if* σ_a *surjective. If they are all elements of* $\mathcal{F}$, *then* $\Gamma^0_{b,a} +^0 \Gamma^0_{c,a} = \Gamma^0_{b+c,a}$.

4. *If* $\mathrm{im}(\sigma_a) \supseteq \mathrm{im}(\sigma_b)$, *then for any* $k \in \mathbb{N}$, *we have* $k\Gamma_{b,a} = \Gamma_{kb,a}$. *Thus* $k\Gamma^0_{b,a} = \Gamma^0_{kb,a}$,

5. *If* $\Gamma_{b,a} \in \mathcal{F}$, *then for any* $k \in \mathbb{Z}$, $\Gamma^0_{b,a} +^0 k = 0$ *if and only if* $b + ak = 0$. *If* $b + ak \neq 0$ *and* $\Gamma_{a,b+ka} \in \mathcal{F}$, *then* $\Gamma^0_{a,b+ka}$ *is a left inverse of* $\Gamma^0_{b,a} +^0 k$.

Proof. 1. The assumption on the inclusion of the images guarantees that all the $\Gamma_{x,y}$ that were named are additive relations, i.e. elements of $\mathcal{A}$. Unraveling the definitions: $(g, g') \in \Gamma_{a,b} * \Gamma_{c,a}$ iff there is an $h \in G$ with $(g, h) \in \Gamma_{c,a}$ and $(h, g') \in \Gamma_{a,b}$. The first membership can be rewritten as $\sigma_c(g) = \sigma_a(h)$ and the second membership can be rewritten as $\sigma_a(h) = \sigma_b(g')$. This implies $\sigma_c(g) = \sigma_b(g')$, so $(g, g') \in \Gamma_{c,b}$. This shows that $\Gamma_{a,b} * \Gamma_{c,a} \subseteq \Gamma_{c,b}$. On the other hand, if $\sigma_c(g) = \sigma_b(g')$ then any $h \in G$ such that $\sigma_a(h) = \sigma_c(g)$ witnesses that $\Gamma_{c,b} \subseteq \Gamma_{a,b} * \Gamma_{c,a}$. We are guaranteed such an h since $\Gamma_{c,a} \in \mathcal{A}$, so $\mathrm{im}(\sigma_a) \supseteq \mathrm{im}(\sigma_c)$. Hence $\Gamma_{c,b} = \Gamma_{a,b} * \Gamma_{c,a}$ and the corresponding statement for connected components follows from the definition of $*^0$ and Proposition 6.1.14.

2. Part (1) with $c = b$ gives us $\Gamma^0_{a,b} *^0 \Gamma^0_{b,a} = \Gamma^0_{b,b}$. Since $\ker(\sigma_b)$ is finite, $\Gamma^0_{b,b} = 1$. The second part follows by symmetry.

3. For a given $g \in G$, suppose $(g, g_1) \in \Gamma_{b,a}$ and $(g, g_2) \in \Gamma_{c,a}$ then $\sigma_b(g) = \sigma_a(g_1)$ and $\sigma_c(g) = \sigma_a(g_2)$. Since $\sigma_b(g) + \sigma_c(g) = \sigma_{b+c}(g)$ and σ_a is a homomorphism, we have $\sigma_{b+c}(g) = \sigma_a(g_1 + g_2)$, so $(g, g_1 + g_2) \in \Gamma_{b+c,a}$. Conversely, suppose $(g, g') \in \Gamma_{b+c,a}$. Without loss of generality, assume $\mathrm{im}(\sigma_a) \supseteq \mathrm{im}(\sigma_b)$. Then there is a $g_1 \in G$ such that $\sigma_b(g) = \sigma_a(g_1)$. But then $\sigma_c(g) = \sigma_{b+c}(g) - \sigma_b(g) = \sigma_a(g') - \sigma_a(g_1)$, so $(g, g' - g_1) \in \Gamma_{c,a}$. Therefore $\Gamma_{b,a} + \Gamma_{c,a} = \Gamma_{b+c,a}$. If $\Gamma_{b,a}, \Gamma_{c,a} \in \mathcal{F}$, then $\mathrm{im}(\sigma_a) \supseteq \mathrm{im}(\sigma_b) + \mathrm{im}(\sigma_c) \supseteq \mathrm{im}(\sigma_{b+c})$. Since $\ker(\sigma_a)$ is finite, we conclude $\Gamma_{b+c,a} \in \mathcal{F}$. Conversely, if σ_a is surjective and $\ker(\sigma_a)$ is finite, then $\Gamma_{x,a} \in \mathcal{F}$ for any nonzero $x \in A$. The statement for connected components follows from the definition of $*^0$ and Proposition 6.1.13.

4. immediate by induction from previous step.

5. Since $\ker(\sigma_a)$ is finite, we may use (2) from Proposition 6.3.3 and since $\text{im}(\sigma_a) \supseteq \text{im}(\sigma_b)$, we may use parts (3) and (4), to obtain altogether:

$$\Gamma^0_{b,a} +^0 k = \Gamma^0_{b,a} +^0 k\Gamma^0_{a,a} = \Gamma^0_{b,a} +^0 \Gamma^0_{ka,a} = \Gamma^0_{b+ka,a}$$

Since $\Gamma_{a,a} \in \mathcal{F}$ by default since $a \neq 0$ and $\Gamma_{b,a} \in \mathcal{F}$, these steps also give us $\Gamma_{b+ka,a} \in \mathcal{F}$. By (3), $\Gamma^0_{b+ka,a}$ has a left inverse unless $b + ka = 0$ or $\Gamma_{a,b+ka} \notin \mathcal{F}$. If we have our assumption on $\Gamma_{a,b+ka}$, then (3) tells us it is a left inverse. If, on the other hand, $b + ka = 0$, then $\Gamma^0_{b+ka,a} = 0$ by (1) of Proposition 6.3.3.

□

Naturally, when the various σ_a are surjective and have finite kernels, many of these hypotheses disappear and we obtain a cleaner version of the previous proposition.

Proposition 6.3.5. *Let $a, b, c \in A$ with σ_a, σ_b, and σ_c surjective and $\ker(\sigma_a), \ker(\sigma_b)$, and $\ker(\sigma_c)$ all finite when a, b, c are nonzero, respectively. Assume $a \neq 0$. Then the following properties hold:*

1. *If $b \neq 0$, then $\Gamma_{c,b} = \Gamma_{a,b} * \Gamma_{c,a}$. So $\Gamma^0_{c,b} = \Gamma^0_{a,b} *^0 \Gamma^0_{c,a}$*

2. *If $b \neq 0$, then $\Gamma^0_{b,a}$ and $\Gamma^0_{a,b}$ are inverses of each other.*

3. *$\Gamma_{b,a} + \Gamma_{c,a} = \Gamma_{b+c,a}$, so $\Gamma^0_{b,a} +^0 \Gamma^0_{c,a} = \Gamma^0_{b+c,a}$.*

4. *For any $k \in \mathbb{N}$, we have $k\Gamma_{b,a} = \Gamma_{kb,a}$. Thus $k\Gamma^0_{b,a} = \Gamma^0_{kb,a}$,*

5. *For any $k \in \mathbb{Z}$, $\Gamma^0_{b,a} +^0 k = 0$ if and only if $b + ak = 0$. If $b + ak \neq 0$ and $\Gamma^0_{a,b+ka} \in \mathcal{F}$ then $\Gamma^0_{a,b+ka}$ is a left inverse of $\Gamma^0_{b,a} +^0 k$.*

These propositions reveal some very particular interactions, which force A, G, and H to take specific forms.

Lemma 6.3.6. *Suppose A, G, H, Σ are as prescribed by Proposition 6.3.1 and let $R = E^0[\mathcal{F}]$. Set $Y = \{a \in A \,|\, a \neq 0, \ker(\sigma_a)$ finite, σ_a surjective $\}$. If $Y \neq \emptyset$, then one of two possibilities occurs:*

1. $\text{char}(R) = 0$, *G has infinite exponent, and Y has no torsion elements,* or

2. $\operatorname{char}(R) = n$ *for some* $n > 0$, $\exp(G) = n$, *ord*$_A(a) = n$ *for all* $a \in Y$, *and exp*$(H)|n$.

Proof. Assume $Y \neq \emptyset$ and consider the condition $k = 0$ in R for an integer $k > 0$. On the one hand, by definition of 1 and $+$, $k = \{(g, kg) \,|\, g \in G\}$ and this is clearly a connected endomorphism since G is connected. The endomorphism k equals $0 = G \times \{0\}$ if and only if $kg = 0$ for all $g \in G$. This occurs exactly when k is a multiple of $\exp(G)$. So $k = 0$ if and only if $\exp(G)|k$.

On the other hand, if a nonzero $a \in A$ has $\ker(\sigma_a)$ finite and σ_a surjective, then Proposition 6.3.5 gives the following identity:

$$k \cdot 1 = k\Gamma^0_{a,a} = \Gamma^0_{ka,a}$$

By (5) in Proposition 6.3.5, the right hand side equals 0 if and only if $ka = 0$, i.e. $\operatorname{ord}_A(a)|k$. Thus we have the following equivalence:

1. $k = 0$ in R

2. $\exp(G)|k$

3. $\operatorname{ord}_A(a)|k$ for some (all) $a \in Y$

Consequently, the following are equivalent:

- $\operatorname{char}(R) = 0$

- $\exp(G)$ is infinite

- Y has no torsion elements

Now assume that $\operatorname{char}(R) \neq 0$. Condition (2) forces $\operatorname{char}(R) = \exp(G)$. For a given $a \in Y$, condition (3) demands that $\operatorname{char}(R) = \operatorname{ord}_A(a)$. Hence we get the following equivalence for $n > 0$:

- $\operatorname{char}(R) = n$

- $\exp(G) = n$

- $\operatorname{ord}_A(a) = n$ for any (all) $a \in Y$

Clearly, since σ_a maps G onto H for any $a \in Y$, $\exp(H)|\exp(G)$. □

Corollary 6.3.7. *Suppose A, G, H, Σ are as prescribed by Proposition 6.3.1 and let $R = E^0[F]$. If $\ker(\sigma_a)$ is finite and σ_a is surjective for all nonzero $a \in A$ and $A \neq \{0\}$, then one of two possibilities occurs:*

1. $\operatorname{char}(R) = 0$*, G has infinite exponent, and A is torsion-free,* or

2. $\operatorname{char}(R) = p$ *for some prime p and A, G, and H are $\mathbb{F}_p$-vector spaces.*

Proof. We use Lemma 6.3.6 with $Y = A\backslash\{0\}$. If $\operatorname{char}(R) = 0$, this lemma spells out the desired possibility outright. If $\operatorname{char}(R) = n > 0$, then $\operatorname{ord}_A(a) = n$ for all nonzero $a \in A$. Since $A \neq \{0\}$, this is only possible if n is prime. The rest follows immediately. □

When we are in the characteristic p prime case, we can naturally extend our additive relation construction to tensors. To maintain clarity in the category of rings of characteristic p, for any finite field F of characteristic p, we have the natural inclusion functor ι_F, which embeds X into $X \otimes_{\mathbb{F}_p} F$ as the set of all $x \otimes 1$. Even though much of the arguments that follow are ultimately consequences of the general properties of the tensor functor, the abstract proofs take as much argument as the direct proofs, so we have presented the direct ones for more elucidation in our particular setting. Moreover, tensoring does not preserve all our objects: a tensored ring of quasiendomorphisms does not produce a ring of quasiendomorphisms, but only a semiring of additive relations.

Lemma 6.3.8. *Suppose that A, G and H are $\mathbb{F}_p$ vector spaces with G and H both connected and there is a definable $\Sigma \subseteq A \times G \times H$ which satisfies properties (1)-(5) listed in the beginning of this section. Assume $A \neq 0$ and let F be any given finite field F of characteristic p. Set $B = A \otimes_{\mathbb{F}_p} F$, $V = G \otimes_{\mathbb{F}_p} F$, and $W = H \otimes_{\mathbb{F}_p} F$.*

Then there is a definable subset $\Sigma' \subseteq B \times V \times W$, such that

- *$\Sigma' \supseteq \iota_F(\Sigma)$, where $\iota_F(\Sigma)$ is the image of Σ as a subset of of $\iota_F(A \times G \times H) \subseteq B \times V \times W$.*
- *the system B, V, W, Σ' satisfies the conditions (1)-(5) listed in the beginning of this section.*

Proof. Let $B = A \otimes_{\mathbb{F}_p} F$, $V = G \otimes_{\mathbb{F}_p} F$, and $W = H \otimes_{\mathbb{F}_p} F$. Fix a basis $\{e_i \,|\, i < \kappa\}$ for F over $\mathbb{F}_p$ with $e_0 = 1$.

Given a nonzero $a \in A$ and $\alpha \in F$, we present a homomorphism $\sigma_{a\otimes\alpha} : V \to W$, given by:

$$\sigma_{a\otimes\alpha}\left(\sum_{i<\kappa} g_i \otimes e_i\right) = \sum_{i<\kappa} \sigma_a(g_i) \otimes \alpha e_i$$

We must check that this is well defined. If $a = 0$ or $\alpha = 0$, then clearly $\sigma_{a\otimes\alpha} \equiv 0$. If $k \in \mathbb{F}_p$ nonzero, then

$$\begin{aligned}
\sigma_{a\otimes k\alpha}\left(\sum_{i<\kappa} g_i \otimes e_i\right) &= \sum_{i<\kappa} \sigma_a(g_i) \otimes k\alpha e_i \\
&= \sum_{i<\kappa} k\sigma_a(g_i) \otimes \alpha e_i \\
&= \sum_{i<\kappa} \sigma_{ka}(g_i) \otimes \alpha e_i \\
&= \sigma_{ka\otimes\alpha}\left(\sum_{i<\kappa} g_i \otimes e_i\right)
\end{aligned}$$

We extend the definition to σ_b for an arbitrary $b \in B$ by linearity, defining $\sigma_{b+b'} = \sigma_b + \sigma_{b'}$. We must verify that such an extension is compatible with the bilinearity of B. It suffices to show that $\sigma_{a\otimes f+a\otimes g} = \sigma_{a\otimes(f+g)}$ and $\sigma_{a\otimes f+a'\otimes f} = \sigma_{(a+a')\otimes f}$. We shall verify the latter, since the former has an analogous proof.

$$\begin{aligned}
\sigma_{a\otimes f+a'\otimes f}\left(\sum_{i<\kappa} g_i \otimes e_i\right) &= \sigma_{a\otimes f}\left(\sum_{i<\kappa} g_i \otimes e_i\right) + \sigma_{a'\otimes f}\left(\sum_{i<\kappa} g_i \otimes e_i\right) \\
&= \left(\sum_{i<\kappa} \sigma_a(g_i) \otimes fe_i\right) + \left(\sum_{i<\kappa} \sigma_{a'}(g_i) \otimes fe_i\right) \\
&= \sum_{i<\kappa} (\sigma_a(g_i) + \sigma_{a'}(g_i)) \otimes fe_i \\
&= \sum_{i<\kappa} \sigma_{a+a'}(g_i) \otimes fe_i \\
&= \sigma_{(a+a')\otimes f}\left(\sum_{i<\kappa} g_i \otimes e_i\right)
\end{aligned}$$

So the homomorphisms $\sigma_b : V \to W$ are well-defined for all $b \in B$.

The bilinearity of the tensor and the definition of the σ's will give us that the definition of the σ_a's is independent of the choice of basis. Indeed, if $f_0, \ldots, f_{\kappa-1}$ is another basis of F, then write $f_i = \sum_{j<\kappa} \mu_{i,j} e_j$. Let $\overline{\sigma}_{a\otimes v}$ denote the mapping if we had defined

$\sigma_{a\otimes v}$ in terms of the f_i instead. Then we get

$$\begin{aligned}
\overline{\sigma}_{a\otimes v}\left(\sum_{i<\kappa} g_i \otimes f_i\right) &= \sum_{i<\kappa} \sigma_a(g_i)\otimes vf_i \\
&= \sum_{i<\kappa} \sigma_a(g_i)\otimes v(\sum_{j<\kappa}\mu_{i,j}e_j) \\
&= \sum_{j<\kappa}\sum_{i<\kappa} \sigma_a(g_i)\otimes v\mu_{i,j}e_j \\
&= \sum_{j<\kappa} \sigma_a\left(\sum_{i<\kappa}\mu_{i,j}g_i\right)\otimes ve_j \\
&= \sigma_{a\otimes v}\left(\sum_{j<\kappa}\left(\sum_{i<\kappa}\mu_{i,j}g_i\right)\otimes e_j\right) \\
&= \sigma_{a\otimes v}\left(\sum_{i<\kappa} g_i\otimes\left(\sum_{i<\kappa}\mu_{i,j}e_j\right)\right) \\
&= \sigma_{a\otimes v}(\sum_{i<\kappa} g_i\otimes f_i)
\end{aligned}$$

So our definitions were indeed independent of the choice of basis of F.

We set $\Sigma' := \{(b, v, w) \in B \times V \times W \mid \sigma_b(v) = w\}$. Note that if $(a, g, h) \in \Sigma$ then clearly $\sigma_{a\otimes 1}(g\otimes 1) = h\otimes 1$, so $(a\otimes 1, g\otimes 1, h\otimes 1) \in \Sigma'$ and thus Σ' extends Σ in the desired way.

Taking stock of our situation, we have $\mathbb{F}_p$-vector spaces V and W. Both of these are connected by Proposition 2.3.10 since G and H are connected and $V \cong G^\kappa$ and $W \cong H^\kappa$ as additive groups. Furthermore, we have another $\mathbb{F}_p$-vector space B and $\Sigma' := \{(b, v, \sigma_b(v)) \mid b \in B,\, v \in V\} \subseteq B \times V \times W$, which yields a uniformly definable family of homomorphisms $\sigma_b : V \to W$ indexed by B. Clearly σ_0 is the zero map, and by the definition of the σ_b, we know that $\sigma_b(v)+\sigma_{b'}(v) = \sigma_{b+b'}(v)$ for all $b, b' \in B$ and $v \in V$. Thus we have verified properties (1)-(4).

Lastly, we must show for $b \in B$ that $\sigma_b \equiv 0$ if and only if $b = 0$. Indeed, assume $\sigma_b \equiv 0$. If $b = \sum_{i<\kappa} a_i \otimes e_i$ for some $a_i \in A$, then for each $g \in G$ we have

$$0 = \sigma_b(g\otimes 1) = \sum_{i<\kappa} \sigma_{a_i}(g)\otimes e_i$$

Since the e_i are a basis and H is an $\mathbb{F}_p$-vector spaces, $W = \oplus_{i<\kappa} H \otimes e_i$, i.e. W as an additive group is just κ copies of H. Hence $0 = \sum_{i<\kappa} \sigma_{a_i}(g)\otimes e_i$ if and only if $\sigma_{a_i}(g) = 0$ for all i. Since $g \in G$ was arbitrary, we conclude that $a_i = 0$ for all $i < \kappa$ and so $b = 0$. $\square$

Since we have the same setting as in the beginning of the section, Σ' produces a family of subgroups $\Gamma_{b,b'}$ of $V \times V$, which are indexed by $B \times B \setminus \{0\}$. Many of these are additive relations on V, so as before, we collect the additive relations and quasiendomorphisms by setting:

$$\begin{aligned} \mathcal{A}_F &= \{0,1\} \cup \{\Gamma_{b,b'} \mid b, b' \in B,\ b' \neq 0,\ \sigma_{b'} \text{ surjective}\} \\ \mathcal{F}_F &= \{0,1\} \cup \{\Gamma_{b,b'} \mid b, b' \in B,\ b' \neq 0,\ \sigma_{b'} \text{ surjective, } \ker(\sigma_{b'}) \text{ finite}\} \end{aligned}$$

which again form two uniformly defined families of additive relations and quasiendomorphsisms, respectively, on V. In some sense, $\mathcal{A}_F$ and $\mathcal{F}_F$ are the "tensors" of the corresponding families on G indexed by elements of $A \times A \setminus \{0\}$. To gain control of which $\Gamma_{b,b'}$ are additive relations, and moreover, quasiendomorphisms, we impose stronger hypotheses on A.

Lemma 6.3.9. *Assume the hypotheses of Lemma 6.3.8 and that for all nonzero $a \in A$, σ_a is both surjective and has finite kernel. Then for any nonzero $a \in A$ and any nonzero $f \in F$, $\sigma_{a\otimes f}$ is surjective and has finite kernel, so for any nonzero $b \in B$, $\Gamma_{b,a\otimes f} \in \mathcal{F}_F$, i.e. $\Gamma^0_{b,a\otimes f}$ is a quasiendomorphism. If σ_b is surjective, then $\Gamma^0_{a\otimes f,b} \in \mathcal{A}_F$ is a right inverse of $\Gamma^0_{b,a\otimes f}$ in the symmetric near semiring $E^0[\mathcal{A}_F] \supseteq E^0[\mathcal{F}_F]$.*

Furthermore, for all nonzero $a, a' \in A$, $\Gamma^0_{a,a'}$ is a unit in $E^0[\mathcal{F}]$, $\Gamma^0_{a\otimes 1,a'\otimes 1}$ is a unit in $E^0[\mathcal{F}_F]$, and their multiplicative orders are equal.

Proof. By Proposition 6.3.2, the assumption that for all nonzero $a \in A$, $\ker(\sigma_a)$ is finite and σ_a is surjective, implies that $\Gamma_{a,b} \in \mathcal{F}$ for any $a, b \in A$ with $b \neq 0$.

Fix nonzero $a \in A$, $f \in F$ and consider $\ker(\sigma_{a\otimes f})$. If $\sum_{i<\kappa} g_i \otimes e_i$ is in this kernel, then $0 = \sum_{i<\kappa} \sigma_a(g_i) \otimes fe_i$. Since f is nonzero, $fe_0, \ldots, fe_{\kappa-1}$ form a basis of F over $\mathbb{F}_p$ as well. Since H is a $\mathbb{F}_p$ vector space, as an $\mathbb{F}_p$-vector space $W = \oplus_{i<\kappa} H \otimes fe_i$. Therefore $\sigma_a(g_i) = 0$ for all $i < \kappa$, so $g_i \in \ker(\sigma_a)$ for all i. Since $\ker(\sigma_a)$ is finite, there are only finitely many choices for tuples $(g_i)_{i<\kappa}$ and hence $\ker(\sigma_{a\otimes f})$ is finite as well.

Now we show $\sigma_{a\otimes f}$ is surjective. Multiplication by f is a change of basis, so we simply need to show that for any desired $h_i \in H$ for $i < \kappa$, we can attain $\sum_{i<\kappa} h_i \otimes fe_i$ in the image of $\sigma_{a\otimes f}$. But since σ_a is surjective, we may choose $g_i \in G$ such that $\sigma_a(g_i) = h_i$ for all $i < \kappa$, and so $\sigma_{a\otimes f}(\sum_{i<\kappa} g_i \otimes e_i) = \sum_{i<\kappa} h_i \otimes fe_i$, as desired.

In combination, we have shown that $\Gamma_{b,a\otimes f}$ is a quasiendomorphism by Proposition 6.3.2, and $\Gamma_{b,a\otimes f} \in \mathcal{F}_F$. By Proposition 6.3.4, since $\sigma_{a\otimes f}$ has finite kernel, we know $\Gamma^0_{b,a\otimes f}$ has $\Gamma^0_{a\otimes f,b}$ as a right inverse if σ_b is surjective.

By Proposition 6.3.5, since σ_a is surjective and has finite kernel for all nonzero $a \in A$, each $\Gamma^0_{a,b}$ is a unit in $E^0[\digamma]$ for all nonzero $a, b \in A$. Similarly, the argument in the above paragraphs gives us that $\Gamma^0_{a\otimes 1, b\otimes 1}$ is an element of $E^0[\digamma_F]$ and moreover, a unit. We claim that for all nonzero $a, b \in A$, $(\Gamma^n_{a,b})^0 = 1$ if and only if $(\Gamma^n_{a\otimes 1,b\otimes 1})^0 = 1$. Note that $(\sum g_i \otimes e_i, \sum g'_i \otimes e_i) \in \Gamma_{a\otimes 1,b\otimes 1}$ if and only if $\sum \sigma_a(g_i) \otimes e_i = \sum \sigma_b(g'_i) \otimes e_i$. Since W is the direct sum of all the $H \otimes e_i$ for $i < \kappa$, this last condition is equivalent to $\sigma_a(g_i) = \sigma_b(g'_i)$ for all $i < \kappa$. In other words, for all $i < \kappa$, $(g_i, g'_i) \in \Gamma_{a,b}$. Iterating, we see (using Lemma 6.1.14) that for any $n \geq 1$:

$$
\begin{aligned}
(\Gamma^0_{a\otimes 1,b\otimes 1})^n &= (\Gamma^n_{a\otimes 1,b\otimes 1})^0 \\
&= \left\{ \left(\sum_{i=1}^{k} g_i \otimes e_i, \sum_{i=1}^{k} g'_i \otimes e_i \right) \in V \times V \,\middle|\, \forall i (g_i, g'_i) \in \Gamma^n_{a,b} \right\}^0
\end{aligned}
$$

One the one hand, by Lemma 6.1.3, if $(\Gamma^n_{a,b})^0 = 1$, then $\Gamma^n_{a,b} = \Delta_G + (\{0\} \times D)$, for the finite group $D = \Gamma^n_{a,b}(0)$. Under this assumption on n, we get

$$
\begin{aligned}
(\Gamma^0_{a\otimes 1,b\otimes 1})^n &= \left\{ \left(\sum_{i=1}^{k} g_i \otimes e_i, \sum_{i=1}^{k} g'_i \otimes e_i \right) \in V \times V \,\middle|\, \forall i (g_i, g'_i) \in \Gamma^n_{a,b} \right\}^0 \\
&= (\Delta_V + (\{0\} \times D_V))^0 \\
&= 1,
\end{aligned}
$$

where $D_V = \{\sum g_i \otimes e_i \in V \mid \forall i, g_i \in D\}$. Conversely, if $(\Gamma^0_{a\otimes 1,b\otimes 1})^n = 1$, then in particular, for every $\sum g_i \otimes e_i$, we must have $(g_i, g_i) \in \Gamma^n_{a,b}$ for all $1 \leq i \leq k$. Hence $\Gamma^n_{a,b} \geq 1$. Since $\Gamma^n_{a,b}$ is a quasiendomorphism because $\Gamma_{a,b}$ is, we apply Lemma 6.1.3 to see that $(\Gamma^n_{a,b})^0 = 1$. □

Proposition 6.3.4 automatically gives us many properties of $E^0[\digamma_F]$ on account of Lemma 6.3.9. This lemma indicates that behavior in $E^0[\digamma]$ at least partially embeds into $E^0[\digamma_F]$. As the next lemma shows, properties of F also embed nicely into $E^0[\digamma_F]$.

Lemma 6.3.10. *Same hypotheses as Lemma 6.3.9. Then the field F embeds into $E^0[\digamma_F] \subseteq E^0[\mathcal{A}_F]$. Specifically, we associate $f \in F$ with $\Gamma_{a\otimes f,a\otimes 1}$ for any nonzero $a \in A$ (they are all equal). Furthermore, under this embedding, F lands in the center of $E^0[\digamma_F]$.*

Proof. For any nonzero $a \in A$ and $f \in F$, consider $\Gamma^0_{a\otimes f,a\otimes 1}$, which is a quasiendomorphism that is a unit by Lemma 6.3.9. Hence, $\Gamma_{a\otimes f,a\otimes 1}$, being a finite extension of $\Gamma^0_{a\otimes f,a\otimes 1}$, is also a quasiendomorphism. Moreover,

$$\begin{aligned}\Gamma_{a\otimes f,a\otimes 1} &= \left\{\left(\sum_{i<\kappa} g_i\otimes e_i, \sum_{i<\kappa} h_i\otimes e_i\right) \middle| \sum_{i<\kappa}\sigma_a(g_i)\otimes fe_i = \sum_{i<\kappa}\sigma_a(h)\otimes e_i\right\}\\ &\supseteq \left\{\left(\sum_{i<\kappa} g_i\otimes e_i, \sum_{i<\kappa} g_i\otimes fe_i\right) \middle| \sum_{i<\kappa} g_i\otimes e_i\in V\right\},\end{aligned}$$

where the set inclusion follows by taking $h_i = g_i$ and using the bilinearity of the tensor and that σ_a is a homomorphism. This final set itself is clearly an endomorphism (again by the bilinearity of tensors), so by Lemma 6.1.3, this endomorphism has finite index in the quasiendomorphism $\Gamma_{a\otimes f,a\otimes 1}$. Therefore they both have the same connected component. Since G^0 is connected, any endomorphism on G is already connected. Thus:

$$\Gamma^0_{a\otimes f,a\otimes 1} = \left\{\left(\sum_{i<\kappa} g_i\otimes e_i, \sum_{i<\kappa} g_i\otimes fe_i\right) \middle| \sum_{i<\kappa} g_i\otimes e_i\in V\right\},$$

The nonzero a serves as a dummy variable (all we needed was that σ_a is surjective and has finite kernel, which we assume is true for all nonzero $a \in A$). So without ambiguity we can define a mapping $\chi : F \to E^0[\digamma_F]$ by $f \mapsto \Gamma^0_{a\otimes f,a\otimes 1}$ for any nonzero $a \in A$. Note that if $a \neq 0$, then χ is injective: if $\Gamma^0_{a\otimes f,a\otimes 1} = \Gamma^0_{a\otimes f',a\otimes 1}$, then $\sum_{i<\kappa} g_i \otimes fe_i = \sum_{i<\kappa} g_i\otimes f'e_i$ for all tuples $g_i \in G$. Taking a tuple which is nonzero only in the first coordinate, we get that $g\otimes fe_0 = g\otimes f'e_0$ so $f = f'$.

From the explicit expression we have of $\chi(f)$, we conclude that for $f, f' \in F$

$$\Gamma^0_{a\otimes f,a\otimes 1} *^0 \Gamma^0_{a\otimes f',a\otimes 1} = \left\{\left(\sum_{i<\kappa} g_i\otimes e_i, \sum_{i<\kappa} g_i\otimes ff'e_i\right) \middle| \sum_{i<\kappa} g_i\otimes e_i\in V\right\}^0 = \Gamma^0_{a\otimes ff',a\otimes 1}$$

so that $\chi(ff') = \chi(f) * \chi(f')$. In particular, since $\chi(1) = 1$ and $\ker(\sigma_{a\otimes 1})$ is finite (by Lemma 6.3.9), we see $(\Gamma^0_{a\otimes f,a\otimes 1})^k = \Gamma^0_{a\otimes f^k,a\otimes 1}$. Thus if $\mathrm{ord}_F(f)|k$, then $(\Gamma^0_{a\otimes f,a\otimes 1})^k = 1$, and injectivity of χ gives us the converse.

Additivity is easy:

$$\chi(f+f') = \Gamma^0_{a\otimes(f+f'),a\otimes 1} = \Gamma^0_{a\otimes f+a\otimes f',a\otimes 1} = \Gamma^0_{a\otimes f,a\otimes 1} + \Gamma^0_{a\otimes f'.a\otimes 1} = \chi(f)+\chi(f')$$

where the third equality comes from Proposition 6.3.4 and the surjectivity of $\sigma_{a\otimes 1}$ (Lemma 6.3.9). Therefore χ is an embedding of F into $E^0[\digamma_F]$.

Now we prove that any $f \in F$ commutes with any $\Gamma \in E^0[\digamma_F]$. If $f = 0$ this is true since $E^0[\digamma_F]$ is a ring. Assume $f \neq 0$. By the distributivity of multiplication in the ring $E^0[\digamma_F]$ and the linearity in the first index (Proposition 6.3.4), it suffices to show that $f *^0 \Gamma^0_{a\otimes\alpha,\sum_{i<\kappa} b_i\otimes e_i} = \Gamma^0_{a\otimes\alpha,\sum_{i<\kappa} b_i\otimes e_i} *^0 f$, and by Lemma 2.3.10, it suffices to show this equality without taking connected components. By definition of composition and our knowledge of f:

$$\begin{aligned}
&\left(\sum_{i<\kappa} g_i \otimes e_i, \sum_{i<\kappa} g_i' \otimes e_i\right) \in \Gamma_{a\otimes\alpha,\sum_{i<\kappa} b_i\otimes e_i} * f \\
\Leftrightarrow\ &\left(\sum_{i<\kappa} g_i \otimes e_i, \sum_{i<\kappa} g_i \otimes fe_i\right) \in f,\ \ \left(\sum_{i<\kappa} g_i \otimes fe_i, \sum_{i<\kappa} g_i' \otimes e_i\right) \in \Gamma_{a\otimes\alpha,\sum_{i<\kappa} b_i\otimes e_i} \\
\Leftrightarrow\ &\sum_{i<\kappa} \sigma_a(g_i) \otimes f\alpha e_i = \sum_{j<\kappa}\sum_{i<\kappa} \sigma_{b_j}(g_i') \otimes e_i e_j \\
\Leftrightarrow\ &\sum_{i<\kappa} \sigma_a(g_i) \otimes \alpha e_i = \sum_{j<\kappa}\sum_{i<\kappa} \sigma_{b_j}(g_i') \otimes f^{-1} e_i e_j \\
\Leftrightarrow\ &\left(\sum_{i<\kappa} g_i \otimes e_i, \sum_{i<\kappa} g_i' \otimes f^{-1} e_i\right) \in \Gamma_{a\otimes\alpha,\sum_{i<\kappa} b_i\otimes e_i} \\
\Leftrightarrow\ &\left(\sum_{i<\kappa} g_i \otimes e_i, \sum_{i<\kappa} g_i' \otimes e_i\right) \in f * \Gamma_{a\otimes\alpha,\sum_{i<\kappa} b_i\otimes e_i}
\end{aligned}$$

So we have shown that f commutes with all elements of $E^0[\digamma_F]$. □

We repeat that for $f \in F$, the nonzero $a \in A$ essentially acts as a dummy variable, so through an abuse of notation, we shall identify $\Gamma^0_{a\otimes f,a\otimes 1}$ with f in $E^0[\digamma_F]$.

Consider Lemma 6.3.7 in the context of $\aleph_0$-categoricity and stability. Any $\aleph_0$-categorical group has finite exponent, so if $A \neq 0$, we are forced into the case where A, G, and H are $\mathbb{F}_p$-vector spaces and our ring of endomorphisms has characteristic p. We know every element of the form $\Gamma_{b,a\otimes f}$, for $a \in A$ and $f \in F$ both nonzero, is a quasiendormophism (i.e. an element of $\digamma_F$. By Proposition 6.3.4, it has $\Gamma_{a\otimes f,b}$ as a right inverse if $\mathrm{im}(\sigma_b) = \mathrm{im}(\sigma_{a\otimes f})$, i.e. σ_b is surjective (Lemma 6.3.9). We would like to guarantee certain elements of this form are right invertible, so we will pay attention to the property for a fixed finite field F of characteristic p:

$\dagger_F$ There is a nonzero $a \in A$ such that for all but finitely many $b \in A$, for all $f \in F$, $\sigma_{a\otimes 1-b\otimes f}$ is surjective.

Since $\sigma_{a\otimes 1}$ is surjective (Lemma 6.3.9), $f = 0$ never poses a problem for $\dagger_F$. Nonzero elements of F are in bijection with a subgroup of $\mathrm{GL}_\kappa(\mathbb{F}_p)$, where $\kappa = \dim_{\mathbb{F}_p} F$ (because multiplication by a nonzero $f \in F$ is a change of basis). Since $V \cong G^\kappa$ and $W \cong H^\kappa$, we can think of $\sigma_{a\otimes 1 - b\otimes f}$ as the linear map $\sigma_a - M\sigma_b : G^\kappa \to H^\kappa$ (for $M \in \mathrm{GL}_\kappa(\mathbb{F}_p)$ corresponding to f) given by

$$(\sigma_a - M\sigma_b)\begin{bmatrix} g_1 \\ \vdots \\ g_\kappa \end{bmatrix} := \begin{bmatrix} \sigma_a(g_1) \\ \vdots \\ \sigma_a(g_\kappa) \end{bmatrix} - M\begin{bmatrix} \sigma_b(g_1) \\ \vdots \\ \sigma_b(g_\kappa) \end{bmatrix}$$

In this light, we can restate $\dagger_F$ in terms of linear maps:

$\dagger_F$ There is a nonzero $a \in A$ such that for all but finitely many $b \in A$, for all $M \in \mathrm{GL}_n(\mathbb{F}_p)$ corresponding to multiplication by a nonzero element of F, $\sigma_a - M\sigma_b : G^n \to H^n$ is surjective.

Conjecture 6.3.11. Assume we are in a stable, $\aleph_0$-categorical context and A, G, H, Σ have properties (1)-(5) of the beginning of this section and for all nonzero $a \in A$, σ_a is surjective and has finite kernel. Then $\dagger_F$ holds in this system.

We believe this conjecture to be true, but have been unable to verify it. All counterexamples we are aware of to $\dagger_F$ are in contexts (e.g. Ore rings) that are not stable and $\aleph_0$-categorical.

Under the assumption of $\dagger_F$, we may use the above tensor lemmas to conclude triviality of the entire structure in this context.

Theorem 6.3.12. *Let A, G and H be three $\mathbb{F}_p$-vector spaces interpretable in a stable, $\aleph_0$-categorical theory. Assume G and H are connected and nontrivial and that we have a definable subset $\Sigma \subseteq A \times G \times H$ satisfying:*

1. $\pi_1(\Sigma) = A$
2. *For all $a \in A$, $\sigma_a := \{(g,h) \in G \times H \mid (a,g,h) \in \Sigma\}$ is a homomorphism from all of G to H. We shall write σ_a functionally as $\sigma_a(g) = h$.*
3. *σ_0 is the zero map $0 : x \mapsto 0$,*
4. *For all $a, b \in A$ and $g \in G$, $\sigma_{a+b}(g) = \sigma_a(g) + \sigma_b(g)$.*
5. *if $a \neq 0$ then σ_a is surjective.*
6. *For all $a \in A$, if $a \neq 0$, then $\ker \sigma_a$ is finite.*

7. $\dagger_F$ holds for all finite fields F of characteristic p.

Then A is a finite-dimensional $\mathbb{F}_p$-vector space.

Proof. Assume A is nontrivial. Since we are working in a stable, $\aleph_0$-categorical context, we may take connected components of definable groups at will. For $a, b \in A$ with $b \neq 0$, define the additive relations $\Gamma^0_{a,b}$ of G as in the beginning of this section; since σ_a is surjective and has finite kernel for all nonzero $a \in A$, by Proposition 6.3.2 all the $\Gamma^0_{a,b}$ for $b \neq 0$ are quasiendomorphisms. They form a uniformly definable family $\mathcal{F}$ and the resulting ring of connected quasiendomorphisms $R = E^0[\mathcal{F}]$ has the properties listed in Proposition 6.3.5. In particular, each $\Gamma^0_{a,b}$ for nonzero $a, b \in A$ will be a unit.

Since we have an $\aleph_0$-categorical theory and each $(\Gamma^0_{a,b})^n$ is definable over a, b, we must have $(\Gamma^0_{a,b})^n = (\Gamma^0_{a,b})^m$ for some $n \neq m$. Since $\Gamma^0_{a,b}$ is a unit when $a \neq 0$, we have $(\Gamma^0_{a,b})^n = 1$ for some $n > 0$. Again, by $\aleph_0$-categoricity, there must be a uniform $n > 0$ such that $(\Gamma^0_{a,b})^n = 1$ for all $a, b \in A$ with $a \neq 0$. Pick the least such n.

Since $f = \Gamma^0_{fa,a}$ is a unit in $E^0[\mathcal{F}]$ whenever f is not a multiple of p, we must have $f^n = (\Gamma^0_{fa,a})^n = 1$. Yet $f \in \langle 1 \rangle_{E^0[\mathcal{F}]} \cong \mathbb{F}_p$, so we conclude that $p-1|n$. Hence n is not power of p. Let $n = kp^e$, where p does not divide k. Note $0 = (\Gamma^0_{a,b})^n - 1 = ((\Gamma^0_{a,b})^k - 1)^{p^e}$ since $\Gamma^0_{a,b}$ commutes with itself and elements of $\mathbb{F}_p$.

Let F be the splitting field of $x^k - 1$ over $\mathbb{F}_p$. Since p does not divide k, $x^k - 1$ is separable. Enumerate the distinct roots of $x^k - 1$ in F as $\omega_1, \ldots, \omega_k = 1$. Using Lemma 6.3.4, we can tensor with F over $\mathbb{F}_p$ to produce $V := G \otimes_{\mathbb{F}_p} F$, $W := H \otimes_{\mathbb{F}_p} F$, $B := A \otimes_{\mathbb{F}_p} F$, and a definable subset $\Sigma' \subseteq B \times V \times W$ which extends Σ (under ι_F). These B, V, W, Σ' will satisfy conditions (1)-(5) from the introduction of this section, so they produce a uniformly definable family of subgroups of $V \times V$, indexed by $B \times B \backslash \{0\}$. Let $\mathcal{A}_F$ be the additive relations and $\mathcal{F}_F$ be the quasiendomorphisms, which extends $\mathcal{A}$ and $\mathcal{F}$, by the identification of $\Gamma^0_{a,b}$ with $\Gamma^0_{a\otimes 1, b\otimes 1}$ as justified in Lemma 6.3.9. Also by Lemma 6.3.9, for each nonzero $a, b \in A$, $\Gamma^0_{a\otimes 1, b\otimes 1}$ must be a unit of order equal to the order of $\Gamma^0_{a,b}$, and hence this order divides n. So, for each nonzero $a, b \in A$,

$$\begin{aligned} 0 &= (\Gamma^0_{a\otimes 1, b\otimes 1})^n - 1 \\ &= (\Gamma^0_{a\otimes 1, b\otimes 1})^{kp^e} - 1 \\ &= \left((\Gamma^0_{a\otimes 1, b\otimes 1})^k - 1\right)^{p^e} \end{aligned}$$

where, again, there is no issue about noncommutativity of multiplication since $\Gamma^0_{a\otimes 1,b\otimes 1}$ commutes with itself and elements of $\mathbb{F}_p$.

Since F embeds into the center of $E^0[\mathcal{F}_F]$ by Lemma 6.3.10, the polynomial $x^k - 1$ factors over $E^0[\mathcal{F}_F]$ as $\prod_{i=1}^k (x-\omega_i)$. There is no ambiguity caused by noncommutativity since F is in the center of $E^0[\mathcal{F}_F]$. When we evaluate this polynomial at $x = \Gamma^0_{a\otimes 1,b\otimes 1}$ (an element of $\mathcal{F}_F$ when $a \neq 0$ by Lemma 6.3.9), we obtain:

$$\begin{aligned}
(\Gamma^0_{a\otimes 1,b\otimes 1})^k -^0 1 &= \prod_{i=1}^{k} (\Gamma^0_{a\otimes 1,b\otimes 1} -^0 \omega_i) \\
&= \prod_{i=1}^{k} (\Gamma^0_{a\otimes 1,b\otimes 1} -^0 \Gamma^0_{b\otimes\omega_i,b\otimes 1}) \\
&= \prod_{i=1}^{k} \Gamma^0_{a\otimes 1-b\otimes\omega_i,\, b\otimes 1}
\end{aligned}$$

The second equality above used Lemma 6.3.10, while the third used Lemma 6.3.3 for dealing with $-^0$ and Lemma 6.3.4 for adding left indices. Recall that in order to use Lemma 6.3.4, we need to know that V, W, B, Σ meet the qualifications of the lemma (which is the case by Lemma 6.3.8) and that $\mathrm{im}(\sigma_{b\otimes 1}) \supseteq \mathrm{im}(\sigma_{a\otimes 1})$ (which is true by Lemma 6.3.9 since $\sigma_{b\otimes 1}$ is surjective and has finite kernel by Lemma 6.3.9).

By Lemma 6.3.4, if $a\otimes 1 - b\otimes\omega_i \neq 0$, then $\Gamma^0_{a\otimes 1-b\otimes\omega_i,b\otimes 1}$ has a right inverse if $\sigma_{a\otimes 1-b\otimes\omega_i}$ is surjective.

We now employ our assumption of $\dagger_F$. Choose $a \in A$ a witness to this property; let $A_0 \subseteq A$ be the finite set of elements $b \in A$ for which there is an $f \in F$ with $\sigma_{a\otimes 1-b\otimes f}$ not surjective. For any $b \in A\backslash A_0$, we have $\sigma_{a\otimes 1-b\otimes\omega_i}$ is surjective for every $1 \leq i \leq k$. So each $\Gamma^0_{a\otimes 1-b\otimes\omega_i,b\otimes 1}$ is right invertible and thus so long as $b \notin A_0$, the element $(\Gamma^0_{a\otimes 1,b\otimes 1})^k - 1$ must be a product of right-invertible elements.

Combining these calculations, we see that for our special $a \in A$, forall $b \notin A_0 \cup \{0\}$, we have

$$\begin{aligned}
0 &= \left((\Gamma^0_{a\otimes 1,b\otimes 1})^k - 1\right)^{p^e} \\
&= \left(\prod_{i=0}^{k-1} \Gamma^0_{a\otimes 1-b\otimes\omega_i,b\otimes 1}\right)^{p^e}
\end{aligned}$$

The right hand side is a product of right-invertible elements in $E^0[\mathcal{A}_F]$, while the left hand side is zero. This is impossible since $0 \neq 1$ in $E^0[\mathcal{A}_F]$. Consequently $A = A_0$ is finite. □

Remark 6.3.13. Note that the proof above does not use stability in any way other than to obtain connected components, although we anticipate that stability will come into play to show $\dagger_F$ holds.

Theorem 6.3.12 states that A (and hence $R = E^0[F]$) must be finite. Before initiating the analysis of that theorem's proof, we can see no reason *a priori* why such a quasiendomorphism ring should be definable. If we were able to conclude definability right from the start, then stability and $\aleph_0$-categoricity would aid us in obtaining finiteness (by using Proposition 2.2.1 to obtain a field and Proposition 2.1 to conclude it is finite). Nor do we see *a priori* a reason for R to be an integral domain. If it were, then by $\aleph_0$-categoricity we would obtain for each nonzero $z \in R$ that $z^n = z^m$ for some $n > m$, and hence $z^{n-m} = 1$. Since finite subsets generate finite subrings by $\aleph_0$-categoricity, we may use Wedderburn's Little Theorem to conclude that R is a field. Then $\aleph_0$-categoricity would again force it to be finite by Proposition 2.1. Therefore, even though there are several more typical avenues of proof for concluding that such a ring be finite, in this case it seems that the above argument involving tensors is necessary to untangle the underlying structure of the quasiendomorphism ring.

We remark that such a theorem about quasiendomorphism rings is potentially very useful as the clinching step in a proof of the BCM Conjecture. Indeed, when Baur, Cherlin, and Macintyre proved that $\aleph_0$-categorical groups of finite Morley rank were abelian by finite (Thm 1.1), they concluded the argument with a minimal counterexample G where $G' = [a_1, G] + \ldots + [a_n, G]$ for some $a_1, \ldots, a_n \in G$. One could then quotient G by $[a_2, G] + \ldots + [a_n, G]$ to obtain a new group G whose commutator is $[a, G]$ for some $a \in A$. If we could circumvent the use of finite Morley rank and further guarantee (as Baur, Cherlin and Macintyre do) that $[b, G] = [a, G]$ for all $a, b \notin Z(G)$, then the corollary below explicitly shows how the above theorem about quasiendomorphism rings would finish a proof by contradiction of the BCM Conjecture. Even beyond these considerations, the corollary below can be applied to some situations which we have already described in Chapter 5.

Corollary 6.3.14. *Suppose G is a $\aleph_0$-categorical, stable group of nilpotence class at most 2. Suppose A and B are two definable subgroups, where*

1. *B is connected,*
2. *for all $a, b \in A \backslash C(B)$, $[a, B] = [b, B]$,*

3. *for all* $a \in A \backslash C(B)$*,* $(C_G(a) \cap B)/(C(A) \cap B)$ *is finite, and*

4. $\dagger_F$ *holds on the commutator maps* $[a, \cdot]$ *for* $a \in A$ *and for all finite fields* F *of characteristic* p*.*

Then $B \subseteq C(A)$ *or* $A/(A \cap C(B))$ *is finite.*

Proof. Assume $B \not\subseteq C(A)$ and $A \backslash C(B)$ is nonempty. Set $H = [x, B]$ for some $x \in A \backslash C(B)$. H is connected by Proposition 2.3.8 since it is the definable image of a connected group. By the same proposition, $B/(C(A) \cap B)$ is a connected group. For each $\overline{a} \in A/(A \cap C(B))$, we have a homomorphism $\sigma_{\overline{a}} : B/(C(A) \cap B) \to H$ given by $\overline{b} \mapsto [a, b]$ for any representatives a of $\overline{a}$ and b of $\overline{b}$. This is well-defined since the restricted commutator map $[\cdot, \cdot] : A \times B \to H$ does not distinguish elements of A equivalent modulo $C(B)$, nor elements of B equivalent modulo $C(A)$. Note that $\sigma_{\overline{a}} \equiv 0$ if and only if $a \in C_G(B)$ for any representative a of $\overline{a}$, i.e. if and only if $\overline{a} = 0$. In all other cases, $\sigma_{\overline{a}}$ maps surjectively onto H by the second hypothesis. Set $\Sigma = \{(\overline{a}, \overline{g}, \sigma_{\overline{a}}(\overline{g}) \,|\, \overline{a} \in A/(A \cap C(B)), \, \overline{g} \in B/(B \cap C(A))\}$. By the bilinearity of $[\cdot, \cdot]$ in a group of nilpotence class 2, the system $A/(A \cap C(B)), B/(B \cap C(A)), H, \Sigma$ satisfies the hypotheses of Theorem 6.3.12, where $\dagger_F$ is interpreted in terms of these maps. So $A/(A \cap C(B))$ is finite. □

Corollary 6.3.15. *Let* G *be a counterexample with no peaks given by Theorem 5.3.1. Assume* $\dagger_F$ *holds for the commutator maps* $[g, \cdot]$ *for* $g \in G$ *and for all finite fields* F *of characteristic* p*. Then for any* $a \in G$*, there are only finitely many* $b \in G$ *distinct modulo* $Z(G)$ *such that* $[a, G] \cap [b, G]$ *is infinite.*

Proof. Given $a \in G$, the set $A_a = \{b \in G \,|\, [b, G] \cap [a, G] \text{ is infinite}\}$ is an a-definable set by $\aleph_0$-categoricity. In fact, by Theorem 5.3.1 $A_a = Z(G) \cup \{b \in G \,|\, [b, G] = [a, G]\}$ and thus is a group. If $A_a = Z(G)$, we are done, so assume $A_a \supsetneq Z(G)$. Since we are in the no peaks case, $C(x)/Z(G)$ is finite for all $x \notin Z(G)$. So we may apply the Corollary 6.3.14 with $A = A_a$ and $B = G$ and conclude that $A_a/(A \cap C(G)) = A_a/Z(G)$ is finite. □

Bibliography

[Bau96a] Andreas Baudisch, *Another stable group*, Ann. Pure Appl. Logic **80** (1996), no. 2, 109–138.

[Bau96b] ______, *A new uncountably categorical group*, Trans. Amer. Math. Soc. **348** (1996), no. 10, 3889–3940.

[Bau00] ______, *Closures in $\aleph_0$-categorical bilinear maps*, J. Symbolic Logic **65** (2000), no. 2, 914–922.

[BCM79] Walter Baur, Gregory Cherlin, and Angus Macintyre, *Totally categorical groups and rings*, J. Algebra **57** (1979), no. 2, 407–440.

[BR77] John T. Baldwin and Bruce Rose, *$\aleph_0$-categoricity and stability of rings*, J. Algebra **45** (1977), no. 1, 1–16.

[BS76] J. T. Baldwin and Jan Saxl, *Logical stability in group theory*, J. Austral. Math. Soc. Ser. A **21** (1976), no. 3, 267–276.

[Che79] Gregory Cherlin, *Groups of small Morley rank*, Ann. Math. Logic **17** (1979), no. 1-2, 1–28.

[CHL85] G. Cherlin, L. Harrington, and A. H. Lachlan, *$\aleph_0$-categorical, $\aleph_0$-stable structures*, Ann. Pure Appl. Logic **28** (1985), no. 2, 103–135.

[CK90] C. C. Chang and H. J. Keisler, *Model theory*, third ed., Studies in Logic and the Foundations of Mathematics, vol. 73, North-Holland Publishing Co., Amsterdam, 1990.

[CR76] Gregory L. Cherlin and Joachim Reineke, *Categoricity and stability of commutative rings*, Ann. Math. Logic **9** (1976), no. 4, 367–399.

[EW00] David M. Evans and Frank O. Wagner, *Supersimple ω-categorical groups and theories*, J. Symbolic Logic **65** (2000), no. 2, 767–776.

[Fel78] Ulrich Felgner, *$\aleph_0$-categorical stable groups*, Math. Z. **160** (1978), no. 1, 27–49.

[Fel75] ______, *$\aleph_1$-Kategorische Theorien nicht-kommutativer Ringe*, Fund. Math. **82** (1974/75), 331–346, Collection of articles dedicated to Andrzej Mostowski on the occasion of his sixtieth birthday, VIII.

[Hal59] Marshall Hall, Jr., *The theory of groups*, The Macmillan Co., New York, N.Y., 1959.

[Her68] I. N. Herstein, *Noncommutative rings*, The Carus Mathematical Monographs, No. 15, Published by The Mathematical Association of America, 1968.

[Her69] ______, *Topics in ring theory*, The University of Chicago Press, Chicago, Ill.-London, 1969.

[Hod97] Wilfrid Hodges, *A shorter model theory*, Cambridge University Press, Cambridge, 1997.

[Hru86] Ehud Hrushovski, *Contributions to stable model theory*, Ph.D. thesis, University of California, Berkeley, 1986.

[Hru89] ______, *A stable ω-categorical pseudoplane*, preprint, 1989.

[Hru93] ______, *A new strongly minimal set*, Ann. Pure Appl. Logic **62** (1993), no. 2, 147–166, Stability in model theory, III (Trento, 1991).

[KW73] Otto H. Kegel and Bertram A. F. Wehrfritz, *Locally finite groups*, North-Holland Publishing Co., Amsterdam, 1973, North-Holland Mathematical Library, Vol. 3.

[KW06] Krzysztof Krupiński and Frank Wagner, *Small profinite groups and rings*, J. Algebra **306** (2006), no. 2, 494–506.

[Lac74] A. H. Lachlan, *Two conjectures regarding the stability of ω-categorical theories*, Fund. Math. **81** (1973/74), no. 2, 133–145, Collection of articles dedicated to Andrzej Mostowski on the occasion of his sixtieth birthday, II.

[Lam01] T. Y. Lam, *A first course in noncommutative rings*, second ed., Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 2001.

[Mac88] H. D. Macpherson, *Absolutely ubiquitous structures and $\aleph_0$-categorical groups*, Quart. J. Math. Oxford Ser. (2) **39** (1988), no. 156, 483–500.

[New96] Ludomir Newelski, *m-rank and meager groups*, Fund. Math. **150** (1996), no. 2, 149–171.

[New02] ———, *Small profinite structures*, Trans. Amer. Math. Soc. **354** (2002), no. 3, 925–943 (electronic).

[Poi81] Bruno Poizat, *Sous-groupes définissables d'un groupe stable*, J. Symbolic Logic **46** (1981), no. 1, 137–146.

[Poi01] ———, *Stable groups*, Mathematical Surveys and Monographs, vol. 87, American Mathematical Society, Providence, RI, 2001, Translated from the 1987 French original by Moses Gabriel Klein.

[PS98] Ya'acov Peterzil and Sergei Starchenko, *A trichotomy theorem for o-minimal structures*, Proc. London Math. Soc. (3) **77** (1998), no. 3, 481–523.

[Sab75a] Gabriel Sabbagh, *Catégoricité en $\aleph_0$ et stabilité: constructions les préservant et conditions de chaîne*, C. R. Acad. Sci. Paris Sér. A-B **280** (1975), A531–A533.

[Sab75b] ———, *Catégoricité et stabilité: quelques exemples parmi les groupes et anneaux*, C. R. Acad. Sci. Paris. Sér. A-B **280** (1975), A603–A606.

[Wag94] Frank O. Wagner, *Relational structures and dimensions*, Automorphisms of first-order structures, Oxford Sci. Publ., Oxford Univ. Press, New York, 1994, pp. 153–180.

[Wag97] ———, *Stable groups*, London Mathematical Society Lecture Note Series, vol. 240, Cambridge University Press, Cambridge, 1997.

[Wag03] ———, *Small profinite m-stable-groups*, Fund. Math. **176** (2003), no. 2, 181–191.

[Wag06] ———, personal communication, 2005 - 2006.

[Zil93] Boris Zilber, *Uncountably categorical theories*, Translations of Mathematical Monographs, vol. 117, American Mathematical Society, Providence, RI, 1993, Translated from the Russian by D. Louvish.