Recurrence in Algebraic Dynamics

by

Ehsaan Hossain

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Pure Mathematics

Waterloo, Ontario, Canada

© Ehsaan Hossain 2020

Examining Committee Membership

The following served on the Examining Committee for this thesis. The decision of the Examining Committee is by majority vote.

External Examiner	Joseph Silverman Professor Department of Mathematics Brown University
Supervisor	Jason Bell Professor Department of Pure Mathematics University of Waterloo
Internal Members	David McKinnon Professor Department of Pure Mathematics University of Waterloo
	Matthew Satriano Assistant Professor Department of Pure Mathematics University of Waterloo
Internal-External Member	Christopher Godsil Professor Emeritus Department of Combinatorics & Optimization University of Waterloo

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

The original contributions contained in this thesis are:

- Theorem 1.2.21(b);
- all of the results of Subsections 1.3.3 – 1.3.4;
- all of the results of Section 2.3;
- and all of the results of Chapter 3.

The entirety of Chapter 3 is coauthored work with Jason Bell and Shaoshi Chen, and is largely obtained from the preprint (available at `arXiv:2005.04281`).

I understand that my thesis may be made electronically available to the public.

Abstract

Let $\varphi : X \dashrightarrow X$ is a rational mapping of an algebraic variety X defined over $\mathbb{C}$. The *orbit* of a point $x \in X$ is the sequence $\{x, \varphi(x), \varphi^2(x), \ldots\}$. Our basic question is: how often does this orbit intersect a given closed set C? Thus we are interested in the *return set*

$$E := \{n \geq 0 : \varphi^n(x) \in C\}.$$

Is it possible for E to be the set of primes? Or the set of perfect squares? The *Dynamical Mordell–Lang Conjecture* (DML) says no: it asserts that E is infinite only when it contains an infinite arithmetic progression. Geometrically, if the orbit intersects C infinitely often, then in fact this intersection must occur periodically.

Although the DML Conjecture remains open in general, an elegant approach of Bell–Ghioca–Tucker obtains this periodicity when E is a set of *positive density*. In this thesis, our first result is the generalization of the Bell–Ghioca–Tucker Theorem to the action of an amenable semigroup on an algebraic variety (these are the semigroups in which "density" can be naturally defined). We also use ultrafilters to provide a combinatorial version for arbitrary semigroups; as a simple example, our result shows that the set E cannot be equal to the ternary automatic set $\{n \in \mathbb{N} : [n]_3 \text{ has no 2's}\}$. Second, in joint work with Bell and Chen, we investigate dynamical sequences of the form $u_n = f(\varphi^n(x))$, where $f : X \dashrightarrow K$ is a rational function; we obtain several DML-type conclusions for this sequence, consequently recovering classical combinatorial theorems of Bézivin, Methfessel, and Polyá. Third, an investigation of other types of noetherian algebraic objects leads us to polycyclic-by-finite groups, and we prove an analogue of the Bell–Ghioca–Tucker Theorem for an automorphism of such a group.

Acknowledgments

Thank you Jason for your infinite patience and commitment over the past seven years in Waterloo. You have stayed patient with me as I tried and failed various projects, and you were always on the lookout for my success and best interests — even when I wasn't looking out for myself. Thank you for the tacos, pizza, and fried chicken; for the collaborative memes; for the oat milk cookie lattes; for recommending The Wire; for the academic and personal advice; for the pep talks; for being a down-to-earth advisor.

I'm grateful to my committee members — Chris Godsil, David McKinnon, Matt Satriano, and Joseph Silverman — for reading my thesis and suggesting helpful ideas and corrections. I'm also grateful to Shaoshi Chen, who coauthored the joint work included in Chapter 3 of this thesis.

I'm lucky to have had many great academic mentors over the years. Ruxandra advised me during my undergrad days, and was always there to offer a confidence boost when I needed it. Ty invited me for my first seminar talk, and in the following years, Chris Schafhauser and Adam Dor-On helped me organize many successful algebra seminars. When I taught my first course, Ross gave me crucial advice in structuring my lectures and problem sets. During the job season, Brian and Carmen offered me tons of advice on teaching and career-building, and they warmly welcomed me to their teaching seminars and the field of mathematical pedagogy. When I was working on multivariable dynamical systems, Matt Kennedy pointed me towards interesting reading in ultrafilters and Ramsey theory. I am incredibly grateful for all the guidance I have received from these people, and it is my mission to pay it forward to my future students.

Brett, Chadi, Carlos, Dan, Hongdi, Mani, Pat, Ragini, Shubham, Zack — my friends and colleagues in the pure math department have offered limitless encouragement and friendship over the past six years. Thanks for everything from cold samosas at C&D to drinks at the grad house. Our departmental administrators: Jackie, Lis, El Pavio, Nan — you're always there for us in a pinch. How many times have I locked myself out of my office? And a big thanks to Kismet Restaurant for the satisfying meals over the years, to the point that "Wanna get lunch?" has become synonymous with "We're going to Kismet." This thesis is fueled by spicy lamb biryani with a side of raita.

Arthur, Drew, Kerry, and Nick — thank you for helping me get back up every time I slipped. Your patience through the years means more to me than I can articulate. Thank you for the amazing home-cooked meals, the horror movies, listening to me rant about video games, sharing the stresses of grad school, and of course all the late nights doing math.

Thank you to my parents and siblings, whose pillars of support have always there been when I needed it. Not everyone is fortunate enough to have such a reliable family, and I am very grateful for that.

Davin, you've been stuck with me for years now, and you have accepted this adverse fate with grace. You've seen me at my highest and lowest points. You elevate me as often as you can. I'm lucky to be growing alongside such a caring partner, and Zoe and Maisy could not have a better mom. Thank you.

Dedication

For my two tuttis.

Contents

Chapter 1

Return Sets in Noetherian Spaces

A classic theorem of Skolem–Mahler–Lech [Lec53] states that if a linear recurrence over $\mathbb{C}$ has infinitely many zeros, then in fact its zeros occur periodically. More specifically, they obtain the structure of the zero set:

Theorem 1.0.1 (Skolem–Mahler–Lech [Lec53])**.** *Let $(a_n)_{n\geq 0}$ be a linear recurrence over a field K of characteristic zero, and let $Z(a_n)$ be the zero set:*

$$Z(a_n) := \{n \geq 0 : a_n = 0\}.$$

Then $Z(a_n)$ is a finite union of arithmetic progressions[1].

Linear recurrences are fundamentally dynamical objects, in the sense that they can be interpolated by linear maps. Given a linear recurrence (a_n) of order d, we can build a $d \times d$ matrix $A \in M_d(\mathbb{C})$ and a vector $v \in \mathbb{C}^d$ such that a_n is the equal to the dth coordinate of $A^n v$ for all $n \geq 0$. For example, the Fibonacci sequence $f_{n+1} = f_n + f_{n-1}$ satisfies

$$\begin{bmatrix} f_{n+1} \\ f_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} f_n \\ f_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n \begin{bmatrix} f_1 \\ f_0 \end{bmatrix} \quad \text{for all } n \geq 0.$$

Thus if $W := \{x \in V : e_d^T x = 0\}$ is the subspace of $\mathbb{C}^d$ consisting of those vectors whose dth coordinate is zero, then the zero set of (a_n) is equal to the following dynamical "return set":

$$\{n \geq 0 : A^n v \in W\}.$$

Think of this as the set of times when the orbit $\{v, Av, A^2v, \ldots\}$ intersects the subspace W. In fact, this is sometimes called the set of *return times*.

Let us introduce notation to generalize this dynamical phenomenon. Given a function $\varphi : X \to X$ on a set X, the **return set** of the φ-orbit of a point $x \in X$ to a subset $C \subseteq X$ is defined as

$$\mathrm{Ret}_\varphi(x, C) := \{n \geq 0 : \varphi^n(x) \in C\}.$$

Thus a dynamical version of the Skolem–Mahler–Lech Theorem may be formulated as follows.

[1]An **arithmetic progression** is a set of the form $\{a, a+b, a+2b, \ldots\}$ where a, b are nonnegative integers. A singleton is an arithmetic progression with $b = 0$.

Theorem 1.0.2. *Let $\varphi : \mathbb{C}^d \to \mathbb{C}^d$ be a linear mapping, let $v \in \mathbb{C}^d$ be a vector, and let $W \subseteq \mathbb{C}^d$ be a subspace. Then the return set $\mathrm{Ret}_\varphi(v, W)$ is a finite union of arithmetic progressions.*

Nonlinear versions of this classical theorem have since been studied; for example, when φ is a polynomial automorphism of the affine space K^d over a field K of characteristic zero [Bell]. Replacing the matrix $A : K^d \to K^d$ with a polynomial mapping $\varphi : X \to X$ of an algebraic variety X, we are lead to the following nonlinear generalization of the Skolem–Mahler–Lech Theorem.

Conjecture 1.0.3 (Dynamical Mordell–Lang Conjecture [Den94, GT])**.** *Let $\varphi : X \to X$ be an endomorphism of an algebraic variety X defined over a field K of characteristic zero. For a point $x \in X$ and a subvariety $C \subseteq X$, define the return set*

$$\mathrm{Ret}_\varphi(x, C) := \{n \geq 0 : \varphi^n(x) \in C\}.$$

Then $\mathrm{Ret}_\varphi(x, C)$ is a finite union of arithmetic progressions.

Geometrically, the DML Conjecture states that if an orbit intersects a subvariety infinitely often, then in fact the intersection must occur periodically. A slogan for this heuristic is thus:

Infinite recurrence implies periodic recurrence.

The original motivation for the DML Conjecture was its analogy with the original Mordell–Lang Conjecture, now Faltings's Theorem [Fal]; indeed, the DML Conjecture recovers the cyclic case of its classical counterpart.

The DML Conjecture has enjoyed resolutions in the cases when φ is an étale morphism [BGT10], or more recently, when $X = \mathbb{A}^2$ [Xie]; see [BGT16] for a history of this problem, including more cases where the DML Conjecture has been resolved. But the DML Conjecture still remains open in general. This thesis is largely motivated by the following "weak" DML Theorem due to Bell–Ghioca–Tucker [BGT15].

Theorem 1.0.4 (Bell–Ghioca–Tucker [BGT15])**.** *Let (X, φ, x, C) be as in the Dynamical Mordell–Lang Conjecture. Then the return set $\mathrm{Ret}_\varphi(x, C)$ is a finite union of arithmetic progressions and a set of* zero Banach density*.*

Here the **Banach density** of a set $E \subseteq \mathbb{N}$ is defined to be the limiting proportion of elements of E among increasingly large intervals I in $\mathbb{N}$:

$$\delta(E) := \limsup_{|I| \to \infty} \frac{|E \cap I|}{|I|}.$$

For example, the set of even numbers has Banach density $1/2$, while the set of prime numbers has density 0. Thus the Bell–Ghioca–Tucker Theorem gives the following "weakened" version of the Dynamical Mordell–Lang mantra:

"Large" recurrence implies periodic recurrence.

Here "large" refers to a return set of positive density. The Bell–Ghioca–Tucker Theorem implies, for example, the geometric fact that a polynomial orbit cannot intersect a subvariety exactly on prime time steps. Notably, their result only uses the fact that φ is a continuous mapping of a *noetherian* space, in particular it works over any field, whereas the DML Conjecture is easily seen to be false in positive characteristic [Lec53].

Our goal in Chapter 1 is to reinforce the mantra of "large recurrence implies periodic recurrence" in two ways, while simultaneously generalizing the action of a single map φ to a semigroup of mappings.

First, we generalize the Bell–Ghioca–Tucker Theorem to the case of multiple commuting mappings, using a suitable density function on $\mathbb{N}^d$. In fact we obtain a very general version for an *amenable* semigroup acting rationally on an algebraic variety, where the Banach density is replaced by an "invariant mean". This is Theorem 1.3.11. Although invariant means are not tractable objects — they are constructed using ultrafilters — we prove that when a set has positive density with respect to a "Følner net", then it is also supported by an invariant mean (Theorem 1.2.21(b)); this is useful because checking Følner density is a much more practical criterion. The general theory of Følner densities and amenability is detailed in section 1.2.

Second, we investigate what happens when the return set is "large" in the following combinatorial sense: a set $E \subseteq \mathbb{N}$ is called an *IP set* if there is a sequence $(s_n)_{n\geq 0}$ of natural numbers such that E contains every finite sum $s_{n_1}+\cdots+s_{n_k}$ with distinct indices $n_1,\ldots,n_k$. For example, the following set is an IP set with $s_n = 3^n$:

$$T := \{3^{n_1}+\cdots+3^{n_k} : n_1 < \cdots < n_k\} = \{n \geq 1 : [n]_3 \text{ has no 2's}\}.$$

Is T equal to a return set in some algebraic dynamical system? Since has zero density, the Bell–Ghioca–Tucker Theorem does not apply here. But a classic theorem of Hindman–Galvin–Glazer [HS] uses ultrafilters to show that every IP set is supported by a suitable measure on $\mathbb{N}$. Thus we prove a combinatorial version of the Bell–Ghioca–Tucker Theorem: if the return set $\mathrm{Ret}_\varphi(x, C)$ is an IP set, then it must contain an infinite arithmetic progression. Our result thus reinforces the theme that "large" recurrence implies periodic recurrence, widening the meaning of the word "large" to include the class of IP sets. This is Theorem 1.3.6, and the general theory behind IP sets is detailed in section 1.1.

1.1 IP Sets

In this section, we study "combinatorially large" subsets of $\mathbb{N}$ and other semigroups. An obvious example is the set $2\mathbb{N}$ of even integers: it is "large" because it takes up half of all positive integers (vaguely speaking), so we say its *density* is 0.5. We will make this precise in section 1.2. A more interesting example — and one we will keep in the back of our minds throughout this section — is the set of all positive integers whose ternary expansion has no 2's.

$$T := \{3^{n_1}+\cdots+3^{n_k} : 1 \leq n_1 < \cdots < n_k\}.$$

Although this set has *zero density*, it can still be considered "large" from a combinatorial standpoint, because it contains all possible sums of distinct terms in the sequence $1, 3, 9, 27, \ldots, 3^n, \ldots$.

The set T is an example of an *IP set* (this abbreviation will be explained in Section 1.1.4). In this section we focus on defining the class of *IP sets* by way of ultrafilters; while this definition is abstract, we also provide a concrete combinatorial characterization of IP sets due to Hindman, supplemented with an ultrafilter-theoretic proof due to Galvin–Glazer. We show how algebraic and topological properties of the Stone–Čech compactification correspond to combinatorial properties of IP sets.

The material in this section is expository, and can be found in [HS, Berg03].

1.1.1 Ultrafilters

The Stone–Čech compactification of a set X is a compact Hausdorff space βX containing X as a dense subspace; the elements of βX are the ultrafilters on X. If G is a semigroup, then βG is also a semigroup by convolution. The idempotent elements of βG give rise to a class of "large" subsets of X, called IP sets, which we will use later in our study of dynamical systems. In this subsection we give a standard treatment of βX, closely following [Berg03] and [HS].

Let X be a set and let $\mathcal{P}(X) = \{0,1\}^X$ denote the power set. A (proper) **filter** on X is a nonempty collection $p \subseteq \mathcal{P}(X)$ of subsets of X with the following three properties:

(i) [upper-closure] If $A \in p$ and $A \subseteq B \subseteq X$, then $B \in p$.

(ii) [intersection-closure] If $A, B \in p$, then $A \cap B \in p$.

(iii) [properness] $\varnothing \notin p$. (In light of (i), this is equivalent to $p \subsetneq \mathcal{P}(X)$.)

Examples of filters include the principal filter $\delta_{A_0} := \{A \subseteq X : A \subseteq A_0\}$ where $A_0 \subseteq X$, the trivial filter $\{X\}$, the collection $\{A \subseteq X : X \setminus A \text{ is finite}\}$ of all cofinite sets (provided X is infinite), and the collection of neighborhoods of a point in a topological space.

To generate other filters: one can attempt to start with any collection of subsets of X, close downward under finite intersections, then close upward under supersets. But the resulting "filter" may not be proper. To fix this, we use the *finite intersection property*.

Lemma 1.1.1. *Let X be a set, and let $\mathcal{A}$ be a family of subsets of X with the* **finite intersection property***: the intersection $A_{\mathcal{F}} := \bigcap_{A \in \mathcal{F}} A$ is nonempty for all finite subfamilies $\mathcal{F} \subseteq \mathcal{A}$. Then*

$$p_{\mathcal{A}} := \{A \subseteq X : A \supseteq A_{\mathcal{F}} \text{ for some finite } \mathcal{F} \subseteq \mathcal{A}\}$$

is a filter. In fact, $p_{\mathcal{A}}$ is the smallest filter containing $\mathcal{A}$.

Proof. If $A \in \mathcal{P}(X)$ contains a finite intersection $A_{\mathcal{F}}$, then any superset of A contains the same $A_{\mathcal{F}}$; thus $p_{\mathcal{A}}$ is upper-closed. If additionally $B \in \mathcal{P}(X)$ contains a finite intersection $A_{\mathcal{G}}$, then $A \cap B$ contains the finite intersection $A_{\mathcal{F}} \cap A_{\mathcal{G}} = A_{\mathcal{F} \cup \mathcal{G}}$; thus $p_{\mathcal{A}}$ is intersection-closed. Finally, if $\varnothing \in p_{\mathcal{A}}$ then $A_{\mathcal{F}} = \varnothing$ for some finite collection $\mathcal{F} \subseteq \mathcal{A}$, contradicting the finite intersection property; thus $\varnothing \notin p_{\mathcal{A}}$ and $p_{\mathcal{A}}$ is proper. Therefore $p_{\mathcal{A}}$ is a filter.

If p is another filter containing $\mathcal{A}$, then by upper- and intersection-closure, p must contain every finite intersection $A_{\mathcal{F}}$ with $\mathcal{F} \subseteq I$. But then $p \supseteq p_{\mathcal{A}}$, which proves that $p_{\mathcal{A}}$ is the *smallest* filter containing $\mathcal{A}$. □

An **ultrafilter** on X is a filter which is inclusion-maximal among all filters on X; a straightforward Zorn's Lemma argument shows that every filter is contained in an ultrafilter. Below are some characterizations of this definition.

Proposition 1.1.2. *The following are equivalent for a filter p on a set X:*

(a) *p is an ultrafilter.*

(b) *If $A \subseteq X$, then either $A \in p$ or $X \setminus A \in p$.*

(c) *If $A \cup B \in p$, then $A \in p$ or $B \in p$.*

Proof. "(a) $\implies$ (b)": Let $A \subseteq X$, and suppose that neither A nor its complement $A^{\complement} := X \setminus A$ are in p; we must show that p is properly contained in another filter q. Indeed, define a filter q by

$$q := \{Q \subseteq X : Q \text{ contains a set of the form } P \cap A \text{ for some } P \in p\}.$$

Notice p is properly contained in q: indeed any $P \in p$ contains $P \cap A$ so that $P \in q$; on the other hand, $A \in q \setminus p$. So it remains to check that q is a filter.

(i) Let $Q \in q$ so that $Q \supseteq P \cap A$ for some $P \in p$. Then any superset of Q also contains $P \cap A$. So q is upper-closed.

(ii) Let $Q, Q' \in q$, so that Q contains some $P \cap A$ and Q' contains some $P' \cap A$. Then the intersection $Q \cap Q'$ contains $(P \cap P') \cap A$, and $P \cap P' \in p$ since p is a filter. Thus $Q \cap Q' \in q$ so that q is intersection-closed.

(iii) If $\varnothing \in q$, then $P \cap A = \varnothing$ for some $P \in p$. But then $P \subseteq A^{\complement}$, so by upper-closure of p we must have $A^{\complement} \in p$ — a contradiction. Thus $\varnothing \notin q$ so that q is proper.

Thus q is a filter properly containing p, contradicting maximality of p.

"(b) $\implies$ (c)": Suppose $A \cup B \in p$, but $A, B \notin p$. Then (b) implies that p contains the complements $A^{\complement}$ and $B^{\complement}$. But then $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement} \in p$, so that $\varnothing = (A \cup B)^{\complement} \cap (A \cup B) \in p$. This contradicts the assumption that p is proper.

"(c) $\implies$ (a)": Suppose that q is a proper filter containing p as a proper subfilter, and select some $A \in q \setminus p$. Then $A \cup A^{\complement} = X \in p$ with $A \notin p$; by (c), we must have $A^{\complement} \in p$. But then $A^{\complement} \in q$ and so $\varnothing = A^{\complement} \cap A$ is in q by intersection-closure. This contradicts the assumption that q was a proper filter. ☐

One views each ultrafilter p as a collection of "large" subsets of X; let us say that a member of p is a **p-large set**. Thus the definition of a filter can be interpreted as saying: (i) a set is p-large if it contains a p-large set; (ii) the intersection of two p-large sets is large, and (iii) the empty set is not p-large. Proposition 1.1.2 states that if $A \cup B$ is p-large, then A or B is p-large.

We remark that an ultrafilter can alternatively be defined via finitely-additive probability "measures", *i.e.* functions $m : \mathcal{P}(X) \to \{0, 1\}$ with the following properties:

(i) $m(X) = 1$.

(ii) $m(A \sqcup B) = m(A) + m(B)$ when A, B are disjoint subsets of X.

Indeed, such a function m is the indicator function of the ultrafilter $p = \{A \subseteq X : m(A) = 1\}$; conversely, each ultrafilter p corresponds to its indicator function $m : \mathcal{P}(X) \to \{0,1\}$, defined by $m(A) = 1$ if and only if $A \in p$, and this m has the properties (i) and (ii) above. It is convenient to think of p-large sets as the sets of “full measure”. We thus conflate each ultrafilter with its corresponding measure when convenient.

There are two main types of ultrafilters: principal and nonprincipal.

Example 1.1.3. Any set $A_0 \subseteq X$ generates the **principal filter**

$$p_{A_0} := \{A \subseteq X : A_0 \subseteq A\}.$$

Indeed p_{A_0} is exactly the filter arising from $\mathcal{A} = \{A_0\}$ in Lemma 1.1.1. When $A_0 = \{x\}$ is a singleton, it is readily verified that p_x satisfies condition (c) of Proposition 1.1.2, and is therefore an ultrafilter. This is called the **principal ultrafilter** generated by x, denoted δ_x:

$$\delta_x := \{A \subseteq X : x \in A\}.$$

It is straightforward to see that ultrafilter is principal if and only if it contains a finite set.

Example 1.1.4. If X is infinite, then the collection of cofinite subsets of X is easily shown to constitute a filter on X, called the **Fréchet filter**. From Proposition 1.1.2, it follows that an ultrafilter is nonprincipal if and only if it contains the Fréchet filter. Thus the existence of a nonprincipal ultrafilter is guaranteed by Zorn’s Lemma: simply choose a maximal filter containing the Fréchet filter.

Essentially, there are no further examples: although nonprincipal ultrafilters exist by Zorn’s Lemma, they are unfortunately impossible to write down, even in the case of $X = \mathbb{N}$.

Next we show that any infinite set is contained in a nonprincipal ultrafilter. For this, we use a modification of Lemma 1.1.1 to obtain nonprincipal ultrafilters.

Lemma 1.1.5. *Let $\mathcal{A}$ be a collection of subsets of a set X, with the property that every finite subfamily of $\mathcal{A}$ has* infinite *intersection. Then $\mathcal{A}$ is contained in a nonprincipal ultrafilter.*

Proof. Let $\mathcal{C}$ be the Fréchet filter, *i.e.* the collection of cofinite subsets of X. By assumption, $\mathcal{A} \cup \mathcal{C}$ has the finite intersection property: indeed, if we have sets $A_1, \ldots, A_m \in \mathcal{A}$ and $C_1, \ldots, C_n \in \mathcal{C}$, let $A := A_1 \cap \cdots \cap A_m$ and $C := C_1 \cap \cdots \cap C_n$ be the corresponding intersections. Then A is infinite and C is cofinite. If $A \cap C = \varnothing$, then A is contained in the finite set $X \setminus C$, contrary to our assumption on $\mathcal{A}$. Thus $A \cap C \neq \varnothing$, verifying the finite intersection property for $\mathcal{A} \cup \mathcal{C}$. Thus Lemma 1.1.1 (followed with an application of Zorn’s Lemma) implies that there is an ultrafilter p containing $\mathcal{A} \cup \mathcal{C}$, and p is nonprincipal because it contains $\mathcal{C}$. $\square$

Corollary 1.1.6. *Let X be an infinite set and let A be an infinite subset. Then A is a member of a nonprincipal ultrafilter.*

Proof. Apply Lemma 1.1.5 to the family $\mathcal{A} := \{A\}$. $\square$

The **Stone–Čech compactification** of a set X (equipped with the discrete topology) is defined to be the set βX of all ultrafilters on X.

$$\beta X := \{p \subseteq \mathcal{P}(X) : p \text{ is an ultrafilter on } X\}.$$

A topology on βX can be generated as follows: for $A \subseteq X$, define

$$\overline{A} := \{p \in \beta X : A \in p\};$$

then the sets $\{\overline{A} : A \subseteq X\}$ constitute a base of open sets in βX. The topology generated by this base is compact and Hausdorff. Moreover, since each point $x \in X$ can be identified with the principal ultrafilter $\delta_x \in \beta X$, we have an inclusion $X \hookrightarrow \beta X$; this map is a homeomorphism to its image. After making this identification, $\overline{A}$ is the closure of the set $A \subseteq X$.

Now we verify the claims in the above paragraph.

Proposition 1.1.7. *Let βX be the set of ultrafilters on a set X. Then the sets*

$$\overline{A} := \{p \in \beta X : A \in p\} \quad \textit{for } A \subseteq X$$

form a base for a topology on X, in which they are all clopen. With respect to this topology:

(a) *βX is compact and Hausdorff.*

(b) *The map $x \mapsto \delta_x$ identifies X with the space of principal ultrafilters, which is a dense, open, discrete subspace of βX.*

Proof. Note that Proposition 1.1.2(c) implies $\overline{A \cup B} = \overline{A} \cup \overline{B}$, and the definition of a filter implies $\overline{A \cap B} = \overline{A} \cap \overline{B}$. Also, clearly $\beta X = \overline{X}$ since every filter contains X. So the set of unions of $\overline{A}$'s constitutes the open sets of a topology on βX. The reason that $\overline{A}$ is clopen is that its complement $(\overline{A})^{\complement} = \overline{A^{\complement}}$ is again a basic open set. Note that this also implies that every closed set is an intersection of sets of the form $\overline{A}$.

(a) First we show βX is Hausdorff. Let $p, q \in \beta X$ be distinct points; choosing a set $A \in p \setminus q$, then Proposition 1.1.2(b) implies that the complement $A^{\complement}$ is in $q \setminus p$. Thus $\overline{A}$ and $\overline{A^{\complement}} = \beta X \setminus \overline{A}$ are disjoint open sets, the former containing p and the latter containing q. Thus βX is Hausdorff.

Next we show that βX is compact by showing that any collection of closed sets with the finite intersection property must have nonempty intersection. Essentially this follows from Proposition 1.1.1. First, note that it suffices to work only with the clopen sets $\overline{A}$, because every closed set is an intersection of such. Thus suppose that $(\overline{A_i})_{i \in I}$ is a family of such sets, all of whose finite intersections are nonempty; we must show that the full intersection $\bigcap_{i \in I} \overline{A_i}$ is nonempty.

For a finite index $F \subseteq I$, notice that $\bigcap_{i \in F} \overline{A_i} = \overline{\bigcap_{i \in F} A_i}$ is nonempty, which implies that $\bigcap_{i \in F} A_i$ must be nonempty. So Proposition 1.1.1 implies that the collection $\{A_i\}_{i \in I}$ is contained in a proper filter on X, which in turn must be contained in some ultrafilter $p \in \beta X$ by Zorn's Lemma. But this just means that every A_i is p-large. So p belongs to the full intersection $\bigcap_{i \in I} \overline{A_i}$, which is exactly what we were trying to prove. This proves that βX is compact.

(b) Let $\Delta := \{\delta_x : x \in X\}$ be the set of principal ultrafilters. Since $\delta_x = \delta_y$ if and only if $x = y$, clearly $x \mapsto \delta_x$ is a bijection between X and Δ. On the other hand, each singleton in Δ is clopen, because $\{\delta_x\} = \overline{\{x\}}$ — so Δ is discrete, and the aforementioned identification is a homeomorphism.

Now Δ is open in βX because it is equal to the union of clopen sets $\bigcup_{x\in X} \overline{\{x\}}$. It is dense because every nonempty basic open set $\overline{A}$ contains $\{\delta_a : a \in A\}$ (the latter of which can be simply called A after making the identification). □

1.1.2 Aside: Ultralimits and Limsups over Nets

A net is a generalization of a sequence, serving as a technical tool to deal with topological spaces in which points may not have a countable neighborhood base. For example, the closure of a set S in a metric space can be defined as the set of all limits of sequences in S; but in a general topological space, one may need to use limits of nets. Later we will require the use of limits, ultralimits, and limsups of nets; it is convenient to describe these processes now.

To define nets, first define a **directed set** as a partially-ordered set $(I, \leq)$ in which any two elements share an upper-bound. Then a **net** in a topological space X is a function $I \to X$ where I is a directed set, usually denoted by $i \mapsto x_i$ or simply $(x_i)_{i\in I}$. A net $(x_i)_{i\in I}$ **converges** to a point $x \in X$ if, for any open neighborhood U of x, there exists $i_0 \in I$ such that $x_i \in U$ for all $i \geq i_0$. In a non-Hausdorff space, a given net may have more than one limit point; despite this, we use the following notation to denote limits of nets:

$$x = \lim_{i\in I} x_i.$$

Example 1.1.8. The set $\mathbb{N}$ with the usual ordering constitutes a directed set. A net indexed by $\mathbb{N}$ is the same thing as a sequence.

Example 1.1.9. Let $\mathcal{N}_x$ be the set of open neighborhoods of a point x in a topological space X; then $\mathcal{N}_x$ is a directed set when ordered by reverse-inclusion. This is useful for defining the closure of a set: if x is in the closure of a set S, then there is a net $\mathcal{N}_x \to S$ converging to x; conversely, if $(x_i)_{i\in I}$ is a net of points in S converging to a point x, then x is in the closure of S. In fact, if X is Hausdorff, then *every* net $\mathcal{N}_x \to X$ converges to x.

Now we define limits along filters. Let $(x_i)_{i\in I}$ be a net in a topological space X, indexed by a directed set I. If p is an filter on I, then a **p-limit** of (x_i) is any point $x \in X$ such that, for all open neighborhoods U of x, we have

$$\{i \in I : x_i \in U\} \in p.$$

The idea is that $x_i \in U$ for a "large" set of indices $i \in I$. Even though p-limits are not necessarily unique in non-Hausdorff spaces, we use the following notation to denote such limits:

$$x = \lim_{i\to p} x_i.$$

Note that if $(x_n)_{n\in\mathbb{N}}$ is a sequence and p is the filter of cofinite sets, then the p-limit of (x_n) is the usual sequence-theoretic limit.

When p is an ultrafilter, a p-limit is called an **ultralimit** along p. In general it is possible that an ultralimit does not exist, or that there is more than one ultralimit; but these pathologies do not occur in compact Hausdorff spaces, as we show below.

Proposition 1.1.10. *Let $(x_i)_{i \in I}$ be a net in X and let p be an ultrafilter on I.*

(a) *If X is Hausdorff, then (x_i) has at most one ultralimit along p.*

(b) *If X is compact, then (x_i) has at least one ultralimit along p.*

In fact, (b) provides a characterization of compactness, although we will not prove this.

Proof. (a) Suppose that x and y are two distinct ultralimits of (x_i). By the Hausdorff condition, we can select disjoint open neighborhoods U, V of x, y respectively. Then the definition of ultralimits provides that the index sets $\{i \in I : x_i \in U\}$ and $\{i \in I : x_i \in V\}$ are both members of p. But the intersection of these two sets is empty; so $\varnothing \in p$ which is a contradiction.

(b) Suppose that (x_i) admits no p-limit; then each point $x \in X$ is *not* an ultralimit of (x_i), meaning there is an open neighborhood U_x of x so that $I_x := \{i \in I : x_i \in U_x\}$ is *not* in p. In this way we have constructed an open cover $(U_x)_{x \in X}$ of X. By compactness, there is a finite subcover $X = U_{x_1} \cup \cdots \cup U_{x_n}$. But this translates to $I = I_{x_1} \cup \cdots \cup I_{x_n}$, so by the ultrafilter condition we must have $I_{x_i} \in p$ for some i, which contradicts the choice of the I_x's. □

It is well-known that if a *sequence* (x_n) converges to a limit x, then any ultralimit of (x_n) must also equal x. But this remark does not generalize to arbitrary nets. Below we make a technical remark on how to mitigate this.

A **tail** in a poset I is a set of the form

$$[a, \infty) := \{b \in I : a \leq b\} \qquad \text{where } a \in I.$$

We say that I has **infinite tails** if every tail in I is infinite. Note that in the usual directed set $(\mathbb{N}, \leq)$, every tail-end is cofinite, hence contained in every nonprincipal ultrafilter. The below fact is meant to generalize this.

Proposition 1.1.11. *Let I be a directed set.*

(a) *Let $(x_i)_{i \in I}$ be a net in a topological space X, and let $p \in \beta I$ be an ultrafilter containing every tail in I. Then every limit of (x_i) is also a p-limit of (x_i):*

$$\lim_{i \in I} x_i = \lim_{i \to p} x_i.$$

(b) *Suppose that I has infinite tails. Then there exists a* nonprincipal *ultrafilter $p \in \beta I$ containing every tail.*

Proof. (a) Let p be the given ultrafilter and let $x := \lim_{i \in I} x_i$. We must show that if U is an open neighborhood of x, then the set $A := \{i \in I : x_i \in U\}$ belongs to p. Since $x_i \to x$ in the usual sense, there must be some $i_0 \in I$ so that $x_i \in U$ for all $i \geq i_0$. Thus A contains the tail-end $[i_0, \infty)$. But p also contains this tail-end, so by upper-closure of p, we must have $A \in p$.

(b) We verify the hypotheses of Lemma 1.1.5. Let $\mathcal{A}$ be the collection of all tail-ends in I:

$$\mathcal{A} := \{[i, \infty) : i \in I\}.$$

We must show that any finite intersection of tail-ends $[i_1, \infty) \cap \cdots \cap [i_n, \infty)$ is infinite. But since I is a directed set, we can select some $j \in I$ larger than all of $i_1, \ldots, i_n$. Then the intersection $[i_1, \infty) \cap \cdots \cap [i_n, \infty)$ contains the tail-end $[j, \infty)$, which is infinite by hypothesis. Thus $\mathcal{A}$ has the "infinite" finite intersection property, so by Lemma 1.1.5, there is a nonprincipal ultrafilter $p \in \beta I$ such that $\mathcal{A} \subseteq p$, as desired. $\square$

Example 1.1.12. In the case $I = \mathbb{N}$, *every* tail-end is cofinite. Thus any nonprincipal ultrafilter $p \in \beta\mathbb{N}$ will contain every tail-end.

Example 1.1.13. Consider the directed set $I = \mathbb{N} \sqcup \{\infty\}$, with the partial order given by $n \leq \infty$ for all $n \in \mathbb{N}$. Then the tail-end starting at ∞ is nothing but the singleton $\{\infty\}$; thus here is a tail-end which cannot be contained in any nonprincipal ultrafilter.

To define density functions in this thesis, we make heavy use of limsups over nets, so we take time to define limsups carefully here. Given a net $(x_i)_{i \in I}$ consisting of real numbers in the closed interval $[0, 1]$, the **limit superior** or **limsup** of this net is the number

$$\limsup_{i \in I}(x_i) = \lim_{i_0 \in I} \sup\{x_i : i \geq i_0\}.$$

Since this is a limit of a decreasing net in a bounded interval, it is a classic calculus exercise to show that the limsup always exists, even if the usual limit does not. If the usual limit $\lim_{i \in I}(x_i)$ exists, then it is equal to the limsup. Of course, when $I = \mathbb{N}$, we recover the usual definition of the limsup of a sequence.

A **subnet** of a net $(x_i)_{i \in I}$ is a net $(x_{\alpha(j)})_{j \in J}$, where $\alpha : J \to I$ is a **cofinal function**: that is, for all $i_0 \in I$, there exists $j_0 \in J$ such that $\alpha(j) \geq i_0$ whenever $j \geq j_0$. Thus the image of α is arbitrarily large. Subnets are used for topological properties where sequences are insufficient: for example, compactness is equivalent to the requirement that every net has a convergent subnet.

The limits of convergent subnets of (x_i) are called the **cluster points** of (x_i); below we show that the limsup is the largest cluster point of a net.

Proposition 1.1.14. *Let $(x_i)_{i \in I}$ be a net in $[0, 1]$. Then*

$$\limsup_{i \in I}(x_i) = \sup\left\{x \in [0, 1] : \textit{there is a subnet } (x_{\alpha(j)}) \textit{ such that } x_{\alpha(j)} \to x\right\}$$

and the sup on the right-hand side is achieved.

Proof. Denote by y_i the sup of the tail-end:

$$y_i := \sup_{m \geq i}(x_m) \quad \text{for } i \in I,$$

so that $y_i \to y := \limsup_{i \in I} x_i$. First we show that y is larger than cluster point. Let $(x_{\alpha(j)})_{j \in J}$ be a subnet of $(x_i)_{i \in I}$ converging to a number $x \in [0, 1]$. Then for all $\varepsilon > 0$ and $i \in I$, we can select a sufficiently large index $j \in J$ so that

$$|x_{\alpha(j)} - x| < \varepsilon \quad \text{and} \quad \alpha(j) \geq i,$$

the latter being possible because $\alpha : J \to I$ is cofinal. But then $x_{\alpha(j)} \leq y_i$ by definition of y_i, so

$$x - \varepsilon < x_{\alpha(j)} \leq y_i.$$

Taking the limit over $i \in I$ shows $x - \varepsilon \leq y$. Since this is true for all $\varepsilon > 0$, we conclude $x \leq y$. This proves that y is larger than every cluster point of (x_i).

Now we show that y is itself a cluster point of (x_i). Let J be the following index set:

$$J := \{(i, \varepsilon) : i \in I, \varepsilon > 0\},$$

ordered by $(i, \varepsilon) \leq (i', \varepsilon')$ whenever $i \leq i'$ and $\varepsilon \geq \varepsilon'$. For an index $j = (i, \varepsilon) \in J$, the definition of $y_i = \sup\{x_m : m \geq i\}$ allows us to select an index $m \geq i$ such that

$$y_i - \varepsilon \leq x_m \leq y_i.$$

Set $\alpha(j) := m$. This defines a cofinal function $\alpha : J \to I$, and the convergence $x_{\alpha(j)} \to y$ is readily verified. $\square$

1.1.3 Stone–Čech Compactification of a Semigroup

Now we investigate the semigroup structure on βG when G is a semigroup. First we introduce the following notations: for a set $A \subseteq G$ and element $g \in G$, we have the image and preimage sets of the left shift $x \mapsto gx$:

$$gA := \{ga : a \in A\} \quad \text{and} \quad g^{-1}A := \{x \in G : gx \in A\}.$$

The right-sided versions Ag and Ag^{-1} are defined similarly. Now, for an ultrafilter $p \in \beta G$, define the **pullback** of A along p by

$$A^{-p} := \{g \in G : g^{-1}A \in p\}.$$

Finally, for ultrafilters $p, q \in \beta X$, define their **convolution** by the formula

$$pq := \{A \subseteq G : A^{-q} \in p\}.$$

The notation has been set up to verify the mnemonic formula that $A \in pq \iff A^{-q} \in p$. Now we quickly check that convolution defines an associative binary operation on βG; this is done through a series of formulas.

Proposition 1.1.15. *Let p, q, r be ultrafilters, let $A \subseteq G$, and let $g \in G$. Then:*

(a) *pq is an ultrafilter.*

(b) *$g^{-1}(A^{-p}) = (g^{-1}A)^{-p}$,* i.e. *ultrafilter pullback commutes with left-shift preimages.*

(c) *$A^{-(pq)} = (A^{-q})^{-p}$,* i.e. *pullback reverses composition.*

(d) *$(pq)r = p(qr)$,* i.e. *convolution is associative.*

Proof. (a) First we check pq is a proper filter. To see that pq is proper, suppose $\varnothing \in pq$, so that $\varnothing^{-q} \in p$. But $\varnothing^{-q} = \varnothing$, so $\varnothing \in q$ which contradicts that q is a proper filter. Thus $\varnothing \notin pq$ and pq is proper.

To see that pq is intersection-closed, suppose $A, B \in pq$. Then A^{-q} and B^{-q} are p-large, so their intersection $(A^{-q}) \cap (B^{-q})$ is also p-large. But $(A^{-q}) \cap (B^{-q})$ is equal to $(A \cap B)^{-q}$: this follows from $g^{-1}(A \cap B) = (g^{-1}A) \cap (g^{-1}B)$. Indeed,

$$\begin{aligned} A^{-q} \cap B^{-q} &= \{g \in G : g^{-1}A \in q \text{ and } g^{-1}B \in q\} \\ &= \{g \in G : (g^{-1}A) \cap (g^{-1}B) \in q\} \\ &= (A \cap B)^{-q}. \end{aligned}$$

Therefore, since p is upper-closed, it follows that $(A \cap B)^{-q}$ is p-large. Thus $A \cap B \in pq$ and pq is intersection-closed.

To see that pq is upper-closed, let $A \in pq$ and suppose $B \supseteq A$. Then A^{-q} is p-large. But A^{-q} is contained in B^{-q}, so B^{-q} is p-large since p is upper-closed. Thus $B \in pq$ and pq is upper-closed.

Finally we check that pq is an ultrafilter by checking that $A \cup B \in pq$ implies $A \in pq$ or $B \in pq$, then appealing to Proposition 1.1.2(b). First, observe that $A \mapsto A^{-q}$ preserves unions:

$$(A \cup B)^{-q} = (A^{-q}) \cup (B^{-q}). \tag{$\heartsuit$}$$

Indeed, if $g \in (A \cup B)^{-q}$ then $g^{-1}(A \cup B) = (g^{-1}A) \cup (g^{-1}B)$ is q-large. Since q is an ultrafilter, either $g^{-1}A$ or $g^{-1}B$ is q-large, so that $g \in (A^{-q}) \cup (B^{-q})$. Conversely, if $g \in (A^{-q}) \cup (B^{-q})$ then one of $g^{-1}A$ or $g^{-1}B$ is p-large; in either case, $(g^{-1}A) \cup (g^{-1}B) = g^{-1}(A \cup B)$ is q-large since q is upper-closed. This verifies equation $\heartsuit$.

Now if $A \cup B \in pq$, then $(A \cup B)^{-q}$ is p-large. But by equation $\heartsuit$, we have $(A^{-q}) \cup (B^{-q}) \in p$ — so since p is an ultrafilter, it follows that either A^{-q} or B^{-q} is p-large. Thus either $A \in pq$ or $B \in pq$. This shows that pq is an ultrafilter by Proposition 1.1.2(b), and we are done.

(b) This equation is a straightforward verification: since $x^{-1}(g^{-1}A) = (gx)^{-1}A$ for all $x, g \in G$ we get

$$\begin{aligned}(g^{-1}A)^{-p} &= \{x \in G : x^{-1}(g^{-1}A) \in p\} \\ &= \{x \in G : (gx)^{-1}A \in p\} \\ &= \{x \in G : gx \in A^{-p}\} \\ &= g^{-1}(A^{-p}).\end{aligned}$$

(c) This is another straightforward verification, using (b):

$$\begin{aligned}A^{-(pq)} &= \{g \in G : g^{-1}A \in pq\} \\ &= \{g \in G : (g^{-1}A)^{-q} \in p\} \\ &= \{g \in G : g^{-1}(A^{-q}) \in p\} \qquad \text{since } (g^{-1}A)^{-q} = g^{-1}(A^{-q}) \text{ by (b)} \\ &= (A^{-q})^{-p}.\end{aligned}$$

(d) Now we use (c) to show that convolution is associative.

$$\begin{aligned}(pq)r &= \{A \subseteq G : A^{-r} \in pq\} \\ &= \{A \subseteq G : (A^{-r})^{-q} \in p\} \\ &= \{A \subseteq G : A^{-(qr)} \in p\} \qquad \text{since } A^{-(qr)} = (A^{-r})^{-q} \text{ by (c)} \\ &= p(qr).\end{aligned}$$

□

Thus we have shown that βG is a semigroup under convolution. The identification $g \mapsto \delta_g$ identifies G with a dense subsemigroup of βG: indeed,

$$\delta_{gh} = \delta_g \delta_h.$$

The topology on βG is compatible with this semigroup structure in the sense that all right translations are continuous.

Proposition 1.1.16. *Let G be a semigroup with Stone–Čech compactification βG.*

(a) *βG is a* **right topological semigroup***: for each $p_0 \in \beta G$, the right shift $\rho_{p_0} : \beta G \to \beta G$, $p \mapsto pp_0$ is continuous.*

(b) *G acts continuously on the left: for each $g \in G$, the left shift $\lambda_g : \beta G \to \beta G$, $p \mapsto \delta_g p$ is continuous.*

Proof. (a) Recall that the sets $\overline{A} := \{p \in \beta G : A \in p\}$ form a base for the topology on βG; to show ρ_{p_0} is continuous, it suffices to show that $\rho_{p_0}^{-1}(\overline{A})$ is open for all $A \subseteq G$. But observe that $\lambda_{p_0}^{-1}(\overline{A}) = \overline{A^{-p_0}}$:

$$\begin{aligned}\rho_{p_0}^{-1}\left(\overline{A}\right) &= \{p \in \beta G : pp_0 \in \overline{A}\} \\ &= \{p \in \beta G : A \in pp_0\} \\ &= \{p \in \beta G : A^{-p_0} \in p\} \\ &= \overline{A^{-p_0}}.\end{aligned}$$

Thus $\rho_{p_0}^{-1}(\overline{A}) = \overline{A^{-p_0}}$ is a basic open set in βG.

(b) Once again we show $\lambda_g^{-1}\left(\overline{A}\right)$ is open for any $A \subseteq G$. Indeed, it is equal to $\overline{g^{-1}A}$:

$$\begin{aligned}\lambda_g^{-1}\left(\overline{A}\right) &= \{p \in \beta G : \delta_g p \in \overline{A}\} \\ &= \{p \in \beta G : A \in \delta_g p\} \\ &= \{p \in \beta G : A^{-p} \in \delta_g\} \\ &= \{p \in \beta G : g \in A^{-p}\} \\ &= \{p \in \beta G : g^{-1}A \in p\} \\ &= \overline{g^{-1}A}.\end{aligned}$$

Thus $\lambda_g^{-1}(\overline{A}) = \overline{g^{-1}A}$ is a basic open set in βG. □

As a side remark on the convolution formula: many authors use the following convolution instead of the one we use in the present thesis.

$$pq := \{A \subseteq G : \{x \in G : Ax^{-1} \in p\} \in q\}.$$

The only reason we deviate from this convention is for the proof of our Theorem 1.3.6 to be notationally convenient.

1.1.4 IP Sets and Hindman's Theorem

In this subsection we follow the exposition of [HS] on IP sets.

Let G be a semigroup. An ultrafilter $p \in \beta G$ is **idempotent** if $p^2 = p$; thus A is p-large if and only if $A^{-p} = \{g \in G : g^{-1}A \in p\}$ is p-large. A set $A \subseteq G$ is called an **idempotent set**, or an **IP set**, if it belongs to an idempotent ultrafilter $p \in \beta G$. The acronym "IP" historically stands for **I**nfinite-dimensional **P**arallelepiped [Fur81] — we will see this motivation shortly, see Example 1.1.22 below — but it can also be remembered serendipitously as **I**dem**P**otent.

While this definition is somewhat abstract, Hindman's Theorem will provide a much more concrete characterization of IP sets, and we will prove it below. For now we investigate generalities on idempotent ultrafilters.

Example 1.1.17. A principal ultrafilter δ_g is idempotent if and only if g is itself idempotent; thus if A is any set containing an idempotent element $g \in G$, then $A \in \delta_g$ and A is an IP set. In particular, the singleton $\{g\}$ is IP. This bodes poorly for our heuristic that IP sets should be "large"; however, we conclude from this that a finite set is IP if and only if it contains an idempotent element. For example, in the cancellative semigroup $(\mathbb{N}, +)$, all IP sets are infinite.

We now show that there exist idempotent ultrafilters on any semigroup. In fact, this follows from a more general remark of Ellis and Numakura. For this, we call a right topological semigroup **minimal** if it has no proper, closed subsemigroup.[2]

Lemma 1.1.18 (Ellis–Numakura [Ell, Num])**.** *Let G be a right topological semigroup,* i.e. *the right-shift $x \mapsto xg$ is continuous for all $g \in G$. Suppose that G is compact and Hausdorff.*

(a) *If G is minimal, then every element of G is idempotent.*

(b) *G admits at least one closed, minimal subsemigroup.*

In particular, G contains an idempotent element.

Proof. (a) Suppose that G is minimal and let $p \in G$. Then the image of the right shift

$$Gp := \{gp : g \in G\}$$

is compact by our continuity assumption, and it is clearly a subsemigroup of G. So the Hausdorff property of G implies that Gp is closed. By minimality, $Gp = G$, which implies that there is some element $g \in G$ so that $gp = p$. This shows that the set

$$pp^{-1} = \{g \in G : gp = p\}$$

is nonempty. On the other hand, pp^{-1} is a subsemigroup, and it is again closed because it is the preimage of the singleton $\{p\}$ under the right shift $x \mapsto xp$ (singletons are closed because G is Hausdorff). So another application of minimality yields $pp^{-1} = G$, which implies $p^2 = p$. This proves that every element of G is idempotent.

(b) We argue using Zorn's Lemma. Let $\mathcal{Z}$ be the collection of closed subsemigroups of G, so that $\mathcal{Z}$ is nonempty because $G \in \mathcal{Z}$. If $\{C_i\}$ is a chain in $\mathcal{Z}$, then any finite subcollection $\{C_{i_1}, \ldots, C_{i_n}\}$ has nonempty intersection: indeed, we may assume the ordering $C_{i_1} \supseteq \cdots \supseteq C_{i_n}$ because $\{C_i\}$ is a chain, and then the intersection $C_{i_1} \cap \cdots \cap C_{i_n} = C_{i_n}$ is nonempty. This shows that $\{C_i\}$ has the finite intersection property, so the full intersection $C := \bigcap C_i$ is nonempty by compactness. Now C is a closed subsemigroup, being a nonempty intersection of such; thus C is a lower bound for the chain $\{C_i\}$. Zorn's Lemma therefore implies the existence of a minimal element of $\mathcal{Z}$. ☐

Corollary 1.1.19. *Any semigroup admits an idempotent ultrafilter.*

Proof. The Stone–Čech compactification βG is compact Hausdorff by Proposition 1.1.7(a), and it is a right topological semigroup by Proposition 1.1.16. Thus apply the Ellis–Numakura Lemma 1.1.18 to βG. ☐

[2] By **subsemigroup**, we mean any nonempty, multiplicatively-closed subset.

Now we are ready to give a combinatorial characterization of IP sets, independent of ultrafilters. For a sequence $s = (s_n)_{n\geq 1}$ of elements of G and a finite set $F \subseteq \mathbb{N}$ of indices, define the **increasing product** s_F by sorting $F = \{n_1, \ldots, n_k\}$ into increasing order $n_1 < \cdots < n_k$, and then setting the product

$$s_F := s_{n_1} \cdots s_{n_k}.$$

Define the **finite product set** generated by the sequence $s = (s_n)$ to be the set of all increasing products of elements in the sequence:

$$\mathrm{FP}(s) := \{s_F : F \subseteq \mathbb{N} \text{ finite}\}.$$

So for example, $\mathrm{FP}(s)$ would contain $s_3s_5s_8$, but it would not necessarily contain the decreasing product $s_8s_5s_3$ (unless this is coincidentally equal to some other increasing product, *e.g.* if G is commutative). If G is an additive semigroup, we call this the **finite sum set** and denote it by $\mathrm{FS}(s)$.

Even though $\mathrm{FP}(s)$ is contained in the subsemigroup generated by (s_n), this inclusion may be strict; even if G is commutative, $\mathrm{FP}(s)$ may not contain, say, s_1^2.

Example 1.1.20. Here is an example where the finite sum set differs from the generated subsemigroup. Consider the sequence $s = (1, 3, 4, 5, 6, 7 \ldots)$, *i.e.* the sequence of all natural numbers except with 2 skipped, in the additive semigroup $(\mathbb{N}, +)$. Then the semigroup generated by this sequence is $\mathbb{N}$ itself simply because $s_1 = 1$ generates $\mathbb{N}$. On the other hand, the finite sum set is $\mathrm{FS}(s) = \mathbb{N} \setminus \{2\}$.

Example 1.1.21. Let p_n be the nth prime in $\mathbb{N}$. Then in the additive semigroup $(\mathbb{N}, +)$, this sequence generates the finite sum set $\mathrm{FS}(p) = \mathbb{N}\setminus\{1, 4, 6\}$ by Bertrand's Postulate, which states that every integer $n \geq 7$ is a sum of distinct primes [Ber, Che52]. However, in the multiplicative semigroup $(\mathbb{N}, \cdot\,)$, the resulting finite product set $\mathrm{FP}(p)$ is the set of all *squarefree* positive integers.

Example 1.1.22. In $\mathbb{N}^3$, the unit cube can be defined to have vertices at the coordinates e_1, e_2, e_3, $e_1 + e_2$, $e_1 + e_3$, $e_2 + e_3$, and $e_1 + e_2 + e_3$ (and 0). Thus $\mathrm{FS}(e_1, e_2, e_3, 0, 0, 0, \ldots)$ is the set of vertices of the unit cube. This serves as a geometric interpretation of finite sum sets.

We can generalize this to infinite dimensions: let $\mathbb{N}^{\mathbb{N}} = \{x : \mathbb{N} \to \mathbb{N}\}$ be the semigroup of all sequences of natural numbers, which is a commutative semigroup under termwise addition. Let e_n be the indicator sequence of the singleton $\{n\}$:

$$e_n(i) := \begin{cases} 1 & \text{if } i = n, \\ 0 & \text{if } i \neq n. \end{cases}$$

Then $\mathrm{FS}(e_n)$ consists of the indicator sequences of finite sets; geometrically, we can think of these sequences as the vertices of an infinite-dimensional cube. Similarly, by starting with a sequence of non-orthogonal vectors, one obtains an infinite-dimensional *parallelepiped*.

Example 1.1.23. In $(\mathbb{N}, +)$, let $s_n := 3^n$. This sequence generates the set of all sums of distinct powers of 3:

$$\mathrm{FS}(s) = \{3^{n_1} + \cdots + 3^{n_k} : n_1 < \cdots < n_k\}.$$

Alternatively, $\mathrm{FS}(s)$ is the set of all positive integers whose ternary expansion contains no 2's. This is an example we will return to in later sections.

Example 1.1.24. If G is any semigroup and $e \in G$ is an idempotent element, then the constant sequence $(e, e, e, \ldots)$ generates the finite product set $\mathrm{FP}(e) = \{e\}$. This is also an IP set, because it contained in the principal idempotent ultrafilter δ_e.

The reason for introducing these finite product sets is the following relationship with IP sets. This is the celebrated theorem of Hindman [Hin74], whose original proof was number-theoretic in the case of $(\mathbb{N}, +)$; he showed that if $\mathbb{N}$ is partitioned into finitely many sets, then at least one cell of the partition must contain a finite sum set. The below ultrafilter-theoretic proof for arbitrary semigroups is due to Galvin–Glazer, and is unpublished; but it can be found in [HS].

Theorem 1.1.25 (Hindman [Hin74], Galvin–Glazer)**.** *Let A be a subset of a semigroup G. Then A is an IP set if and only if it contains a finite product set,* i.e. *there is a sequence $s = (s_n)$ of elements in G such that* $\mathrm{FP}(s) \subseteq A$.

Proof of "$\Longrightarrow$". Suppose that there is an idempotent ultrafilter p containing A. Then $A \in p^2$ implies that the set $A^{-p} := \{g \in G : g^{-1}A \in p\}$ is p-large. So the intersection $A \cap A^{-p}$ is also p-large; in particular it is nonempty, so we can select some $s_1 \in A \cap A^{-p}$. In other words, $s_1 \in A$ and $s_1^{-1}A \in p$. This implies that the intersection $A_1 := A \cap s_1^{-1}A$ is p-large, so it is an IP set.

Now repeat this on A_1: we can select any element $s_2 \in A_1 \cap A_1^{-p}$, which implies $A_2 := A_1 \cap s_2^{-1}A_1$ is p-large. By construction, we know that A must contain s_1 and s_2, and since $s_2 \in A_1 \subseteq s_1^{-1}A$, we know that the increasing product s_1s_2 also belongs to A.

Our goal now is to repeat this procedure to construct the desired sequence (s_n), but we write out the formalities in gory detail here.

Inductively suppose we have constructed n elements $s_1, \ldots, s_n \in G$ and sets $A_1, \ldots, A_n$ such that:

(i) $A_i = A_{i-1} \cap s_i^{-1}A_{i-1}$ for $1 \leq i \leq n$; and

(ii) $s_i \in A_{i-1} \cap A_{i-1}^{-p}$ for $1 \leq i \leq n$ (where $A_0 := A$).

It follows that every A_i is p-large. Then the idempotence of p implies that A_n^{-p} is also p-large, so we can construct the next element in the sequence by choosing any s_{n+1} in the p-large set $A_n \cap A_n^{-p}$, and then setting

$$A_{n+1} := A_n \cap s_{n+1}^{-1}A_n.$$

In this way, we construct an infinite sequence $s := (s_n)$ of elements of G and a descending chain of p-large sets $A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \cdots$, such that $s_{n+1} \in A_n \cap A_n^{-p}$ and $A_{n+1} = A_n \cap s_{n+1}^{-1}A_n$ for all n.

Expanding the recursive definition of A_n, we obtain an expression involving left-shift preimages of A over all increasing products in s:

$$A_n = A \cap \left(\bigcap_{F \subseteq \{1,\ldots,n\}} s_F^{-1}A \right).$$

From this it is clear that $\mathrm{FP}(s) \subseteq A$. Indeed, let $s_F = s_{n_1} \cdots s_{n_k}$ be an increasing product in s, where $1 \leq n_1 < \cdots < n_k$. If $k = 1$, then $s_F = s_{n_1}$ already belongs to A by construction, so assume $k \geq 2$. Setting $n := n_k$, the above expression for A_{n-1} implies that the right-most letter s_n belongs to the set $\bigcap s_{F'}^{-1}A$, where the intersection is taken over all finite subsets F' of $\{1, \ldots, n-1\}$. Taking $F' := \{n_1, \ldots, n_{k-1}\} = F \setminus \{n_k\}$ shows that $s_F = s_{F'}s_n$ belongs to A, as required. $\square$

To prove the "if" direction in Hindman's Theorem, we must show that every finite product set $\mathrm{FP}(s)$ is an IP set. To do this, we construct a particular closed subsemigroup of βG from which we select an idempotent using the Ellis–Numakura Lemma 1.1.18, and this idempotent will contain $\mathrm{FP}(s)$. The following idempotent construction lemma formalizes this.

Lemma 1.1.26 (idempotent construction)**.** *Let $s = (s_n)$ be a sequence in a semigroup G, generating a finite product set $\mathrm{FP}(s)$. Then*

$$C := \bigcap_{N \geq 1} \overline{\mathrm{FP}(s_n)_{n \geq N}}$$

is a closed subsemigroup of βG, and $C \subseteq \overline{\mathrm{FP}(s)}$.

Proof. First we fix some notation. For $N \geq 1$, let $A_N := \mathrm{FP}(s_n)_{n \geq N}$ be the finite product set generated by the Nth tail-end of our sequence, and let $C_N := \overline{A_N}$ be the corresponding basic (cl)open set in βG. Then the descending chain $A_N \supseteq A_{N+1}$ translates into a descending chain $C_N \supseteq C_{N+1}$. Thus by compactness, the intersection

$$C = \bigcap_{N \geq 1} C_N$$

is nonempty. Clearly C is closed, being an intersection of closed sets; thus it remains to show that C is closed under convolution. For this we prove the following claim:

Claim A: For $g \in A_N$, there exists $M = M(g) \gg 0$ such that $A_M \subseteq g^{-1}A_N$.

To establish this claim, let $g \in A_N$ and write g as an increasing product $g = s_{n_1} \cdots s_{n_k}$ with $N \leq n_1 < \cdots < n_k$. Take $M := n_k + 1$; we will show $A_M \subseteq g^{-1}A_N$. Indeed, let $h \in A_M$ and write $h = s_{m_1} \cdots s_{m_\ell}$ with $M \leq m_1 < \cdots < m_\ell$. Then $m_1 > n_k$ by choice of M, so that $gh = s_{n_1} \cdots s_{n_k} s_{m_1} \cdots s_{m_\ell}$ is another increasing product in A_N. Thus $gh \in A_N$, or $h \in g^{-1}A_N$, as required.

Now let us show how Claim A allows us to prove that C is a semigroup. Let $p, q \in C$, which means A_N belongs to both p and q for all $N \geq 1$. We must show that $pq \in C$, *i.e.* that $A_N \in pq$ for all $N \geq 1$. Fix N. Then Claim A tells us that $g^{-1}A_N$ contains the p-large set $A_{M(g)}$, and therefore $g^{-1}A_N$ is itself p-large for all $g \in A_N$. Thus A_N^{-p} contains the q-large set A_N, so that A_N^{-p} is also q-large. Thus $A_N^{-p} \in q$, which is precisely what it means for A_N to belong to the convolution pq. Since this is true for all $N \geq 1$, we have shown $pq \in C$, as required.

Finally, we have $\overline{\mathrm{FP}(s)} = C_1 \supseteq C$ since $\mathrm{FP}(s) = A_1$. $\square$

Now we complete the proof of sufficiency in Hindman's Theorem.

Proof of "$\Longleftarrow$" in Theorem 1.1.25. Suppose that A contains a finite product set $\mathrm{FP}(s)$. Since ultrafilters are upper-closed, it is enough to show that $\mathrm{FP}(s)$ is an IP set. Construct the closed subsemigroup C as in the Idempotent Construction Lemma 1.1.26; then in particular, C is a compact Hausdorff left-topological semigroup. By the Ellis–Numakura Lemma 1.1.18, there is an idempotent $p \in C$, which implies $\mathrm{FP}(s) \in p$. This proves that $\mathrm{FP}(s)$ is an IP set, and we are done. $\square$

1.1.5 Aside: Nonprincipal IP Sets and Moving Semigroups

The sequence (s_n) constructed in Hindman's Theorem may result in a trivial finite product set: for example, a singleton $\{e\}$ containing an idempotent e will always be an IP set, contained in the principal idempotent ultrafilter δ_e. Thus the presence of idempotents in G means that finite sets can be IP, which causes problems for the heuristic that IP sets should be "combinatorially large". To combat this, we introduce a mild cancellation condition which allows us to work with *nonprincipal* idempotent ultrafilters.

Let G^* be the collection of nonprincipal ultrafilters on a semigroup G:

$$G^* := \beta G \setminus G.$$

Since βG contains G as an open subset, G^* is a closed hence compact set. But G^* may not be a subsemigroup of βG, in fact it is empty when (and only when) G is finite. Let us say that G is a **moving semigroup** if G^* is a (nonempty) subsemigroup of βG.

Before giving examples, we give a concrete, combinatorial characterization of moving semigroups, which appears to be a weak cancellation property.

Proposition 1.1.27 ([GoTs13])**.** *Let G be an infinite semigroup. Then G is moving if and only if: for every finite set $F \subseteq G$ and infinite set $I \subseteq G$, there are elements $g_1, \dots, g_n \in I$ such that $g_1^{-1}F \cap \cdots \cap g_n^{-1}F$ is finite.*

Proof. "$\Longrightarrow$": Suppose that G is moving. Let $F \subseteq G$ be a (nonempty) finite set and let $I \subseteq G$ be infinite. Consider the sets $g^{-1}F$ for $g \in I$; if all finite intersections of these sets are infinite, then Lemma 1.1.5 (applied to $\mathcal{A} = \{g^{-1}F : g \in I\}$) implies that there is a nonprincipal ultrafilter $q \in G^*$ containing every $g^{-1}F$, $g \in I$. This means that $I \subseteq F^{-q}$.

Now select a nonprincipal ultrafilter $p \in G^*$ containing I (guaranteed again by Lemma 1.1.5 applied to $\mathcal{A} = \{I\}$). Then $I \subseteq F^{-q}$ implies that F^{-q} is p-large, which means exactly that $F \in pq$. Thus pq contains the finite set F, and so pq is principal and $pq \notin G^*$. This contradicts the assumption that G^* is closed under ultrafilter convolution.

"$\Longleftarrow$": Conversely, assume that G satisfies the combinatorial property, and let $p, q \in G^*$. We will show that $pq \in G^*$. Towards contradiction, suppose that pq is principal, and select some $x \in G$ so that $pq = \delta_x$. Let $F := \{x\} \in pq$, which means precisely that the set $I := Fq^* = \{g \in G : g^{-1}F \in q\}$ is p-large; in particular, I is infinite. On the other hand, for any elements $g_1, \dots, g_n \in I$, the intersection $g_1^{-1}F \cap \cdots \cap g_n^{-1}F$ is p-large and is therefore also infinite. This contradiction proves that pq must be nonprincipal. □

Corollary 1.1.28. *If G is infinite and left cancellative, then G is moving.*

Recall that G is **left cancellative** if $gx = gy$ implies $x = y$ for all $g, x, y \in G$.

Proof. It is enough to check the condition given in Proposition 1.1.27. If G is left cancellative, then the set $g^{-1}a = \{x \in G : gx = a\}$ has at most one element for any $g, a \in G$. So if $F \subseteq G$ is a finite set and $I \subseteq G$ is an infinite set, then $g^{-1}F = \bigcup_{f \in F} g^{-1}f$ must be finite for any $g \in G$. □

Example 1.1.29. Any group is left (and right) cancellative, as is any subsemigroup of a group. In particular, the additive semigroups $\mathbb{Z}$, $\mathbb{N}$, and $\mathbb{N}^d$ for $d \geq 1$ are all moving by Corollary 1.1.28.

Example 1.1.30. The multiplicative semigroup $(\mathbb{N}, \cdot)$ is cancellative, and is therefore moving by Corollary 1.1.28. Note that $(\mathbb{N}, \cdot)$ is the free commutative monoid generated by a countable set, namely the set of primes.

Example 1.1.31. Generalizing the cancellative examples: for $B \geq 1$, let us say that G is **left B-to-one** if for all $g, x \in G$, there are at most B elements $y \in G$ so that $gx = gy$. Thus left cancellative semigroups are left one-to-one. It is not hard to use Proposition 1.1.27 to see that all left B-to-one semigroups are moving — but it is key that there is a uniform bound B, since there examples of finitely generated finite-to-one semigroups which are *not* moving [Ste].

Now we give a modification of Hindman's Theorem for moving semigroups. The proof is the same, with only some small changes.

Theorem 1.1.32 (nonprincipal Hindman's Theorem [GoTs13])**.** *Let G be a moving semigroup. Then the following are equivalent for a set $A \subseteq G$:*

(a) *There is a* nonprincipal *idempotent ultrafilter $p \in G^*$ containing A.*

(b) *There is a sequence of* distinct *elements $s = (s_n)$ in G such that* $\mathrm{FP}(s) \subseteq A$.

Proof. "(a) $\Longrightarrow$ (b)": This is the exact same argument as in the "$\Longrightarrow$" direction of Theorem 1.1.25, with the following change. If p is nonprincipal then it contains every cofinite set. Thus, instead of selecting s_{n+1} to be in the intersection $A_n \cap A_n^{-p}$, we select it in the smaller set $A_n \cap A_n^{-p} \cap \{s_1, \ldots, s_n\}^\complement$, which is still p-large because $\{s_1, \ldots, s_n\}^\complement$ is cofinite. In this way we select the elements s_n to be distinct. The rest of the argument is identical.

Note that we have not yet used the assumption that G is moving.

"(b) $\Longrightarrow$ (a)": Now assume that we are given a sequence $s = (s_n)$ of distinct elements in G such that $\mathrm{FP}(s) \subseteq A$. To prove (a), it is enough to show that $\mathrm{FP}(s)$ itself is contained in a nonprincipal idempotent. By Lemma 1.1.26, the set

$$C := \bigcap_{N \geq 1} \overline{\mathrm{FP}(s_n)_{n \geq N}}$$

is a closed subsemigroup of βG. Since G^* is also a closed subsemigroup, so is the intersection $C \cap G^*$, provided this intersection is nonempty. Then, selecting an idempotent $p \in C \cap G^*$ by the Ellis–Numakura Lemma 1.1.18, we have $\mathrm{FP}(s) \in p$ as required.

Thus it remains to show that $C \cap G^*$ is nonempty. This is a simple modification of the proof of Lemma 1.1.26: adopt the same notation

$$A_N := \mathrm{FP}(s_n)_{n \geq N} \quad \text{and} \quad C_N := \overline{A_N} = \{p \in \beta G : A_N \in p\}.$$

Now A_N is infinite because the s_n's are distinct, so there is a nonprincipal ultrafilter containing A_N by Lemma 1.1.5. Thus $C_N \cap G^*$ is nonempty. Now observe that

$$C \cap G^* = \bigcap_{N \geq 1} C_N \cap G^*$$

is the intersection of the infinite descending chain $C_1 \cap G^* \supseteq C_2 \cap G^* \supseteq C_3 \cap G^* \supseteq \cdots$ of nonempty closed sets. Thus compactness of βG implies that $C \cap G^*$ is nonempty, as required. $\square$

1.2 Density

In this section, we keep an eye toward the following "technical lemma" of Bell–Ghioca–Tucker, regarding density in the positive integers. The **upper Banach density** of a set $A \subseteq \mathbb{N}$ is defined to be

$$\delta^*(A) := \limsup_{|I|\to\infty} \frac{|A \cap I|}{|I|},$$

where the lim sup is taken over all intervals of positive integers.

Lemma (Bell–Ghioca–Tucker [BGT15])**.** *Suppose that A has positive density. Then there exists $b \geq 1$ so that $A \cap (A - b)$ has positive density.*

Bell–Ghioca–Tucker originally gave a direct and quantitative proof: the quantities b and $\delta^*(A \cap (A - b))$ were bounded below in terms of $\delta^*(A)$; then they used it to prove a "weak" version of the Dynamical Mordell–Lang Conjecture. Presently we give a conceptual, "soft" analytic proof of this theorem by drawing an analogy to the Poincaré Recurrence Theorem from ergodic theory. In fact we show that if A has positive density, then it has positive *measure* with respect to a finitely additive, translation-invariant probability measure on $\mathbb{N}$, which can be constructed using ultralimits. We generalize this to any *amenable* semigroup, thus obtaining the corresponding "weak" dynamical result for amenable semigroups acting rationally on a quasiprojective variety.

The material in this section is mostly an exposition of amenability and the strong Følner condition for semigroups, adapted from various sources: [AW, Fur79, Fur81, GK, Nam, Berg00]. The only original contribution in this section is part (b) of Theorem 1.2.21, where we adapt an argument of [GK] to obtain an estimate needed elsewhere in the thesis.

1.2.1 The Strong Følner Condition

The two main types of densities on $(\mathbb{N}, +)$ are the **natural** and **Banach densities**, denoted δ and δ^* respectively:

$$\delta(A) := \limsup_{n\to\infty} \frac{|A \cap \{1, \ldots, n\}|}{n} \qquad \text{and} \qquad \delta^*(A) := \limsup_{|I|\to\infty} \frac{|A \cap I|}{|I|}.$$

Here the latter lim sup is taken over all intervals $I = [a, b]$ of natural numbers. Both of these densities are translation-invariant, in the sense that $\delta(A + b) = \delta(A)$ and $\delta^*(A + b) = \delta^*(A)$ for all $A \subseteq \mathbb{N}$, $b \in \mathbb{N}$. To define similar translation-invariant densities in more general semigroups, the correct property of the family $\{[1, n] : n \geq 1\}$ is that it forms a *Følner net* in $(\mathbb{N}, +)$.

A **Følner net** in a semigroup G is a net $\mathcal{F} = (F_\lambda)_{\lambda\in\Lambda}$ of nonempty, finite subsets $F_\lambda \subseteq G$, such that we have the following limit for all $g \in G$:

$$\lim_{\lambda\in\Lambda} \frac{|F_\lambda \setminus gF_\lambda|}{|F_\lambda|} = 0.$$

Heuristically, this limit says that the overlap of F_λ and gF_λ takes up a large proportion of F_λ. Here $A \setminus B$ is used to denote the set-theoretic difference of two sets

A, B. The index set Λ is a *directed set*, and the above limit is taken in the sense of nets; see subsection 1.1.2 for details on limits over nets. The motivation for the above limit is that it represents the "error term" between $\mu(E)$ and $\mu(g^{-1}E)$, which will later allow us to construct a translation-invariant measure on G.

It is worth remarking that many authors use the *symmetric difference*

$$F \triangle gF := (F \setminus gF) \sqcup (gF \setminus F)$$

in place of the set-theoretic difference $F \setminus gF$ that we have used here. However, the resulting definition is equivalent to the one given above: this is due to the inequalities

$$|F \setminus gF| \leq |F \triangle gF| \leq 2|F \setminus gF|,$$

valid for all finite sets $F \subseteq G$ and elements $g \in G$.

The admission of a Følner net can be verified using the following more uniform condition.

Proposition 1.2.1 ([Nam]). *The following are equivalent for a semigroup G:*

(a) *G admits a Følner net $\mathcal{F} = (F_\lambda)_{\lambda \in \Lambda}$.*

(b) **[SFC]** *G satisfies the* **strong Følner condition***: for all finite sets $A \subseteq G$ and $\varepsilon > 0$, there is a finite set $F \subseteq G$ such that*

$$|F \setminus gF| < \varepsilon |F| \qquad \textit{for all } g \in A.$$

Proof. "(a) $\Longrightarrow$ (b)": The members of a Følner net $\mathcal{F} := (F_\lambda)_{\lambda \in \Lambda}$ can be used to verify the SFC. Let $A \subseteq G$ be a finite set and let ε. Then given $g \in A$, the definition of Følner nets implies that we can select $\lambda_0 \in \Lambda$ large enough so that

$$\frac{|F_\lambda \setminus gF_\lambda|}{|F_\lambda|} < \varepsilon$$

for all $\lambda \geq \lambda_0$. In fact, since A is finite and Λ is a directed set, we can select λ_0 uniformly so that the above inequality holds for *all* $g \in A$. This is exactly the desired strong Følner condition.

"(b) $\Longrightarrow$ (a)": Suppose that G satisfies the Følner condition; we will construct a Følner net. First, let Λ be the following index set:

$$\Lambda := \{(A, \varepsilon) : A \subseteq G \text{ is finite, and } \varepsilon > 0\}.$$

Then Λ is directed by inclusion in the first coordinate and reverse-order in the second coordinate; thus the max of (A, ε) and (A', ε') is simply $(A \cup A', \min\{\varepsilon, \varepsilon'\})$. For an index $\lambda = (A, \varepsilon) \in \Lambda$, the strong Følner condition allows us to select a finite set F_λ so that

$$|F_\lambda \setminus gF_\lambda| < \varepsilon |F_\lambda| \qquad \text{for all } g \in A.$$

Now we verify that $(F_\lambda)_{\lambda \in \Lambda}$ is a Følner net by directly showing that $|gF_\lambda \setminus F_\lambda|/|F_\lambda|$ tends to zero for all $g \in G$.

For $g \in G$ and $\varepsilon > 0$, define an index $\lambda_0 := (\{g\}, \varepsilon) \in \Lambda$. Then for $\lambda \geq \lambda_0$, write $\lambda = (A, \varepsilon')$ so that $g \in A$ and $\varepsilon' \leq \varepsilon$. Then by choice of F_λ, we get the estimate

$$\frac{|F_\lambda \setminus gF_\lambda|}{|F_\lambda|} < \varepsilon' \leq \varepsilon$$

as required. This proves that $\lim_{\lambda \in \Lambda} |F_\lambda \setminus gF_\lambda|/|F_\lambda| = 0$, so $\mathcal{F} = (F_\lambda)_{\lambda \in \Lambda}$ is a Følner net. $\square$

Corollary 1.2.2. *Let G be a countable semigroup. Then G satisfies the SFC if and only if G admits a Følner sequence* (i.e. *a Følner net indexed by* $\mathbb{N}$).

Proof. Since G is countable, there is a chain of finite sets $A_1 \subseteq A_2 \subseteq A_3 \subseteq \cdots$ which exhausts G:

$$G = \bigcup_{n\geq 1} A_n.$$

Applying the strong Følner condition with $A = A_n$ and $\varepsilon = 1/n$, we get a finite set F_n so that

$$|F_n \setminus gF_n| < \frac{1}{n}|F_n| \quad \text{for all } g \in A_n.$$

Now it is easily checked that

$$\lim_{n\to\infty} \frac{|F_n \setminus gF_n|}{|F_n|} = 0 \quad \text{for all } g \in G;$$

thus $(F_n)_{n\geq 1}$ is the desired Følner sequence. □

The term "strong" Følner condition is used in contrast with the **weak Følner condition**, which only requires the weaker (yet similar) estimate

$$|gF \setminus F| < \varepsilon|F|.$$

The strong Følner condition implies the weak version, simply because of the inequalities

$$|gF \setminus F| \leq |F \setminus gF| \leq |F \triangle gF| \leq 2|F \setminus gF|,$$

which are valid for all elements $g \in G$ and finite sets $F \subseteq G$.[3] If g is a left cancellable element (*i.e.* the left shift $x \mapsto gx$ is injective), then $|gF| = |F|$ and all of the above inequalities are actually equalities — thus, for left cancellable semigroups such as $(\mathbb{N}^d, +)$, the strong and weak Følner properties are equivalent.

The remainder of this subsection is dedicated to specific examples of semigroups satisfying the SFC, in addition to various permanence properties of the SFC such as direct products and direct unions.

Example 1.2.3. Let $(\mathbb{N}, +)$ be the additive semigroup of natural numbers. We will show that the initial intervals $F_n := [1, n] = \{1, \ldots, n\}$ define a Følner sequence. Given $g \in \mathbb{N}$, we must determine sufficiently large $n \geq 1$ so that $F_n \setminus (g + F_n)$ is a small proportion of F_n. In this case, $n = g + 1$ will work. Indeed, the difference between F_n and $g + F_n$ is

$$F_n \setminus (g + F_n) = [1, g+1] \setminus [g+1, 2g+1] = [1, g].$$

This has g elements. So now we calculate the desired limit:

$$\lim_{n\to\infty} \frac{|F_n \setminus (g + F_n)|}{|F_n|} = \lim_{n\to\infty} \frac{g}{n} = 0.$$

Therefore $(F_n)_{n\in\mathbb{N}}$ is a Følner sequence for $(\mathbb{N}, +)$.

[3] Note that $|gF| \leq |F|$, so $|gF \setminus F| = |gF| - |gF \cap F| \leq |F| - |F \cap gF| = |F \setminus gF|$.

Example 1.2.4. More generally, let $(I_n)_{n\in\mathbb{N}}$ be a sequence of intervals in $\mathbb{N}$ such that $|I_n| \to \infty$ as $n \to \infty$. Then $(I_n)_{n\in\mathbb{N}}$ is a Følner net in $\mathbb{N}$. Indeed, let $g \in \mathbb{N}$, and select sufficiently large n so that $|I_n| > g+1$. Writing $I_n = [a, a+h]$ with $h > g$, we get

$$I_n \setminus (g + I_n) = [a, a+h] \setminus [a+g, a+g+h] = [a, a+g]$$

and so this difference has size $|I_n \setminus (g+I_n)| = |[a, a+g]| = g+1$. Now calculate the limit of these differences:

$$\lim_{n\to\infty} \frac{|I_n \setminus (g+I_n)|}{|I_n|} = \lim_{n\to\infty} \frac{g+1}{|I_n|} = 0.$$

Therefore $(I_n)_{n\in\mathbb{N}}$ is a Følner net.

Example 1.2.5 (product Følner net)**.** Let us show that a finite product of SFC semigroups is again SFC. Let G, H be two semigroups with Følner nets $(A_i)_{i\in I}$, $(B_j)_{j\in J}$ respectively. Then we can form a product Følner net

$$F_{ij} := A_i \times B_j.$$

This is indexed by the product directed set $I \times J$, which is ordered componentwise. Then $(F_{ij})_{(i,j)\in I\times J}$ is a Følner net: indeed, let $x = (g, h) \in G \times H$. Then a straightforward set-theoretic check shows that the difference $F_{ij} \setminus xF_{ij}$ can be split into two parts.

$$F_{ij} \setminus xF_{i,j} \subseteq \Big[(A_i \setminus gA_i) \times B_j\Big] \cup \Big[A_i \times (B_j \setminus hB_j)\Big].$$

We can use this to bound the difference $|F_{ij} \setminus xF_{ij}|$ with two terms.

$$\begin{aligned} |F_{ij} \setminus xF_{ij}| &\le \Big|(A_i \setminus gA_i) \times B_j\Big| + \Big|A_i \times (B_j \setminus hB_j)\Big| \\ &\le |A_i \setminus gA_i||B_j| + |A_i||B_j \setminus hB_j|. \end{aligned}$$

Now divide by $|F_{ij}|$ and take limits.

$$\begin{aligned} \frac{|F_{ij} \setminus xF_{ij}|}{|F_{ij}|} &\le \Big|(A_i \setminus gA_i) \times B_j\Big| + \Big|A_i \times (B_j \setminus hB_j)\Big| \\ &\le \frac{|A_i \setminus gA_i||B_j|}{|F_{ij}|} + \frac{|A_i||B_j \setminus hB_j|}{|F_{ij}|} \\ &= \frac{|A_i \setminus gA_i||B_j|}{|A_i||B_j|} + \frac{|A_i||B_j \setminus hB_j|}{|A_i||B_j|} && \text{since } |F_{ij}| = |A_i||B_j| \\ &= \frac{|A_i \setminus gA_i|}{|A_i|} + \frac{|B_j \setminus hB_j|}{|B_j|} \\ &\longrightarrow 0. \end{aligned}$$

Therefore $(F_{ij})_{(i,j)\in I\times J}$ is a Følner net for $G \times H$, proving that $G \times H$ satisfies the SFC. Inductively, we can conclude that the SFC is preserved for finite products.

Example 1.2.6. The product construction in Example 1.2.5 can be used to construct a Følner net on $\mathbb{N}^d$ for $d \ge 1$, which is useful in many applications and examples. Explicitly, a **box** in $\mathbb{N}^d$ is a product of d intervals:

$$B = [a_1, b_1] \times \cdots \times [a_d, b_d].$$

When ordered by inclusion, these constitute a Følner net for $\mathbb{N}^d$. We can also use the **initial boxes**

$$B_n := [1, n] \times \cdots \times [1, n].$$

These form a subsequence of the net of all boxes, and therefore $(B_n)_{n\geq 1}$ is a Følner sequence for $\mathbb{N}^d$.

This is an interesting example for our dynamics applications: in later sections, we will work with several commuting endomorphisms $\varphi_1, \ldots, \varphi_d : X \to X$ of a variety X, and these induce an action of $\mathbb{N}^d$ on X. In this way, we can use Følner nets to generalize any density-theoretic dynamical results to the case of multiple commuting mappings.

In the below three examples, we show that the multiplicative semigroup $(\mathbb{N}, \cdot)$ satisfies the SFC. This follows from the fact that $(\mathbb{N}, \cdot)$ is the free commutative semigroup on a countable set (namely the primes). Thus we show that (i) the multiplicative semigroup generated by a finite set of primes is SFC; and (ii) G is SFC if all of its finitely generated subsemigroups are.

Example 1.2.7. Let $S = \{p_1, \ldots, p_n\} \subseteq \mathbb{N}$ be a finite set of primes and let $G(S)$ be the multiplicative semigroup generated by S; thus $G(S)$ is the set on which the p_i-adic valuations are supported for $1 \leq i \leq n$.

$$G(S) = \{p_1^{i_1} \cdots p_n^{i_n} : i_1, \ldots, i_n \geq 0\}.$$

This is called the semigroup of S**-units**. Since S is a multiplicatively independent generating set for $G(S)$, we have an isomorphism $(G(S), \cdot) \simeq (\mathbb{N}^n, +)$. Therefore $G(S)$ satisfies the SFC by Example 1.2.6.

Example 1.2.8. Let G be a semigroup with a net of subsemigroups $(G_i)_{i\in I}$. We say that G is the **direct union** of the G_i's if:

(i) $G = \bigcup_{i\in I} G_i$; and

(ii) $G_i \subseteq G_j$ for $i \leq j$.

For example, every group is the direct union of its finitely generated subgroups.

Since the SFC is a local property, it is not hard to check that a direct union of SFC semigroups is again SFC. Indeed, let $A \subseteq G$ be a finite subset of G, and let $\varepsilon > 0$. Then we can select large enough $i \in I$ so that $A \subseteq G_i$. Since G_i satisfies the SFC, we can find a finite set $F \subseteq G_i$ such that $|F \setminus gF| < \varepsilon|F|$ for all $g \in A$. This proves that G satisfies the SFC.

Example 1.2.9. Now consider the multiplicative semigroup $(\mathbb{N}, \cdot)$. By unique prime factorization, $(\mathbb{N}, \cdot)$ can be realized as the direct union of the subsemigroups $G(S)$ defined in Example 1.2.7. By Example 1.2.8, it follows that the multiplicative semigroup $(\mathbb{N}, \cdot)$ satisfies the SFC.

Example 1.2.10. Every finite *group* satisfies SFC, because the constant sequence $F_n := G$ forms a Følner net: since $gG = G$ for all $g \in G$, we have $G \setminus gG = \varnothing$, so the strong Følner condition is trivially verified.

However, a finite *semi*group need not be SFC — unlike the group case, the constant sequence $F_n = G$ will not work because $G \setminus gG$ may be nonempty. For an example of a finite semigroup which is not SFC: let G be a set with at least two elements, and define a multiplication by $xy := x$. Thus every element in G is right-absorbing.

We will show that this G is not SFC. Indeed, $gF = \{g\}$ for any subset $F \subseteq G$, so the required set difference is

$$|F \setminus gF| = |F \setminus \{g\}| = \begin{cases} |F| & \text{if } g \notin F, \\ |F| - 1 & \text{if } g \in F. \end{cases}$$

Thus $|F \setminus gF|/|F| \geq 1$ for any $F \subseteq G$, and so the strong Følner condition cannot hold. However, this G satisfies the right-sided version of the SFC, since $Gg = G$ for all $g \in G$. So this is also a degenerate example showing that the SFC is not a symmetric condition.

Example 1.2.11. Every commutative semigroup satisfies the SFC; this is a theorem of Argabright–Wilde [AW].

1.2.2 Følner Densities

In this subsection, we define the Følner density with respect to a Følner net; in the case of the semigroup $(\mathbb{N}, +)$ and the Følner net $F_n := [1, n]$, we recover the natural density function. The Banach density is not a Følner density, but we can use Følner nets to partially recover the Banach density, and this is enough for the dynamical applications later.

Let G be a semigroup satisfying the strong Følner condition (SFC), and let $\mathcal{F} = (F_\lambda)_{\lambda \in \Lambda}$ be a Følner net. Then the **upper $\mathcal{F}$-density** of a set $E \subseteq G$ is defined to be the limiting proportion of elements of E among all elements of F_λ:

$$\delta_{\mathcal{F}}(E) := \limsup_{\lambda \in \Lambda} \frac{|E \cap F_\lambda|}{|F_\lambda|} = \lim_{\lambda_0 \in \Lambda} \sup \left\{ \frac{|E \cap F_\lambda|}{|F_\lambda|} : \lambda \geq \lambda_0 \right\}.$$

Since each term $|E \cap F_\lambda|/|F_\lambda|$ is between 0 and 1, this lim sup exists as a number in $[0, 1]$. The corresponding limit, however, may not exist.

Note: the *lower $\mathcal{F}$-density* can be defined similarly, using a lim inf in place of a lim sup; the *$\mathcal{F}$-density* can then be defined whenever the upper and lower $\mathcal{F}$-densities agree. However, we will not use these notions in the present thesis.

Example 1.2.12. Let $G = \mathbb{N}$. The density with respect to the sequence of initial intervals $[1, n] = \{1, \ldots, n\}$ is called the **upper natural density**:

$$\delta(E) := \limsup_{n \to \infty} \frac{|E \cap \{1, \ldots, n\}|}{n}.$$

For example, the following natural densities are readily verified.

(i) For $a, b \geq 1$, the density of the arithmetic progression $a + \mathbb{N}b = \{a + nb : n \geq 1\}$ is $\delta(a + \mathbb{N}b) = 1/a$.

(ii) Fix $d \geq 2$ and let $S_d = \{1^d, 2^d, 3^d, \ldots\}$ be the set of perfect dth powers; then $\delta(S_d) = 0$. To see this, note that $|S_d \cap \{1, \ldots, n\}| \leq n^{1/d}$ for any n. Thus we calculate

$$\begin{aligned}\delta(S_d) &= \limsup_{n\to\infty} \frac{|S_d \cap \{1,\ldots,n\}|}{n} \\ &\le \limsup_{n\to\infty} \frac{n^{1/d}}{n} \\ &= \limsup_{n\to\infty} \frac{1}{n^{1-1/d}} \\ &= 0.\end{aligned}$$

(iii) Fix $p \ge 2$ and let $T_p := \{1, p, p^2, p^3, \ldots\}$ be the set of powers of p; then $\delta(T_p) = 0$. To see this, note that $|T_p \cap \{1,\ldots,n\}| \le \log_p(n)$ for any n. Thus we calculate

$$\begin{aligned}\delta(T_p) &= \limsup_{n\to\infty} \frac{|T_p \cap \{1,\ldots,n\}|}{n} \\ &\le \limsup_{n\to\infty} \frac{\log_p(n)}{n} \\ &= 0.\end{aligned}$$

(iv) Let $P = \{2, 3, 5, 7, 11, \ldots\}$ be the set of prime numbers; then $\delta(P) = 0$. This follows from the Prime Number Theorem [Had], which provides the asymptotic

$$|P \cap \{1,\ldots,n\}| \sim \frac{n}{\log(n)}.$$

Indeed, selecting a constant $C > 0$ so that $|P \cap \{1,\ldots,n\}| \le Cn/\log(n)$ for $n \gg 0$, we calculate

$$\begin{aligned}\delta(P) &= \limsup_{n\to\infty} \frac{|P \cap \{1,\ldots,n\}|}{n} \\ &\le \limsup_{n\to\infty} \frac{Cn/\log(n)}{n} \\ &= \limsup_{n\to\infty} \frac{C}{\log(n)} \\ &= 0.\end{aligned}$$

Example 1.2.13. There is a more sensitive density on $\mathbb{N}$, but it is not defined with respect to a Følner net. It is called the **upper Banach density:**

$$\delta^*(E) := \limsup_{|I|\to\infty} \frac{|E \cap I|}{|I|}.$$

The Banach and natural densities agree in many common cases: *e.g.* for the four sets in Example 1.2.12. In general, the two density functions can be compared by $\delta(E) \le \delta^*(E)$, but it is possible for this inequality to be strict. The reason for this is that δ keeps track of *all* integers from 1 to n, while δ^* only records "local" information.

Here is an example where E has such large gaps so that its natural density is 0, but it has full Banach density because it has arbitrarily long runs.

$$E := \{1,2\} \sqcup \{8,9,10\} \sqcup \{27,28,29,30\} \sqcup \cdots = \bigsqcup_{n\geq 1}[n^3, n^3+n].$$

It is clear that $\delta^*(E) = 1$: if we take intervals $J_n := [n^3, n^3+n]$, then $|J_n| \to \infty$ while

$$1 \geq \delta^*(E) \geq \lim_{n\to\infty} \frac{|E \cap J_n|}{|J_n|} = \lim_{n\to\infty} \frac{|J_n|}{|J_n|} = 1.$$

Thus $\delta^*(E) = 1$.

Next we show that $\delta(E) = 0$ by comparing $|E \cap [1,b]|$ to the size of b. Select the largest $N \geq 1$ so that $N^3 + N \leq b$, so that

$$E \cap [1,b] \subseteq \bigsqcup_{n=1}^{N} [n^3, n^3+n]$$

and thus, noting that $|[n^3, n^3+n]| = n+1$, we bound $|E \cap [1,b]|$ by

$$|E \cap [1,b]| \leq \sum_{n=1}^{N} |[n^3, n^3+n]| \leq \frac{1}{2}(N+1)(N+2).$$

Dividing through by b gives

$$\frac{|E \cap [1,b]|}{b} \leq \frac{\frac{1}{2}(N+1)(N+2)}{N^3+N} \longrightarrow 0,$$

and we conclude that $\delta(E) = 0$. Therefore $\delta(E) < \delta^*(E)$.

This is also an example of a set E of positive Banach density which does *not* contain an infinite arithmetic progression: if E contained such a progression, we would have $\delta(E) > 0$. For an example of a set with positive *natural* density but no arithmetic progression, simply let

$$F := \mathbb{N} \setminus E = \bigsqcup_{n=1}^{\infty} [n^3+n+1, (n+1)^3+n].$$

It is not hard to see that $\delta(F) = 1 - \delta(E) = 1$. On the other hand, F has arbitrarily long gaps, and therefore cannot contain an infinite arithmetic progression.

Even though the Banach density is not an example of a Følner density, we can still use it in our dynamical applications using the following reduction.

Lemma 1.2.14. *Given a set $E_0 \subseteq \mathbb{N}$, there exists a Følner sequence $\mathcal{F}$ on $\mathbb{N}$ such that $\delta^*(E) \geq \delta_{\mathcal{F}}(E)$ for all $E \subseteq \mathbb{N}$, with equality when $E = E_0$.*

This shows that if E_0 has positive Banach density, then it has positive density with respect to some Følner sequence $\mathcal{F}$; conversely, all sets of positive $\mathcal{F}$-density also have positive Banach density. This back-and-forth correspondence is exactly what we will need later.

Proof. Choose a sequence of intervals $(I_n)_{n\in\mathbb{N}}$ such that $|I_n| \to \infty$ and which achieves the limsup for E_0:

$$\lim_{n\to\infty} \frac{|E_0 \cap I_n|}{|I_n|} = \delta^*(E_0).$$

Then $\mathcal{F} := (I_n)_{n\in\mathbb{N}}$ is a Følner sequence by Example 1.2.4, and clearly $\delta_{\mathcal{F}}(E_0) = \delta^*(E_0)$. On the other hand, since the lim sup represents the largest subsequential limit, it also follows that $\delta^*(E) \geq \delta_{\mathcal{F}}(E)$ for all $E \subseteq \mathbb{N}$. Thus $\mathcal{F}$ is the required Følner net, establishing the claim. □

Now we give analogous examples for densities $\mathbb{N}^d$ for $d \geq 1$. This setting allows us to generalize density-theoretic dynamical claims to the case of multiple commuting mappings.

Example 1.2.15. For $n \geq 1$, define the **initial box** in $\mathbb{N}^d$:

$$B_n := [1, n] \times \cdots \times [1, n].$$

Then $\mathcal{B} = (B_n)_{n\geq 1}$ is a Følner sequence for $\mathbb{N}^d$ (see Example 1.2.6). The $\mathcal{B}$-density is called the **natural box density** on $\mathbb{N}^d$:

$$\delta(A) := \limsup_{n\to\infty} \frac{|\{(a_1, \ldots, a_d) \in A : a_1, \ldots, a_d \in [1, n]\}|}{n^d} \quad \text{for } A \subseteq G.$$

Example 1.2.16. The **box Banach density** on $\mathbb{N}^d$ is defined as follows:

$$\delta^*(A) := \limsup_{|B|\to\infty} \frac{|A \cap B|}{|B|} \quad \text{for } A \subseteq G.$$

Here the limsup is taken over all boxes $B = [a_1, b_1] \times \cdots \times [a_d, b_d]$.

Once again, the box Banach density is not actually a Følner density. But the exact same argument as in Lemma 1.2.14 gives the following useful method to replace the box Banach density with a bona fide Følner density.

Lemma 1.2.17. *Given a set $E_0 \subseteq \mathbb{N}^d$, there exists a Følner sequence $\mathcal{F}$ on $\mathbb{N}^d$ such that $\delta^*(E) \geq \delta_{\mathcal{F}}(E)$ for all $E \subseteq \mathbb{N}^d$, with equality when $E = E_0$.*

Our dynamical applications will involve both sets of positive density and IP sets. In the below two examples, we show that there is no implication between these two properties, even in $\mathbb{N}$.

Example 1.2.18. Not every IP set has positive density: for example, we can make a sequence (s_n) of natural numbers with such large gaps that even the set of finite sums $\mathrm{FS}(s_n)$ has large gaps. Let $s_n := 3^n$. Then

$$T := \mathrm{FS}(s_n) = \{3^{n_1} + \cdots + 3^{n_k} : n_1 < \cdots < n_k\}$$

is the set of all sums of distinct powers of 3; alternatively, it is the set of those natural numbers n whose ternary expansion contains no 2's. This T is an IP set by Hindman's Theorem 1.1.25, but we will prove that $\delta(T) = 0$.

For this we again compare $|T \cap [1, b]|$ to the size of b. Let $[n]_3$ denote the ternary string representing $n \in \mathbb{N}$, and write $[b]_3 = b_0 \cdots b_L$ where $b_i \in \{0, 1, 2\}$ and $b_L \neq 0$. Then $3^L \leq b < 3^{L+1}$, so

$$T \cap [1, b] \subseteq T \cap [1, 3^{L+1}) = \{n \geq 1 : [n]_3 \text{ has no 2's, and length}([n]_3) \leq L\}.$$

The size of this latter set is clearly at most 2^L, since it counts binary strings of length $\leq L$. Therefore, since $L \to \infty$ as $b \to \infty$, we have the limit

$$\frac{|T \cap [1, b]|}{b} \leq \frac{2^L}{3^L} \longrightarrow 0$$

and we conclude that $\delta(T) = 0$.

Example 1.2.19. Not every set of positive density must be IP. For example, the set $\{1, 3, 5, 7, \ldots\}$ of odd positive integers has natural density 0.5, but it cannot contain a finite sum set because it contains no set of the form $\{a, b, a + b\}$.

Before closing this subsection, we verify several useful properties involving the upper density.

Proposition 1.2.20. *Let $\delta_{\mathcal{F}}$ denote the upper density with respect to a Følner net $\mathcal{F} = (F_\lambda)$ in an SFC semigroup G. Then:*

(a) *$\delta_{\mathcal{F}}$ is increasing: if $A \subseteq B$ then $\delta_{\mathcal{F}}(A) \leq \delta_{\mathcal{F}}(B)$.*

(b) *$\delta_{\mathcal{F}}$ is subadditive: $\delta_{\mathcal{F}}(A \cup B) \leq \delta_{\mathcal{F}}(A) + \delta_{\mathcal{F}}(B)$ for all $A, B \subseteq G$.*

(c) *$\delta_{\mathcal{F}}$ is* **partition-regular***: a union of finitely many sets of zero density again has zero density.*

Proof. (a) This is obvious from the inequality

$$\frac{|A \cap F_\lambda|}{|F_\lambda|} \leq \frac{|B \cap F_\lambda|}{|F_\lambda|}.$$

(b) This is obvious from the inequality

$$\frac{|(A \cup B) \cap F_\lambda|}{|F_\lambda|} = \frac{|(A \cap F_\lambda) \cup (B \cap F_\lambda)|}{|F_\lambda|} \leq \frac{|A \cap F_\lambda|}{|F_\lambda|} + \frac{|B \cap F_\lambda|}{|F_\lambda|}.$$

(c) Let $A_1, \ldots, A_n$ be finitely many sets all of zero density. Then their union $A := A_1 \cup \cdots \cup A_n$ also has zero density by subadditivity:

$$\delta_{\mathcal{F}}(A) \leq \delta_{\mathcal{F}}(A_1) + \cdots + \delta_{\mathcal{F}}(A_n) = 0. \qquad \square$$

1.2.3 Cancellable Følner Nets

Our ultimate goal is to show how the Følner density $\delta_{\mathcal{F}}$ can induce a finitely-additive, G-invariant probability measure μ on G. In this subsection, we handle a technical cancellation condition that we can use the define μ, following a theorem of Gray–Kambites. When G is already left cancellative, this modification is unnecessary.

Let $\mathcal{K} = (K_\lambda)_{\lambda\in\Lambda}$ be a Følner net for a semigroup G. Then $\mathcal{K}$ is **eventually left cancellable**, or simply **cancellable**, if it satisfies the following condition: for all $g \in G$, there is an index λ_0 such that

$$gx = gy \implies x = y \qquad \text{for all } x, y \in K_\lambda, \lambda \geq \lambda_0.$$

Thus g acts injectively by left-translation on all sufficiently large F_λ's.

It is seemingly stronger to require that a semigroup admits a cancellable Følner net than an ordinary one. However, Gray–Kambites uses several clever estimates to show that any Følner net can be shrunk to a cancellable one [GK]. We also adapt their argument to show that if a set has positive density with respect to a Følner net, then it also has positive density with respect some cancellable Følner net.

Theorem 1.2.21. *Let G be a semigroup satisfying the strong Følner condition.*

(a) (Gray–Kambites [GK]) *For all finite sets $A \subseteq G$ and $\varepsilon > 0$, there is a finite set $K \subseteq G$ such that*

  (i) *$|K \setminus gK| < \varepsilon|F|$ for all $g \in A$; and*

  (ii) *$gx = gy$ implies $x = y$ for all $g \in A$, $x, y \in K$.*

  Thus G admits a cancellable Følner net.

(b) *Let $E \subseteq G$. If E has positive density with respect to some Følner net $\mathcal{F}$, then E has positive density with respect to some* cancellable *Følner net $\mathcal{K} = (K_\gamma)_{\gamma\in\Gamma}$ such that Γ has infinite tails*[4]*.*

Proof. (a) Fix a finite set $A \subseteq G$ and $\varepsilon > 0$. Define a function $\psi(t)$ as follows:

$$\psi_A(t) := \frac{(1+2|A|)t}{1-2|A|t}.$$

Then $\psi(t)$ is continuous on the open interval $0 < t < 1/2|A|$, and $\psi(t) \to 0$ as $t \to 0$. Thus we can select t in this interval small enough so that $\psi(t) < \varepsilon$. Applying the strong Følner condition to this choice of $t > 0$, we can find a finite set F such that

$$|F \setminus gF| < t|F| \quad \text{for all } g \in A.$$

Now we will remove from F any instances of distinct elements $x, y \in F$ such that $gx = gy$ for some $g \in A$. Thus define a set of "bad" elements for each $g \in A$:

$$C_g := \{x \in F : \text{there exists } y \in F \setminus \{x\} \text{ such that } gx = gy\}.$$

Thus $x \in C_g$ if and only if $|F \cap g^{-1}(gx)| \geq 2$. Since each fiber of the left translation $g : C_g \to gC_g$ has at least two elements, we have an inequality

$$|gC_g| \leq \frac{1}{2}|C_g| \quad \text{for all } g \in A. \tag{1.1}$$

which holds even when C_g is empty. We will also need the following estimate on the cardinality of C_g.

$$|C_g| \leq 2|F|t \quad \text{for all } g \in A. \tag{1.2}$$

[4]Recall that a poset I has **infinite tails** if for all $a \in I$, there are infinitely many distinct $b \in I$ with $a \leq b$.

To prove 1.2, suppose towards contradiction that $|C_g| > 2|F|t$ for some $g \in A$. Then we calculate

$$
\begin{aligned}
|gF| &\leq |gC_g| + |gF \setminus gC_g| \\
&\leq |gC_g| + |g(F \setminus C_g)| && \text{since } gF \setminus gC_g \subseteq g(F \setminus C_g) \\
&\leq |gC_g| + |F \setminus C_g| \\
&\leq \frac{1}{2}|C_g| + |F \setminus C_g| && \text{by 1.1} \\
&= \frac{1}{2}|C_g| + |F| - |C_g| \\
&= |F| - \frac{1}{2}|C_g| \\
&< |F| - t|F| && \text{since } |C_g| > 2|F|t \\
&= (1-t)|F|.
\end{aligned}
$$

But this implies $t|F| < |F| - |gF| \leq |F \setminus gF|$, contrary to the choice of F. This contradiction proves 1.2. Note that 1.2 holds even when C_g is empty.

Now we define the desired set K: it consists of those $x \in F$ on which A acts injectively, *i.e.* $gx = gy$ implies $x = y$ for all $g \in A$, $y \in F$.

$$K := \{x \in F : F \cap g^{-1}(gx) = \{x\} \text{ for all } g \in A\} = \bigcap_{g \in A} F \setminus C_g.$$

Since K was constructed by removing all "bad" elements, it is clear that K satisfies the cancellation condition (ii). It remains to verify the Følner condition (i). For this we use the following estimate:

$$|F \setminus K| \leq 2|F||A|t. \tag{1.3}$$

To prove this, first note that $F \setminus K = \bigcup_{g \in A} C_g$ by definition of the sets C_g. Therefore, we use estimate 1.2 to obtain

$$|F \setminus K| \leq \sum_{g \in A} |C_g| \leq \sum_{g \in G} 2|F|t = 2|F||A|t.$$

This proves 1.3, which also implies the inequality

$$|K| \geq |F| - 2|F||A|t = (1 - 2|A|t)|F|. \tag{1.4}$$

Now we can finally verify that $|K \setminus gK| < \varepsilon|K|$ for any $g \in A$:

$$\begin{aligned}
|K \setminus gK| &\leq |F \setminus gK| && \text{since } K \subseteq F \\
&\leq |(F \setminus gF) \sqcup (gF \setminus gK)| \\
&\leq |F \setminus gF| + |gF \setminus gK| \\
&\leq |F \setminus gF| + |g(F \setminus K)| && \text{since } gF \setminus gK \subseteq g(F \setminus K) \\
&\leq |F \setminus gF| + |F \setminus K| \\
&< t|F| + |F \setminus K| && \text{since } |F \setminus gF| < t|F| \\
&\leq t|F| + 2t|F||A| && \text{by 1.3} \\
&= (1 + 2|A|)t|F| \\
&\leq \frac{(1 + 2|A|)t}{1 - 2|A|t}|K| && \text{by 1.4} \\
&= \psi_A(t)|K| \\
&< \varepsilon|K| && \text{by choice of } t.
\end{aligned}$$

This verifies (i) and completes the proof.

(b) Let $E \subseteq G$, and suppose that $\delta_{\mathcal{F}}(E) > 0$ for some Følner net $\mathcal{F} = (F_\lambda)_{\lambda\in\Lambda}$. We construct a cancellable Følner net $\mathcal{K} = (K_\gamma)_{\gamma\in\Gamma}$ with the desired properties.

First, let $\alpha := \delta_{\mathcal{F}}(E) > 0$. By dropping to a subnet of $\mathcal{F}$ if necessary, we can assume that α is achieved by a limit (rather than a lim sup):

$$\alpha = \delta_{\mathcal{F}}(E) = \lim_{\lambda\in\Lambda} \frac{|E \cap F_\lambda|}{|F_\lambda|}.$$

Next, define the indexing set Γ as

$$\Gamma := \{(A, \varepsilon) : A \subseteq G \text{ finite, } 0 < \varepsilon < \alpha\}.$$

As in the proof of Proposition 1.2.1, we order Γ by inclusion in the first coordinate and reverse-order in the second coordinate: thus

$$(A, \varepsilon) \leq (A', \varepsilon') \quad \iff \quad A \subseteq A' \text{ and } \varepsilon \geq \varepsilon',$$

and it is clear that Γ is a directed set with infinite tails. For a given index $\gamma = (A, \varepsilon) \in \Gamma$, fix $t = t(\gamma) > 0$ small enough so that it satisfies $0 < \psi_A(t) < \varepsilon$ and $t < (\alpha - \varepsilon)/2|A|$ (where $\psi_A(t)$ is the function defined in part (a)); then choose a sufficiently large index $\lambda = \lambda(\gamma) \in \Lambda$ so that the following two inequalities hold:

$$\frac{|E \cap F_\lambda|}{|F_\lambda|} > \alpha - \varepsilon \qquad \text{and} \qquad |F_\lambda \setminus gF_\lambda| < t|F_\lambda| \quad \text{for all } g \in A.$$

The first inequality is possible by definition of α, and the second one is by definition of Følner net. Now follow the construction as in part (a), starting with $F = F_\lambda$ and ending with $K = K_\gamma$, so that the estimate 1.3 gives

$$|F_\lambda \setminus K_\gamma| < 2|F_\lambda||A|t. \tag{1.5}$$

From the estimate

$$\frac{|K_\gamma \setminus gK_\gamma|}{|K_\gamma|} < \psi(t) < \varepsilon \quad \text{for all } g \in A,$$

it follows as in the proof of Proposition 1.2.1 that $\mathcal{K} := (K_\gamma)_{\gamma\in\Gamma}$ is a Følner net, and $\mathcal{K}$ is cancellable as in part (a).

It remains to check that E has positive $\mathcal{K}$-density. Suppose for contradiction that $\delta_{\mathcal{K}}(E) = 0$. Then setting $\beta := \frac{1}{2}(\alpha - \varepsilon - 2|A|t) > 0$, there is a sufficiently large index $\gamma = (A, \varepsilon) \in \Gamma$ so that

$$\frac{|E \cap K_\gamma|}{|K_\gamma|} < \beta.$$

But if we let $t = t(\gamma)$ and $\lambda = \lambda(\gamma)$ as above, we can use 1.5 to get

$$\begin{aligned}
\beta|K_\gamma| &> |E \cap K_\gamma| \\
&= |E \cap F_\lambda| - |E \cap (F_\lambda \setminus K_\gamma)| && \text{since } K_\gamma \subseteq F_\lambda \\
&\geq (\alpha - \varepsilon)|F_\lambda| - |E \cap (F_\lambda \setminus K_\gamma)| && \text{by choice of } \lambda \\
&\geq (\alpha - \varepsilon)|F_\lambda| - |F_\lambda \setminus K_\gamma| \\
&\geq (\alpha - \varepsilon)|F_\lambda| - 2|F_\lambda||A|t && \text{by 1.5} \\
&= (\alpha - \varepsilon - 2|A|t)|F_\lambda| \\
&\geq (\alpha - \varepsilon - 2|A|t)|K_\gamma| && \text{since } F_\lambda \supseteq K_\gamma \\
&> \beta|K_\lambda| && \text{by choice of } \beta.
\end{aligned}$$

This contradiction proves that $\delta_{\mathcal{K}}(E) > 0$, as required. □

1.2.4 Amenable Semigroups

In this subsection, we use cancellable Følner nets and ultralimits to define probability measures on semigroups, thus proving that every SFC semigroup is *amenable.*

Let G be a semigroup. A **left invariant mean** on G is a set function

$$\mu : \mathcal{P}(G) \to [0, 1]$$

such that

(i) $\mu(G) = 1$;

(ii) μ **is finitely additive:** $\mu(A \sqcup B) = \mu(A) + \mu(B)$ for all disjoint subsets $A, B \subseteq G$;

(iii) μ **is translation-invariant:** $\mu(g^{-1}A) = \mu(A)$ for all $g \in G$ and $A \subseteq G$.

A **left amenable semigroup** is one admitting a left invariant mean; throughout this thesis, by **amenable** we mean left amenable. Like ultrafilters, these invariant means are usually impossible to write down, but they are useful theoretical tools.

Example 1.2.22. We prove below (Theorem 1.2.25) that every SFC semigroup is amenable: thus the class of amenable semigroups includes all commutative semigroups, finite left cancellative semigroups, and finite products of such.

Example 1.2.23. Argabright–Wilde [AW] showed that amenability is equivalent to the strong Følner condition for left cancellative semigroups.

Example 1.2.24. Let F_2 be the free group on two generators a, b; then F_2 is not amenable. To see this, suppose that μ is an invariant mean on F_2. For a word

$w \in F_2$, let $W(w)$ denote the set of (reduced) words on $a^{\pm 1}, b^{\pm 1}$ that start with w. Then since μ is subadditive[5], from $F_2 = W(a) \cup a^{-1}W(a)$, we calculate

$$1 = \mu(F_2) \leq \mu(W(a)) + \mu(a^{-1}W(a)) = 2\mu(W(a))$$

so that $\mu(W(a)) \geq 1/2$. The same holds for all the sets $W(a^{-1})$, $W(b)$, and $W(b^{-1})$ — all these sets have measure at least $1/2$. But then applying μ to the decomposition $F_2 = \{1\} \sqcup W(a) \sqcup W(b) \sqcup W(a^{-1}) \sqcup W(b^{-1})$, we get

$$\begin{aligned} 1 &= \mu(F_2) \\ &= \mu(\{1\}) + \mu(W(a)) + \mu(W(b)) + \mu(W(a^{-1})) + \mu(W(b^{-1})) \\ &\geq 2. \end{aligned}$$

This contradiction shows the famous fact that F_2 does not admit an invariant mean.

We show now that the strong Følner condition implies amenability. For our dynamical applications, it is pertinent to keep track of the actual construction of the invariant mean from a given Følner net, so we record the following version of the theorem.

Theorem 1.2.25. *If G satisfies the strong Følner condition, then G is amenable.*

In fact, suppose that $\mathcal{F} = (F_\lambda)_{\lambda \in \Lambda}$ is a cancellable Følner net such that Λ has infinite tails, and that p is nonprincipal ultrafilter on Λ containing every tail in Λ. Then the function

$$\mu_{\mathcal{F}}(A) := \lim_{\lambda \to p} \frac{|A \cap F_\lambda|}{|F_\lambda|}$$

defines an invariant mean on G, satisfying $\mu_{\mathcal{F}}(A) \leq \delta_{\mathcal{F}}(A)$ for all $A \subseteq G$.

Proof. If G satisfies the strong Følner condition, then by Theorem 1.2.21, there is a cancellable Følner net $\mathcal{F} = (F_\lambda)_{\lambda \in \Lambda}$ such that Λ has infinite tails; by Proposition 1.1.11, there exists a nonprincipal ultrafilter p on Λ containing every tail. Thus amenability of G follows from the below construction of an invariant mean.

For $A \subseteq G$, define $\mu(A)$ as the following ultralimit along p:

$$\mu(A) := \lim_{\lambda \to p} \frac{|A \cap F_\lambda|}{|F_\lambda|}.$$

Since all the numbers $|A \cap F_\lambda|/|F_\lambda|$ lie in the interval $[0, 1]$, the above ultralimit exists as a number in $[0, 1]$ (see subsection 1.1.2). Now we verify that μ is an invariant mean on G. Clearly $\mu(G) = 1$, because $|G \cap F_\lambda|/|F_\lambda| = |F_\lambda|/|F_\lambda| = 1$ for all λ.

Now we verify that μ is finitely-additive. If $A, B \subseteq G$ are disjoint, then

$$|(A \sqcup B) \cap F_\lambda| = |A \cap F_\lambda| + |B \cap F_\lambda|.$$

[5] Any invariant mean μ satisfies $\mu(A \cup B) \leq \mu(A) + \mu(B)$, even when A, B are not disjoint.

Since ultralimits preserve addition, we thus obtain

$$\begin{aligned}\mu(A \sqcup B) &= \lim_{\lambda\to p} \frac{|(A \sqcup B) \cap F_\lambda|}{|F_\lambda|} \\ &= \lim_{\lambda\to p} \frac{|(A \cap F_\lambda) \sqcup (B \cap F_\lambda)|}{|F_\lambda|} \\ &= \lim_{\lambda\to p} \left(\frac{|A \cap F_\lambda|}{|F_\lambda|} + \frac{|B \cap F_\lambda|}{|F_\lambda|} \right) \\ &= \lim_{\lambda\to p} \frac{|A \cap F_\lambda|}{|F_\lambda|} + \lim_{\lambda\to p} \frac{|B \cap F_\lambda|}{|F_\lambda|} \\ &= \mu(A) + \mu(B).\end{aligned}$$

Thus μ is finitely-additive.

To check invariance of μ, this is where we use the extra assumptions on the Følner net $\mathcal{F}$. Note that since the numbers $|F_\lambda \setminus gF_\lambda|/|F_\lambda|$ tend to zero, the corresponding ultralimit is also zero:

$$\lim_{\lambda\to p} \frac{|F_\lambda \setminus gF_\lambda|}{|F_\lambda|} = 0.$$

Note that here is where we finally use the technical assumption that Λ has infinite tails (see Proposition 1.1.11).

Now we want to show $\mu(g^{-1}A) = \mu(A)$ for all $g \in G$ and $A \subseteq G$. Fix such g and A, and let $\varepsilon > 0$. Since $\mathcal{F}$ is cancellable, we can select an index $\lambda_0 \in \Lambda$ so that

(i) $|F_\lambda \setminus gF_\lambda| < \varepsilon|F_\lambda|$ for all $\lambda \geq \lambda_0$, and

(ii) $gx = gy$ implies $x = y$ for all $x, y \in F_\lambda$, $\lambda \geq \lambda_0$.

This implies that the left-translation $x \mapsto gx$ gives a bijection between $g^{-1}A \cap F_\lambda$ and $A \cap gF_\lambda$, so

$$|g^{-1}A \cap F_\lambda| = |A \cap gF_\lambda| \quad \text{for all } \lambda \geq \lambda_0.$$

Thus we estimate the difference between $|A \cap F_\lambda|$ and $|g^{-1}A \cap F_\lambda|$:

$$\begin{aligned}|A \cap F_\lambda| - |g^{-1}A \cap F_\lambda| &= |A \cap F_\lambda| - |A \cap gF_\lambda| \\ &\leq |A \cap (F_\lambda \setminus gF_\lambda)| \\ &\leq |F_\lambda \setminus gF_\lambda|.\end{aligned}$$

(The first inequality follows from the inequality $|P| \leq |P \setminus Q| + |Q|$, valid for any finite sets P, Q.) Combined with the Følner condition, this estimate immediately shows the limit

$$\lim_{\lambda\in\Lambda} \frac{|A \cap F_\lambda|}{|F_\lambda|} - \frac{|g^{-1}A \cap F_\lambda|}{|F_\lambda|} = 0.$$

Thus we compute the difference of the measures $\mu(A)$ and $\mu(g^{-1}A)$:

$$\begin{aligned}
\mu(A) &= \lim_{\lambda\to p} \frac{|A\cap F_\lambda|}{|F_\lambda|} \\
&= \lim_{\lambda\to p} \left(\frac{|A\cap F_\lambda|}{|F_\lambda|} - \frac{|g^{-1}A\cap F_\lambda|}{|F_\lambda|} + \frac{|g^{-1}A\cap F_\lambda|}{|F_\lambda|} \right) \\
&= \lim_{\lambda\to p} \frac{|g^{-1}A\cap F_\lambda|}{|F_\lambda|} + \lim_{\lambda\to p} \left(\frac{|A\cap F_\lambda|}{|F_\lambda|} - \frac{|g^{-1}A\cap F_\lambda|}{|F_\lambda|} \right) \\
&= \lim_{\lambda\to p} \frac{|g^{-1}A\cap F_\lambda|}{|F_\lambda|} \\
&= \mu(g^{-1}A).
\end{aligned}$$

This is the required invariance of μ, thus completing the proof. □

By modifying the above argument to keep track of the indices, we can construct μ so that it agrees with the density of a given subset of G. This results in a finitely additive version of the well-known *Furstenberg Correspondence Principle.*

Corollary 1.2.26. *Let $\mathcal{F}$ be a cancellable Følner net for a semigroup G whose index set has infinite tails, and fix a subset $A_0 \subseteq G$. Then there is an invariant mean $\mu : \mathcal{P}(G) \to [0,1]$ such that $\mu(E) \leq \delta_{\mathcal{F}}(E)$ for all $E \subseteq G$, with equality when $E = E_0$.*

Proof. First, we may drop to a subnet that realizes the density of E_0: *i.e.* select a subnet $\mathcal{F}' := (F_{\lambda_i})_{i\in I}$ so that

$$\delta_{\mathcal{F}}(E_0) = \lim_{i\in I} \frac{|E_0 \cap F_{\lambda_i}|}{|F_{\lambda_i}|}.$$

Then clearly $\mathcal{F}'$ is still a cancellable Følner net, and dropping to this subnet only makes the density function smaller: $\delta_{\mathcal{F}'}(E) \leq \delta_{\mathcal{F}}(E)$ for all $E \subseteq G$, with equality when $E = E_0$ by choice of the subnet. Thus the invariant mean $\mu := \mu_{\mathcal{F}'}$ constructed in Theorem 1.2.25 satisfies the desired properties. □

Corollary 1.2.27. *Let G be an SFC semigroup, and let $E \subseteq G$ have positive density with respect to some Følner net. Then $\mu(E) > 0$ for some invariant mean μ on G.*

Proof. If E has positive density with respect to some Følner net, then by Theorem 1.2.21(b), there is a cancellable Følner net $\mathcal{F}$ with infinite tails such that $\delta_{\mathcal{F}}(E) > 0$. By Corollary 1.2.26, we can find an invariant mean μ such that $\mu(E) = \delta_{\mathcal{F}}(E) > 0$, as required. □

1.2.5 Poincaré Recurrence Theorem

Theorem 1.2.25 shows that if a set has positive density with respect to a Følner net, then it has positive measure with respect to some invariant mean. This elucidates a deep connection between combinatorial statements about density in semigroups and statements about measure-preserving systems in ergodic theory. When viewed under this lens, a technical lemma of Bell–Ghioca–Tucker translates into an elegant theorem about recurrence in measure-preserving systems, called the *Poincaré Recurrence Theorem.* In this subsection, we use this ergodic point-of-view to generalize their lemma to arbitrary semigroups satisfying the strong Følner condition.

If (X, μ) is a (finitely additive) probability space, then a measurable map $\varphi : X \to X$ is **measure-preserving** if

$$\mu(\varphi^{-1}(E)) = \mu(E) \qquad \text{for all measurable sets } E \subseteq G.$$

The Poincaré Recurrence Theorem states that, in a measure-preserving system, almost all points in a set E of positive measure will return to E infinitely often. See [Berg00] for an account of the history of this old theorem. Since the proof uses only finite additivity instead of the full countable additivity, we state it with this weaker hypothesis.

Theorem 1.2.28 (Poincaré Recurrence)**.** *Let $\varphi : X \to X$ be a measure-preserving transformation of a finitely additive probability space (X, μ), and let $E \subseteq X$ be a set of positive measure. Then there exists $n \geq 1$ so that*

$$\mu(E \cap \varphi^{-n}(E)) > 0.$$

Proof. Let $E_n := \varphi^{-n}(E)$ so that $\mu(E_n) = \mu(E)$ for all $n \geq 1$ (because φ is measure-preserving). Also, for $m \leq n$ we have $E_m \cap E_n = \varphi^{-m}(E \cap E_{n-m})$, so again the measure-preserving property of φ implies that

$$\mu(E_m \cap E_n) = \mu(E \cap E_{n-m}) \qquad \text{for all } n \geq m.$$

Thus it is enough to show that $E_m \cap E_n$ has positive measure for some pair $n > m$.

Suppose that all of these intersections have measure zero. Choose any positive integer $N > \frac{1}{\mu(E)}$. Then for each $n \in \{1, \ldots, N\}$, let $\widehat{E_n}$ denote the removal of all other E_i's from E_n:

$$\widehat{E_n} := E_n \setminus \left(\bigcup_{\substack{i=1 \\ i \neq n}}^{N} E_i \right) = E_n \setminus \left(\bigcup_{\substack{i=1 \\ i \neq n}}^{N} E_i \cap E_n \right).$$

Thus we have removed a null set from E_n, so that $\mu\left(\widehat{E_n}\right) = \mu(E_n) = \mu(E)$. On the other hand, the sets $\widehat{E_1}, \ldots, \widehat{E_N}$ are obviously pairwise disjoint, so finite additivity of μ gives

$$\begin{aligned}
\mu\left(\widehat{E_1} \sqcup \cdots \sqcup \widehat{E_N}\right) &= \mu\left(\widehat{E_1}\right) + \cdots + \mu\left(\widehat{E_N}\right) \\
&= \mu(E) + \cdots + \mu(E) \\
&= N\mu(E) \\
&> 1.
\end{aligned}$$

Therefore $\widehat{E_1} \sqcup \cdots \sqcup \widehat{E_n}$ has strictly larger measure than X itself, which is impossible. This contradiction yields the desired conclusion. $\square$

Via Theorem 1.2.26, the Poincaré Recurrence Theorem immediately translates into the following combinatorial statement about density in semigroups. Unfortunately we still require the infinite tails condition to make ultralimits work.

Corollary 1.2.29. *Let $\mathcal{F}$ be a cancellable Følner net whose indexing set has infinite tails, and let $E \subseteq G$ be a set of positive upper $\mathcal{F}$-density. Then for any $g \in G$, there exists $n \geq 1$ so that $E \cap g^{-n}E$ also has positive upper $\mathcal{F}$-density.*

Proof. Fix the set E. By Theorem 1.2.26, there is an invariant mean $\mu : \mathcal{P}(G) \to [0,1]$ so that $\mu(A) \leq \delta_{\mathcal{F}}(A)$ for all $A \subseteq G$, with equality when $A = E$.

Now (G, μ) is a finitely additive probability space, and the invariance of μ means that every $g \in G$ acts as a measure-preserving transformation by left multiplication. Since $\mu(E) = \delta_{\mathcal{F}}(E) > 0$, the Poincaré Recurrence Theorem 1.2.28 implies that there exists $n \geq 1$ so that $E \cap g^{-n}E$ has positive measure with respect to μ. But now we are done because of the inequality

$$0 < \mu(E \cap g^{-n}E) \leq \delta_{\mathcal{F}}(E \cap g^{-n}E). \qquad \square$$

We note that the cancellable and infinite tails conditions are automatic if G is already a countable and left cancellative semigroup; thus we can remove the technical hypotheses of Corollary 1.2.29 in this case.

Corollary 1.2.30. *Let G be a countable, left cancellative semigroup, and let $\mathcal{F}$ be a Følner sequence for G. Let $E \subseteq G$ be a set of positive $\mathcal{F}$-density. Then for any $g \in G$, there exists $n \geq 1$ so that*

$$\delta_{\mathcal{F}}(E \cap g^{-n}E) > 0.$$

Proof. If $\mathcal{F}$ is a Følner *sequence*, then its indexing set $\mathbb{N}$ already has infinite tails. Also, $\mathcal{F}$ is automatically cancellable because G is left cancellative. So the result follows from Corollary 1.2.29. $\square$

Applying this directly to the case where $G = (\mathbb{N}, +)$ and $\mathcal{F} = ([1,n])_{n\geq 1}$ is the net of initial intervals, we recover the following result of Bell–Ghioca–Tucker.

Corollary 1.2.31 (Bell–Ghioca–Tucker [BGT15]). *Let $E \subseteq \mathbb{N}$ be a set of positive natural density. Then there exists $b \geq 1$ such that*

$$\{n \in E : n + b \in E\}$$

has positive natural density.

Proof. By Corollary 1.2.30 applied with $G = \mathbb{N}$, the natural density δ, and $g = 1$, there exists $b \geq 1$ so that

$$E \cap (E - b) = \{n \in E : n + b \in E\}$$

has positive density, as required. $\square$

For the Banach density — which is not a Følner density — we pass through Lemma 1.2.14 to obtain Bell–Ghioca–Tucker's result. Recall that the Banach density is denoted by δ^* (Example 1.2.13).

Corollary 1.2.32. *Let $E \subseteq \mathbb{N}$ be a set of positive Banach density. Then there exists $b \geq 1$ such that*

$$\{n \in E : n + b \in E\}$$

has positive Banach density.

Proof. By Lemma 1.2.14, there is a Følner sequence $\mathcal{F}$ on $\mathbb{N}$ such that $\delta^*(A) \geq \delta_{\mathcal{F}}(A)$ for all $A \subseteq \mathbb{N}$, with equality when $A = E$. Now apply Corollary 1.2.30 to this Følner sequence: we obtain $b \geq 1$ so that $E \cap (E - b)$ has positive $\mathcal{F}$-density. But then

$$0 < \delta_{\mathcal{F}}(E \cap (E - b)) \leq \delta^*(E \cap (E - b))$$

as required. $\square$

1.2.6 Szemerédi's Theorem

In this subsection we specialize to the additive semigroup $(\mathbb{N}, +)$. In this case, a set of positive density in $\mathbb{N}$ admits arbitrarily long arithmetic progressions — this is the famous theorem of Szemerédi. We give a sketch of Furstenberg's proof of Szemerédi's Theorem using Furstenberg's Correspondence Principle. In fact, Theorem 1.2.26 can be viewed as a finitely additive version of the following theorem.

Theorem 1.2.33 (Furstenberg Correspondence)**.** *Let $A \subseteq \mathbb{N}$ be a set of positive density. Then there is a probability space (X, μ), a measure-preserving mapping $\varphi : X \to X$, and a measurable set $E \subseteq X$, such that*

$$\mu(E \cap \varphi^{-k_1}(E) \cap \cdots \cap \varphi^{-k_n}(E)) \leq \delta(A \cap (A - k_1) \cap \cdots \cap (A - k_n))$$

for all $k_1, \ldots, k_n \in \mathbb{N}_0$, with equality only when all $k_i = 0$.

This theorem allows us to convert density-theoretic statements into ergodic statements in measure-preserving dynamical systems, like two sides of the same coin. The below Multiple Recurrence Theorem is the ergodic interpretation of Szemerédi's Theorem.

Theorem 1.2.34 (Furstenberg's Multiple Recurrence Theorem [Fur79])**.** *Let (X, μ) be a probability space, let $\varphi : X \to X$ be a measure-preserving mapping, and let $E \subseteq X$ be a set of positive measure. Then for all $\ell \geq 1$, there exists $b \geq 1$ such that*

$$\mu\left(E \cap \varphi^{-b}(E) \cap \cdots \cap \varphi^{-\ell b}(E)\right) > 0.$$

Note that the Multiple Recurrence Theorem is a vast generalization of the Poincaré Recurrence Theorem, because the latter is exactly the $\ell = 1$ case of the former.

Now we show how Furstenberg's Multiple Recurrence Theorem 1.2.34 implies Szemerédi's Theorem that a set of positive density must contain arbitrarily long arithmetic progressions. In fact, there is a *positive density* set of arithmetic progressions of a given length.

Corollary 1.2.35 (Szemerédi's Theorem [Sze75])**.** *Let $A \subseteq \mathbb{N}$ be a set of positive natural upper density. Then A contains arbitrarily long (but finite) arithmetic progressions. In fact, for each length $\ell \geq 1$, there exists $b \geq 1$ such that*

$$\delta\left(\{a \in A : a, a + b, \ldots, a + \ell b \in A\}\right) > 0.$$

Proof. By the Furstenberg Correspondence Theorem 1.2.33, there is a measure-preserving mapping $\varphi : X \to X$ of a probability space (X, μ), along with a measurable subset $E \subseteq X$, such that

$$\mu(E \cap \varphi^{-k_1}(E) \cap \cdots \cap \varphi^{-k_n}(E)) \leq \delta(A \cap (A - k_1) \cap \cdots \cap (A - k_n)) \qquad (\heartsuit)$$

for all $k_1, \ldots, k_n \in \mathbb{N}_0$, with equality when all $k_i = 0$. Now let $\ell \geq 1$. Then by Furstenberg's Multiple Recurrence Theorem 1.2.34, there exists $b \geq 1$ such that the measurable set

$$E \cap \varphi^{-b}(E) \cap \cdots \cap \varphi^{-\ell b}(E)$$

has positive measure. By inequality $\heartsuit$, this implies that

$$A \cap (A - b) \cap \cdots \cap (A - \ell b) = \{a \in A : a, a + b, \ldots, a + \ell b \in A\}$$

has positive density. This is exactly what was to be shown. $\square$

1.3 Dynamics in Noetherian Spaces

In this section, we apply the notions of *IP set* and *Følner density* to dynamical systems. For a rational map $\varphi : X \dashrightarrow X$ of an algebraic variety X, we investigate the return set

$$E := \{n \geq 0 : \varphi^n(x) \in C\},$$

where $x \in X$ is a point and C is a subvariety of X. The Dynamical Mordell–Lang Conjecture asserts that if E is infinite, then it contains an arithmetic progression; equivalently, C contains a φ-periodic subvariety. Although this problem remains open in general, a theorem of Bell–Ghioca–Tucker provides an "asymptotic" version of this conjecture, showing that either E has zero upper density or contains an arithmetic progression. Heuristically, their theorem shows that E can be "large" only when it has some reasonable recurrence property. First, we generalize this result to the action of a semigroup on a noetherian space, and investigate when E can be an IP set. Second, we prove that if E is an IP set, then some closed subset of C is invariant for some subsemigroup.

In this section, we introduce the basic definitions and properties of a dynamical system on an algebraic variety, and more generally on *noetherian* topological spaces.

1.3.1 Orbits and Return Sets

In this section we define the orbit of a continuous map $\varphi : X \to X$. To include the action of a rational map on an algebraic variety, we broaden our setting to include partially-defined maps $\varphi : X \dashrightarrow X$.

Let X be a topological space. We write $\varphi : X \dashrightarrow X$ to denote the **germ** of a continuous mapping $\varphi : U \to X$ defined on some open subset U of X; we frequently conflate φ with its germ. Let us denote the domain $\mathrm{dom}(\varphi) := U$. Two such partially-defined mappings may be composed by restricting the domain appropriately; to avoid empty domains, we may assume that X is irreducible (*i.e.* any two nonempty open sets have nonempty intersection). Thus we have defined the compositional semigroup of continuous maps $\varphi : X \dashrightarrow X$, which contains the subsemigroup consisting of (the germs of) *globally*-defined continuous maps $\varphi : X \to X$. The following notations will be used to denote these semigroups:

$$\mathrm{Top}(X) := \{\text{globally-defined continuous maps } \varphi : X \to X\}$$

$$\mathrm{Top}^{\#}(X) := \{\text{partially-defined continuous maps } \varphi : X \dashrightarrow X\}$$

By an **action** (resp. **partial action**) of a semigroup G on X, we mean a semigroup homomorphism $G \to \mathrm{Top}(X)$ (resp. $G \to \mathrm{Top}^{\#}(X)$). We make no effort to distinguish an element $g \in G$ from the corresponding function in $\mathrm{Top}(X)$ or $\mathrm{Top}^{\#}(X)$, so we write gx to denote the image of a point $x \in X$ under an element $g \in G$. We use the notation $G \curvearrowright X$ to denote both actions and partial actions.

Given a partial action $G \curvearrowright X$, a point $x \in X$ is said to have **well-defined G-orbit** if x lies in the domain of every $g \in G$, and also hx lies in the domain of every $g \in G$ for all $h \in G$. Thus the **domain** of the action $G \curvearrowright X$ is the set of points with well-defined G-orbit:

$$\mathrm{dom}(G) := \{x \in X : x, hx \in \mathrm{dom}(g) \text{ for all } g, h \in G\}.$$

There are two advantages to this definition. First, $\mathrm{dom}(G)$ is a G-invariant subset of X: if $x \in \mathrm{dom}(G)$ and $g \in G$, then $gx \in \mathrm{dom}(G)$. Second, the restricted action $G \curvearrowright \mathrm{dom}(G)$ is globally-defined. This frequently allows us to reduce to the case of a globally-defined action.

In this thesis, we are primarily interested in the intersection of an orbit with a given closed set $C \subseteq X$. Thus, for a set $C \subseteq X$ and $x \in \mathrm{dom}(G)$, we define the **return set** of x to C by

$$\mathrm{Ret}(x, C) = \mathrm{Ret}_G(x, C) := \{g \in G : gx \in C\}.$$

This is one of the most important notations in this thesis, because all our main results concern the structure of return sets in dynamical systems.

Example 1.3.1. Fix any continuous partial mapping $\varphi : X \dashrightarrow X$. Then φ induces an action of the semigroup $\mathbb{N}$ on X by

$$\mathbb{N} \to \mathrm{Top}^{\#}(X), \qquad n \mapsto \varphi^n.$$

Conversely, any action $\mathbb{N} \curvearrowright X$ is determined by $1 \mapsto \varphi$.

Example 1.3.2. Let $\varphi_1, \ldots, \varphi_d : X \dashrightarrow X$ be commuting mappings under composition, *i.e.* $\varphi_i \circ \varphi_j = \varphi_j \circ \varphi_i$ for all i, j. These induce an action of $\mathbb{N}^d$ on X by

$$\mathbb{N}^d \to \mathrm{Top}^{\#}(X), \qquad (a_1, \ldots, a_d) \mapsto \varphi_1^{a_1} \circ \cdots \circ \varphi_d^{a_d}.$$

Conversely, any action $\mathbb{N}^d \curvearrowright X$ is determined by $e_i \mapsto \varphi_i$, where $e_i \in \mathbb{N}^d$ is the ith standard unit vector.

1.3.2 Noetherian Spaces

A topological space X is **noetherian** if it does not contain an infinite descending chain of closed subsets; equivalently, X does not contain an infinite ascending chain of open sets. The most salient examples are quasiprojective varieties, which are Noetherian spaces when equipped with the Zariski topology. Noetherian spaces are exactly those that satisfy the **noetherian induction principle**: every nonempty collection of closed subsets of X must have a minimal element. Thus many arguments involving noetherian spaces can be done by assuming we have solved the problem for proper subspaces and proceeding by induction.

Below is a neat characterization of noetherian spaces.

Proposition 1.3.3. *A topological space X is noetherian if and only if every subset of X is compact. Consequently, the only Hausdorff noetherian spaces are the discrete finite sets.*

Proof. Suppose that X is noetherian. Clearly every subset of X is noetherian with the subspace topology; thus it suffices to show that X is compact. Let $(U_i)_{i \in I}$ be an open cover of X indexed by some infinite set I, and denote the open set $U_F := \bigcup_{i \in F} U_i$ for each finite set $F \subseteq I$. Since each U_F is open, the noetherian property allows us to select a maximal such U_F. Then clearly $U_F = X$, so we have obtained a finite subcover.

Conversely, suppose every subset of X is compact. Towards contradiction, assume that there is some infinite ascending chain $U_1 \subseteq U_2 \subsetneq U_3 \subsetneq \cdots$ of open subsets of X. Then by hypothesis, the full union $K := \bigcup_{n\geq 1} U_n$ is compact, so there is a finite subcover $K = U_1 \cup \cdots \cup U_n$ for some $n \geq 1$. But then $U_n = U_{n+1}$, which is a contradiction. Thus there can be no such ascending chain, and we are done.

Now assume X is noetherian and Hausdorff. Then every subset of X is compact, hence closed, so X is discrete. If X contains infinitely many elements $x_1, x_2, x_3, \ldots$, then $\{x_1\} \subsetneq \{x_1, x_2\} \subsetneq \{x_1, x_2, x_3\} \subsetneq$ is an infinite ascending chain of closed sets. Thus X is finite. $\square$

Our main example of noetherian spaces are algebraic varieties.

Example 1.3.4. Any quasiprojective variety X is a noetherian space. Indeed, X would be a subspace of some n-dimensional projective space $\mathbb{P}^n$ (over some field K), so it is enough to show that $\mathbb{P}^n$ is noetherian. But $\mathbb{P}^n$ is a union of finitely many copies of the n-dimensional affine space $\mathbb{A}^n$, so in turn it is enough to show that the affine space is noetherian. This last claim follows from the fact that the polynomial ring $K[x_1, \ldots, x_n]$ is a noetherian ring; this is Hilbert's Basis Theorem [Har77].

1.3.3 IP Return Sets on Noetherian Spaces

Now we begin our investigation of when return sets are IP sets. The key heuristic is that, in a noetherian space, an orbit should not return to a closed set C "too often" — unless it already returns to C periodically. In this subsection, the term "too often" refers to an IP set. But below is an example where the heuristic fails when "too often" means "infinitely often".

Example 1.3.5 ([Lec53])**.** Let $\mathbb{F}_p$ be the field of p elements, and let $K = \mathbb{F}_p(t)$ be the function field in an indeterminate t. Let $X := \mathbb{A}^2(K)$ be the affine plane over K so that X is a noetherian space, and define a linear map

$$\varphi : X \to X, \quad \varphi(x, y) := (tx, (1 + t)y).$$

Let $q := (1, 1) \in X$ and let C be the line $y = 1 + x$:

$$C := \{(x, y) \in X : y = 1 + x\}.$$

Then the associated return set is

$$\mathrm{Ret}_\varphi(q, C) = \{1, p, p^2, p^3, \ldots\}.$$

Indeed, observe that $\varphi^n(q) = (t^n, (1 + t)^n)$, which lays on the line $y = 1 + x$ if and only if

$$(1 + t)^n = 1 + t^n \qquad \Longleftrightarrow \qquad n = p^k \quad \text{for some } k \geq 0.$$

In particular, the return set is infinite and yet not IP. Moreover, $\mathrm{Ret}_\varphi(x, C)$ has zero density with respect to both natural and Banach densities, so it cannot contain an infinite arithmetic progression.

Note that this example relies on the characteristic of K being positive. The Dynamical Mordell–Lang Conjecture implies that an example as above cannot exist in characteristic zero.

Now we prove that if the return set *is* an IP set, then in fact the return must occur periodically. In the case $G = \mathbb{N}$, the word "periodically" would mean "along an infinite arithmetic progression". For general semigroups, we use cosets instead of arithmetic progressions: by a **right coset** in G, we mean a set of the form Hg, where $g \in G$ and H is a subsemigroup of G. Note that the side of the coset is irrelevant when G is a group, due to the identity $Hg = g(g^{-1}Hg)$.

Theorem 1.3.6. *Let G be a semigroup acting partially on a noetherian space X, let $x \in X$ be a point whose G-orbit is defined, and let $C \subseteq X$ be a closed set; define the return set*

$$E_C := \mathrm{Ret}_G(x, C) = \{g \in G : gx \in C\}.$$

If E_C is an IP set, then it contains a right coset of a subsemigroup of G.

Proof. First, we can immediately reduce to the case where G acts by *globally*-defined mappings, simply by replacing X with the G-invariant subspace $X' := \mathrm{dom}(G)$ of points with well-defined G-orbit. Note that X' is nonempty since it contains x. Since noetherian-ness is preserved for taking subspaces, and the return set is unchanged upon restricting the action to X', we may thus make the replacements $X \mapsto X'$ and $C \mapsto C \cap X'$ to assume that every $g \in G$ is globally defined.

Now we proceed by noetherian induction on C; thus assume we have proven the result for $E_{C'}$ for every proper closed subset C' of C.

Let p be an idempotent ultrafilter containing $E := E_C$. Then the set $E^{-p} = \{g \in G : g^{-1}E \in p\}$ is p-large, in particular it is nonempty, so we can select some element $b \in E^{-p}$. Now define the following closed subset of C:

$$C' := C \cap b^{-1}C = \{x \in X : x, bx \in C\}$$

If $C' = C$, then $C \subseteq b^{-1}C$, which means that C is b-invariant. In this case we are done: if $g \in E$ is chosen arbitrarily, then E contains the right coset $\langle b \rangle g$. Here $\langle b \rangle = \{b^n : n \geq 1\}$ is the subsemigroup generated by b.

Thus assume $C' \subsetneq C$. But the return set of C' is $E_{C'} = E \cap b^{-1}E$, which is a member of p (being the intersection of the two p-large sets E and $b^{-1}E$) and so $E_{C'}$ is an IP set. Thus, by noetherian induction, $E_{C'}$ contains a translate of a subsemigroup. We are done because $E_{C'} \subseteq E_C$. $\square$

An equivalent formulation of Theorem 1.3.6 is that if E_C is an IP set, then C must contain a G-periodic closed subset. Here we say that a subset A of X is **G-periodic** if there is a subsemigroup H of G such that A is H-invariant.

Corollary 1.3.7. *If E_C is an IP set, then C contains a G-periodic closed subset C' such that $gx \in C'$ for some $g \in G$.*

Proof. If E_C is IP, then Theorem 1.3.6 implies that there is a subsemigroup H and element $g_0 \in G$ so that $Hg_0 \subseteq E_C$. Now fix any element $h_0 \in H$, and let $y_0 := (h_0 g_0) \cdot x$. Then $y \in C$. Let C' be the closure of the H-orbit of y; we immediately see that $y \in C' \subseteq C$ and that C' is H-invariant. Thus C' is the desired G-periodic closed set. $\square$

Theorem 1.3.6 can be used to give an example of an infinite IP set which is *not* a dynamical return set.

Example 1.3.8. Recall the ternary set $T \subseteq \mathbb{N}$ from Example 1.1.23: it consists of those integers $n \in \mathbb{N}$ whose ternary expansion has no 2's.

$$T = \mathrm{FS}(3^n) = \{3^{n_1} + \cdots + 3^{n_k} : n_1 < \cdots < n_k\}.$$

Thus T is an IP set. But T cannot contain an arithmetic progression because its natural density is zero (see Example 1.2.18). By Theorem 1.3.6, it follows that T cannot be the return set in any action $(\mathbb{N}, +) \curvearrowright X$ on a noetherian space X.

One drawback in Theorem 1.3.6 is that the coset may be a singleton: for example, if G has an identity and $H = \{1\}$ is trivial, then any coset of H is a singleton — so the conclusion is degenerate in this case. In fact, if $x \in C$ then E_C is an IP set because it is a member of the principal ultrafilter δ_1. So Theorem 1.3.6 should be used with caution.

Since $\mathbb{N}^d$ has no idempotent elements (and thus, no principal idempotent ultrafilters), there is no issue of a degenerate IP set. Thus we have the following version of Theorem 1.3.6 for finitely many commuting mappings (for which even the $d = 1$ case is interesting).

Corollary 1.3.9. *Let $\varphi_1, \ldots, \varphi_d : X \dashrightarrow X$ be a finite collection of commuting maps, and let*

$$E_C = \{(n_1, \ldots, n_d) \in \mathbb{N}^d : (\varphi_1^{n_1} \circ \cdots \circ \varphi_d^{n_d})(x) \in C\}.$$

If E_C is an IP set, then it contains a multiprogression, i.e. *a set of the form*

$$\vec{a} + \mathbb{N}\vec{b} = \{(a_1, \ldots, a_d) + n(b_1, \ldots, b_d) : n \geq 1\},$$

where $\vec{a} = (a_1, \ldots, a_d)$ and $\vec{b} = (b_1, \ldots, b_d)$ are positive integer vectors.

Proof. Theorem 1.3.6 implies that E_C contains a coset $\vec{a} + B$ where B is a subsemigroup of $\mathbb{N}^d$. But now, selecting any $\vec{b} \in B$, it is clear that $\vec{a} + \mathbb{N}\vec{b} \subseteq \vec{a} + B \subseteq E_C$. Thus $\vec{a} + \mathbb{N}\vec{b}$ is the desired multiprogression. □

Another way to avoid a trivial coset in Theorem 1.3.6 is by making a few mild assumptions on G; note that this applies when G is a finitely generated abelian group.

Theorem 1.3.10. *Suppose that G is a left cancellative semigroup with at most finitely many torsion elements. Suppose that there is a sequence of* distinct *elements $(g_n)_{n \geq 1}$ such that $\mathrm{FP}(g_n) \subseteq E_C$. Then E_C contains a coset of an infinite subsemigroup.*

Proof. Since G has only finitely many torsion elements, we can assume that all the g_n's have infinite order without loss of generality (by replacing the sequence (g_n) with a sufficiently late tail-end). Also, since E_C contains the finite product set generated by a sequence of *distinct* elements, Theorem 1.1.32 implies that E_C belongs to a *nonprincipal* idempotent ultrafilter $p \in \beta G \setminus G$.

Now follow the proof of Theorem 1.3.6 until the point where we select an element $b \in E^{-p}$: since p is nonprincipal, we know that E^{-p} is infinite, so we can select some element $b \in E^{-p}$ of infinite order. Thus the subsemigroup $\langle b \rangle$ is infinite, and the rest of the proof is identical to Theorem 1.3.6. □

In the case $G = \mathbb{N}$, it would be nice to obtain a neat statement such as "E_C is a finite union of arithmetic progressions with a non-IP set". Unfortunately, an adaptation of the argument in [BGT15, Theorem 1.4] would involve translating a IP set, which may not result in an IP set (*e.g.* $2\mathbb{N}$ is IP whereas $1 + 2\mathbb{N}$ is not IP).

1.3.4 Return Sets of Positive Density

In this subsection, we turn our attention to the action of an amenable semigroup G on a noetherian space X. In the case $G = \mathbb{N}$ we recover the "weak" Dynamical Mordell–Lang Conjecture of Bell–Ghioca–Tucker. Our prototypical theorem says that if a return set has positive measure with respect to some invariant mean on G, then it contains a coset of a subsemigroup.

Theorem 1.3.11. *Let G be an amenable semigroup acting on a noetherian space X, let $x \in X$ be a point with well-defined G-orbit, and let $C \subseteq X$ be a closed set; define the return set*

$$E_C := \mathrm{Ret}_G(x, C) = \{g \in G : gx \in C\}.$$

If E_C has positive measure with respect some invariant mean on G, then E_C contains a right coset of a subsemigroup of G.

Proof. The argument is very similar to that of Theorem 1.3.6, except in place of the idempotence property "$E \cap g^{-1}E \in p$", we apply the Poincaré Recurrence Theorem 1.2.28.

As in Theorem 1.3.6, we immediately reduce to the case where every $g \in G$ is a globally-defined mapping on X. Let μ be an invariant mean such that $\mu(E_C) > 0$, and fix an arbitrary element $b \in G$. Then by the Poincaré Recurrence Theorem, there exists $n \geq 1$ so that

$$\mu(E_C \cap b^{-n} E_C) > 0.$$

But if we let $C' := C \cap b^{-n}C$, it is clear that the return set to C' is exactly

$$E_{C'} = E_C \cap b^{-n} E_C.$$

Now C' is a closed subset of X. If $C' \subsetneq C$, then we may proceed by noetherian induction. Otherwise $C' = C$, which implies that C is b^n-invariant, and therefore E_C contains the coset $\langle b^n \rangle g$ for any $g \in E_C$. Either way, the proof is complete. □

Theorem 1.3.11 is not practical, since our only examples of invariant means are abstract ultralimit constructions; however, Corollary 1.2.27 allows us to replace invariant means by Følner densities, of which we have many useful examples.

Corollary 1.3.12. *Let G be a semigroup satisfying the strong Følner condition, and suppose that E_C has positive density with respect to a Følner net on G. Then E_C contains a coset of a subsemigroup.*

Proof. If E_C has positive density, then by Corollary 1.2.27, there is an invariant mean μ such that $\mu(E_C) > 0$. It follows from Theorem 1.3.11 that E_C contains a coset of a subsemigroup. □

Theorem 1.3.11 has the same issues as its combinatorial cousin Theorem 1.3.6: the resulting coset may be a singleton. The problem stems from the arbitrary choice of b in the proof, but we can solve this by choosing b to have infinite order, *i.e.* b generates an infinite subsemigroup.

Corollary 1.3.13. *Suppose that G is amenable with at least one element $b \in G$ of infinite order, suppose that $\mu(E_C) > 0$ for some invariant mean μ on G. Then E_C contains a coset of an infinite subsemigroup of G.*

Proof. Follow the proof of Theorem 1.3.11 — except instead of selecting $b \in G$ arbitrarily, select b of infinite order and note that $\langle b^n \rangle$ must be infinite. $\square$

Our analysis recovers a result of Bell–Ghioca–Tucker for a single mapping $\varphi : X \dashrightarrow X$, which is Corollary 1.3.12 for the Banach density on $\mathbb{N}$. In fact, we apply our results with $G = \mathbb{N}^d$ to get a version for several commuting maps just like Corollary 1.3.9. Recall the **box Banach density** from Example 1.2.16:

$$\delta^*(E) := \limsup_{|B|\to\infty} \frac{|E \cap B|}{|B|} \quad \text{for } E \subseteq \mathbb{N}^d,$$

where the limsup is taken over all boxes $B = [a_1, b_1] \times \cdots \times [a_d, b_d]$. In the below theorem, we define a **multiprogression** in $\mathbb{N}^d$ to be a set of the form

$$\vec{a} + \mathbb{N}\vec{b} = \{(a_1, \ldots, a_d) + n(b_1, \ldots, b_d) : n \geq 1\},$$

where $\vec{a} = (a_1, \ldots, a_d), \vec{b} = (b_1, \ldots, b_d) \in \mathbb{N}^d$ are vectors of positive integers.

Corollary 1.3.14. *Let $\varphi_1, \ldots, \varphi_d : X \dashrightarrow X$ be a finite collection of commuting maps, let $x \in X$ be a point in the domain of $\varphi_1^{n_1} \circ \cdots \circ \varphi_d^{n_d}$ for all $n_1, \ldots, n_d \in \mathbb{N}$, let $C \subseteq X$ be a closed set, and consider the return set*

$$E_C := \{(n_1, \ldots, n_d) \in \mathbb{N}^d : (\varphi_1^{n_1} \circ \cdots \circ \varphi_d^{n_d})(x) \in C\}.$$

If $\delta^*(E_C) > 0$, then E_C contains a multiprogression.

For $d = 1$, this is [BGT15, Proposition 3.1].

Proof. Note that $\varphi_1, \ldots, \varphi_d$ induce a semigroup action $\mathbb{N}^d \curvearrowright X$, where

$$(n_1, \ldots, n_d) \mapsto \varphi_1^{n_1} \circ \cdots \circ \varphi_d^{n_d}.$$

If $\delta^*(E_C) > 0$, then by Lemma 1.2.17, E_C has positive density with respect to some Følner sequence. The result now follows from Corollary 1.3.12, noting that that every coset of a subsemigroup of $\mathbb{N}^d$ contains a multiprogression. $\square$

Chapter 2

Automorphism Dynamics in Polycyclic Groups

Motivated by the noetherian spaces used in Chapter 1, in this chapter we examine groups satisfying a an ascending chain condition on their subgroups. Our setting will be the famous class of *polycyclic-by-finite groups*, which are groups built from extensions of cyclic and finite groups. We show a "weak" Dynamical Mordell–Lang type theorem for an automorphism $\varphi : G \to G$ of a polycyclic-by-finite group G: for a normal subgroup $N \trianglelefteq G$ and element $x \in G$, we show that if $\varphi^n(x) \in N$ for n in a set of positive density, then in fact the intersection occurs for n in an infinite arithmetic progression.

2.1 Polycyclic Groups

In this section, we introduce polycyclic-by-finite groups as iterated extensions of cyclic and finite groups. Examples of these groups include finitely generated nilpotent groups and solvable noetherian groups. We define the *Hirsch length* of a polycyclic group, using the Schreier Refinement Theorem to prove that Hirsch length is well-defined.

A good introduction to polycyclic groups and Hirsch length can be found in [Mann], and we loosely follow this source for the exposition below.

2.1.1 Subnormal Series and Extensions

A **cyclic-by-finite group** is one containing a cyclic normal subgroup of finite index. Such G fits into a short exact sequence

$$1 \to N \to G \to G/N \to 1$$

where the second term is cyclic and the fourth term is finite. More generally, we can define *X-by-Y* groups — for example, an abelian-by-finite group would have a normal abelian subgroup of finite index, and a finite-by-abelian group would have a finite normal subgroup with abelian quotient. This notation can be nested: for example, a group like $(\mathbb{Z} \times \mathbb{Z}) \rtimes \mathbb{Z}_2$ is (cyclic-by-cyclic)-by-cyclic. To deal with these iterated extensions, we introduce subnormal series.

A **subnormal series** in a group G is a finite descending chain of subgroups of the form

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_m = \{1\}$$

where each G_i is a normal subgroup of G_{i-1} (but we do not require that G_i is normal in G). The quotient groups G_i/G_{i+1} are called the **factors** of this subnormal series. For example, if G is (abelian-by-finite)-by-cyclic, then G has a normal abelian-by-finite subgroup G_1 such that the quotient G/G_1 is cyclic, and in turn G_1 has an abelian normal subgroup G_2 of finite index. In total, we have a subnormal series $G \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \{1\}$ where the factors G/G_1, G_1/G_2, and G_2 are respectively cyclic, finite, and abelian. This is an example of how we will use subnormal series to represent iterated extensions.

Finally, a **polycyclic group** is a group admitting a subnormal series all of whose factors are cyclic; such a series will be referred to as **cyclic series**. Such a group is obtained by taking repeated extensions by cyclic groups. Of course, one can similarly define *poly-X groups* where X is some group-theoretic property; for example, polyabelian groups are better known as **solvable** groups.

Example 2.1.1. Cyclic groups are obviously polycyclic, with a cyclic series of length 1. Thus $\mathbb{Z}$ is polycyclic, and $\mathbb{Z}/n\mathbb{Z}$ is polycyclic for any $n \geq 1$.

Example 2.1.2. A direct product of two polycyclic groups is again polycyclic. Recall that if G, H are two groups, then they each embed as normal subgroups of the direct product $G \times H$, and we therefore have an extension

$$1 \to G \to G \times H \to H \to 1.$$

Thus G is a polycyclic normal subgroup of $G \times H$ such that $(G \times H)/G \simeq H$ is polycyclic. It follows that $G \times H$ is polycyclic by Proposition 2.1.11 below.

Now we can see that any finitely generated abelian group is polycyclic, because such a group is a direct product of finitely many cyclic groups.

Example 2.1.3. Generalizing the last example: the *semidirect* product of two polycyclic groups is again polycyclic. Recall that if $\sigma : H \to \mathrm{Aut}(G)$ is a group homomorphism, then we can define a multiplication on $G \times H$ using σ as a twist:

$$(g, h)(g', h') = (g\sigma_h(g'), hh').$$

Identifying G, H with $G \times \{1\}$, $\{1\} \times H$ respectively, this product can be remembered as $\sigma_h(g) = hgh^{-1}$, which makes every σ_h into an inner automorphism. This operation results in a group called the **semidirect product**, denoted $G \rtimes_\sigma H$. Now $g \mapsto (g, 1)$ gives an embedding of G as a normal subgroup of $G \rtimes_\sigma H$, and the corresponding quotient is $(G \rtimes_\sigma H)/G \simeq H$. Thus $G \rtimes_\sigma H$ fits in a short exact sequence

$$1 \to G \to G \rtimes_\sigma H \to H \to 1.$$

If G, H are polycyclic, it follows from Proposition 2.1.11 (below) that $G \rtimes_\sigma H$ is polycyclic.

Example 2.1.4. The cyclic group $\mathbb{Z}_2 \simeq \{1, -1\}$ acts on $\mathbb{Z}$ by multiplication. Since $\mathbb{Z}_2$ and $\mathbb{Z}$ are both polycyclic, the resulting semidirect product $D_\infty := \mathbb{Z}_2 \ltimes \mathbb{Z}$ is also polycyclic. This is known as the **infinite dihedral group**. A presentation for this nonabelian group is

$$D_\infty \simeq \langle x, y : xy = y^{-1}x, x^2 = 1\rangle.$$

Example 2.1.5. Poly-$\mathbb{Z}$ groups have a special structure that we investigate here. First, note that a short exact sequence of the form

$$1 \to N \to G \to \mathbb{Z} \to 1$$

must split: *i.e.* the map $G \to \mathbb{Z}$ has a right inverse homomorphism $\mathbb{Z} \to G$, say $n \mapsto z_n$. This is because $\mathbb{Z}$ is the free group on one generator, so we can define $\mathbb{Z} \to G$ on the generator and extend to a homomorphism. A split extension always results in a semidirect product: thus

$$G \simeq N \rtimes \mathbb{Z}.$$

This proves that any extension with infinite cyclic quotient must split as a semidirect product. An inductive argument based on this observation shows that any poly-$\mathbb{Z}$ group G must be isomorphic to an iterated semidirect product of the form

$$G \simeq (((\mathbb{Z} \rtimes \mathbb{Z}) \rtimes \mathbb{Z}) \rtimes \cdots) \rtimes \mathbb{Z}.$$

The choice of automorphism at each extension allows one to create a myriad of examples from this construction. In the next section, we will see that any virtually polycyclic group is a finite extension of a poly-$\mathbb{Z}$ group of the above form.

Example 2.1.6. Let $\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ denote the cyclic group of order 2. Then $\mathbb{Z}_2$ acts on $\mathbb{Z}\times\mathbb{Z}$ by swapping coordinates: $(x, y) \mapsto (y, x)$. The resulting semidirect product $(\mathbb{Z} \times \mathbb{Z}) \rtimes \mathbb{Z}_2$ is polycyclic.

Example 2.1.7. The **Heisenberg group** is the subgroup of $\mathrm{GL}_3(\mathbb{Z})$ consisting of all 3×3 upper-triangular matrices with 1's along the diagonal.

$$H = \begin{bmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{bmatrix} = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{Z} \right\}.$$

This group has the following presentation:

$$H \simeq \langle x, y, z : z = [x, y], [x, z] = [y, z] = 1 \rangle$$

where x, y, z are the three matrices

$$x := \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad y := \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \quad z := \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

From this, it follows that $H_1 := \langle x, z \rangle$ is a normal subgroup of H and $H_2 := \langle x \rangle$ is a normal subgroup of H_1, so that we have a cyclic series

$$H \trianglerighteq \langle x, z \rangle \trianglerighteq \langle x \rangle \trianglerighteq \{1\}.$$

Therefore H is polycyclic.

Example 2.1.8. Recall that a **solvable group** is one admitting a subnormal series with abelian factors; thus every polycyclic group is solvable. But here we use wreath products to give an example of a finitely generated solvable group which is *not* polycyclic.

First we define the lamplighter group L as the wreath product $\mathbb{Z}_2 \wr \mathbb{Z}$. Let $U := \bigoplus_{i\in\mathbb{Z}} \mathbb{Z}_2$ be the abelian group of all finitely supported, doubly infinite sequences

$$u = (u_n)_{n\in\mathbb{Z}} = (\dots, u_{n-1}, u_n, u_{n+1}, \dots)$$

with entries mod 2, under termwise addition. Think of these as an infinite line of street lamps, each of which is either "on" or "off", with only finitely many lit at once. Then we have a group action $\mathbb{Z} \curvearrowright U$ by shifting: for $g \in \mathbb{Z}$ and a sequence $u = (u_n) \in U$, we define the shifted sequence $g \cdot u \in U$ by

$$(g \cdot u)_n := u_{n-g}.$$

Thus we have a homomorphism $\mathbb{Z} \to \mathrm{Aut}(U)$. The resulting semidirect product is called the **restricted wreath product** $\mathbb{Z}_2 \wr \mathbb{Z}$:

$$L := \mathbb{Z}_2 \wr \mathbb{Z} := U \rtimes \mathbb{Z}.$$

This is also known as the **lamplighter group**: there is a generator a of order 2 representing how the lamplighter can switch a lamp on/off, and a generator b of infinite order representing how the lamplighter moves one lamp to the next. More concretely, L has the following presentation with infinitely many relations:

$$L = \left\langle a, b : (ab^n ab^{-n})^2 = 1 \text{ for all } n \in \mathbb{Z} \right\rangle.$$

Thus L is finitely generated. To see that L is solvable, note that it fits in a short exact sequence

$$1 \to U \to L \to \mathbb{Z} \to 1$$

where the second term is abelian and the third term is infinite cyclic. Thus L is abelian-by-cyclic, thus solvable.

On the other hand, L is not polycyclic, or even polycyclic-by-finite. Indeed, every subgroup of a polycyclic-by-finite group is finitely generated by Proposition 2.1.20 below, and yet L has the infinitely generated subgroup $U = \bigoplus_{i\in\mathbb{Z}} \mathbb{Z}_2$. Therefore the lamplighter group is not polycyclic.

Example 2.1.9. Every finitely generated nilpotent group is polycyclic. Recall that a group G is **nilpotent** if its **lower central series**

$$G = \gamma_0(G) \trianglerighteq \gamma_1(G) \trianglerighteq \gamma_2(G) \trianglerighteq \cdots$$

defined recursively by

$$\gamma_{i+1}(G) := [\gamma_i(G), G]$$

terminates with $\gamma_n(G) = 1$ for some n. For a proof that all finitely generated nilpotent groups are polycyclic, see [Mann, Theorem 2.18].

Example 2.1.10. Polycyclic groups have deep connections to linear groups. Malcev showed that a solvable subgroup of $\mathrm{GL}_n(\mathbb{Z})$ is polycyclic [Mal]; conversely, Auslander–Swan showed that *every* polycyclic group admits a faithful representation in $\mathrm{GL}_n(\mathbb{Z})$ for some $n \geq 1$ [Swan].

Below we verify various permanence properties of polycyclicity that were used in the above examples: polycyclicity is preserved for subgroups, quotients, and extensions.

Proposition 2.1.11. *Let G be a group.*

(a) *Let $H \leq G$. If G is polycyclic, then so is H.*

(b) *Consider a short exact sequence*

$$1 \to N \to G \to G/N \to 1$$

where N is a normal subgroup of G. Then G is polycyclic if and only if N and G/N are both polycyclic.

Proof. (a) We intersect H with an appropriate subnormal series of G. Let

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = \{1\}$$

be a cyclic series for G. Then we have the restricted subnormal series

$$H = H \cap G_0 \trianglerighteq H \cap G_1 \trianglerighteq \cdots \trianglerighteq H \cap G_m = \{1\},$$

whose factors are cyclic because of the embeddings $(H \cap G_i)/(H \cap G_i) \hookrightarrow G_i/G_{i+1}$ and the fact that a subgroup of a cyclic group is cyclic. This shows that the above is a cyclic series and we are done.

(b) First suppose that G is polycyclic; then N is polycyclic by (a). To see that G/N is polycyclic: start with any cyclic series $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = \{1\}$ for G, and take the quotient modulo N to get a subnormal series

$$\frac{G}{N} = \frac{NG_0}{N} \trianglerighteq \frac{NG_1}{N} \trianglerighteq \frac{NG_2}{N} \trianglerighteq \cdots \trianglerighteq \frac{NG_m}{N} = \{1\}$$

for G/N. The factors of this series are cyclic because of the inclusions

$$\frac{NG_i/N}{NG_{i+1}/N} \hookrightarrow \frac{G_i}{G_{i+1}}.$$

This proves that G/N is polycyclic.

Conversely, suppose that N and G/N are both polycyclic. Then a cyclic series $G/N = Q_0 \trianglerighteq \cdots \trianglerighteq Q_m = \{1\}$ corresponds, via the quotient map, to a subnormal series of the form $G = G_0 \trianglerighteq \cdots \trianglerighteq G_m = N$, where $G_i/N = Q_i$; the factor G_i/G_{i+1} is cyclic because it naturally embeds in the cyclic group Q_i/Q_{i+1}. Next, we append a cyclic series for N to the bottom of this one. Indeed, if $N = N_0 \trianglerighteq \cdots \trianglerighteq N_n = \{1\}$ is a cyclic series for N, then we can create a subnormal series for G as follows:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = N = N_0 \trianglerighteq N_1 \trianglerighteq \cdots \trianglerighteq N_n = \{1\}.$$

This is a cyclic series because it is the appension of two such. This proves that G is polycyclic. $\square$

We conclude this subsection with an important property of polycyclic groups.

Proposition 2.1.12. *Every polycyclic group is finitely generated.*

Proof. Suppose that

$$G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_m = \{1\}$$

is a cyclic series for G. We prove the proposition by induction on m. If $m = 1$, then $G_1 = \{1\}$ and $G \simeq G/G_1$ is already cyclic, hence finitely generated.

Now assume $m \geq 2$. It's clear that G_1 has a subnormal series of length $m-1$, and G/G_1 has a subnormal series of length 1 because it is already cyclic. By induction, G_1 and G/G_1 are finitely generated. But now we have a short exact sequence

$$1 \to G_1 \to G \to G/G_1 \to 1$$

where the second and fourth terms are finitely generated groups. It is a standard group theory exercise to show that the middle term in such a sequence must also be finitely generated; therefore G is finitely generated. $\square$

2.1.2 Virtually Polycyclic Groups

A group is **virtually polycyclic** if it admits a polycyclic subgroup of finite index. At first, this seems to be slightly weaker than being polycyclic-by-finite, which requires the admission of a *normal* polycyclic subgroup of finite index. But by using the following group-theoretic trick, we will see that "virtually polycyclic" and "polycyclic-by-finite" are in fact equivalent.

Lemma 2.1.13. *Let G be a group and let H be a subgroup of finite index. Then:*

(a) *H contains a finite index subgroup N such that N is normal in G.*

(b) *Suppose that G is finitely-generated. Then H contains a finite index subgroup N such that N is invariant for every endomorphism of G.*

Proof. (a) Let $d := [G : H]$ be the number of distinct left cosets of H in G. The group action $G \curvearrowright G/H$ manifests itself as a homomorphism

$$G \to \mathrm{Sym}(G/H),$$

where $\mathrm{Sym}(G/H)$ is the symmetric group on the coset space G/H. Let N be the kernel of this homomorphism:

$$N = \{g \in G : g(xH) = xH \text{ for all } x \in G\}.$$

Clearly $[G : N] \leq |\mathrm{Sym}(G/H)| = d!$, so N has finite index in G. Also, notice that $N \leq H$: indeed, H is equal to the stabilizer of the coset H under the action $G \curvearrowright G/H$, and this stabilizer contains the kernel N. Thus $H \geq N$ and N is the desired normal subgroup.

(b) The assumption that G is finitely generated can be used to show that G has at most finitely many subgroups of a given index.

Claim A: Let $d \geq 1$. Then G has only finitely many subgroups of index d.

To prove this, let K be a subgroup of index d. Then as in part (a), K can be realized as the stabilizer of the point $K \in G/K$ under the left-translation action

$G \curvearrowright G/K$; conversely, given a transitive action $G \curvearrowright \{1, \ldots, d\}$, the stabilizer of any given element is a subgroup of index d. This gives a bijection between:

$$\left\{ \begin{matrix} \text{subgroups } K \le G \\ \text{of index } [G:K] = d \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{stabilizers of a point} \\ \text{in a transitive group action} \\ G \curvearrowright \{1, \ldots d\} \end{matrix} \right\}$$

On the other hand, there are at most finitely many such group actions: a group action $G \to S_d$ is determined by where it sends a finite generating set of G, and there are only finitely many such choices because S_d is finite. This proves Claim A.

Now take $d := [G : H]$ to be the index of H in G; then by Claim A, there are only finitely many subgroups of G of index $\le d$. Let N be the intersection of these subgroups:

$$N := \bigcap_{\substack{K \le G \\ [G:K] \le d}} K.$$

Clearly H is among the subgroups in the above intersection, so $N \le H$. Also, $[G : N] < \infty$ because N is a finite intersection of finite index subgroups.

Finally, we prove that N is invariant for every endomorphism of G. Let $\varphi : G \to G$ be an endomorphism and let $K \le G$ have index $\le d$. We will show that the preimage $\varphi^{-1}(K)$ also has index $\le d$.

Claim B: $[G : \varphi^{-1}(K)] \le d$.

For this, note what happens when we take a preimage of a coset: it is either empty, or it is a coset of the preimage.

$$\varphi^{-1}(tK) = \begin{cases} s\varphi^{-1}(K) & \text{if } t = \varphi(s) \text{ for some } s \in G, \\ \varnothing & \text{otherwise.} \end{cases} \tag{$\spadesuit$}$$

Now write G as a disjoint union of cosets $G = t_1 K \sqcup \cdots \sqcup t_m K$ where $m \le d$. Then taking preimages, we get a disjoint union

$$G = \varphi^{-1}(G) = \varphi^{-1}(t_1 K) \sqcup \cdots \sqcup \varphi^{-1}(t_m K).$$

By formula $\spadesuit$, each of these cosets is either a coset of $\varphi^{-1}(K)$ or else it is empty. Thus we see that G is a union of at most d cosets of $\varphi^{-1}(K)$:

$$G = s_1 \varphi^{-1}(K) \sqcup \cdots \sqcup s_n \varphi^{-1}(K)$$

for some $s_1, \ldots, s_n$, where $n \le m \le d$. This proves Claim B.

Now we are ready to show that N is φ-invariant. Let $x \in N$; we must show that $\varphi(x)$ belongs to every subgroup of index $\le d$. But if K is one such subgroup, then so is $\varphi^{-1}(K)$ by Claim B, so $x \in \varphi^{-1}(K)$. This means that $\varphi(x) \in K$. Thus $\varphi(x) \in N$, proving that N is φ-invariant. □

Lemma 2.1.13(a) proves that there is no difference between "polycyclic subgroup of finite index" and "*normal* polycyclic subgroup of finite index", because we can always drop down to a normal subgroup. Thus

"polycyclic-by-finite" = "virtually polycylic"

The same holds when "polycyclic" is replaced by any property which is closed for subgroups:

$$\begin{aligned}\text{"abelian-by-finite"} &= \text{"virtually abelian"} \\ \text{"(poly-}\mathbb{Z}\text{)-by-finite"} &= \text{"virtually poly-}\mathbb{Z}\text{"}\end{aligned}$$

and so on. From now on, we use these equivalences liberally.

Now we provide several equivalent characterizations of virtually polycyclic groups.

Theorem 2.1.14. *The following are equivalent for a group G:*

(a) *G is virtually polycyclic.*

(b) *G is poly-$\{$cyclic, finite$\}$,* i.e. *G admits a subnormal series each of whose factors are either cyclic or finite.*

(c) *G is (poly-$\mathbb{Z}$)-by-finite.*

While property (b) states that G has a subnormal series whose factors are either finite or cyclic, property (c) allows us to assume that the first factor is finite and the rest are *infinite* cyclic. So all finite parts can be "shuffled" to the top while keeping the infinite factors below.

Proof. "(a) $\implies$ (b)": Let G be virtually polycyclic; then G has a finite index subgroup H such that H is polycyclic. By Lemma 2.1.13(a), we may assume that H is normal in G. To show that G is poly-$\{$cyclic, finite$\}$, simply start with a cyclic series for H, say

$$H = H_0 \trianglerighteq \cdots \trianglerighteq H_m = \{1\},$$

and then append G to the top of this series:

$$G \trianglerighteq H = H_0 \trianglerighteq \cdots \trianglerighteq H_m = \{1\}.$$

This is a subnormal series for G, and the first factor G/H is finite while the rest of the factors are cyclic. This proves that G is poly-$\{$cyclic, finite$\}$.

"(b) $\implies$ (c)": Let G be poly-$\{$cyclic, finite$\}$, so that there is a subnormal series

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = \{1\}$$

such that each factor G_i/G_{i+1} is cyclic or finite. We proceed by induction on m. If $m = 1$, then G is either finite (in which case $\{1\}$ is a polycyclic subgroup of finite index) or cyclic (in which case G is itself a polycyclic subgroup of finite index). Either way, G is virtually polycyclic.

Now suppose $m \geq 1$. Then $N := G_1$ is a poly-$\{$cyclic, finite$\}$ normal subgroup of G, so N is (poly-$\mathbb{Z}$)-by-finite by induction, which means that N has a normal poly-$\mathbb{Z}$ subgroup N_0 of finite index. Now G/N is either finite or cyclic. If G/N is finite, then N_0 is a finite index poly-$\mathbb{Z}$ subgroup of G, and we can assume that N_0 is normal in G by Lemma 2.1.13(a). This proves that G is (poly-$\mathbb{Z}$)-by-finite, at least in the case where G/N is finite.

Thus we are left with the case where G/N is infinite cyclic. Let $z \in G$ be a preimage of a generator for G/N. Maintaining the notation that N_0 is a normal poly-$\mathbb{Z}$ subgroup of N with $[N : N_0] < \infty$, we let $H := N_0\langle z\rangle$, noting that H is poly-$\mathbb{Z}$ because it fits in an extension

$$1 \to N_0 \to H \to \langle z\rangle \to 1$$

and poly-$\mathbb{Z}$ groups are preserved for such extensions (same proof as Proposition 2.1.11(b)). Thus we are done if we prove that H has finite index in G. For this, we use the fact that $[N : N_0] < \infty$, so that we can write N as a finite union of cosets

$$N = t_1N_0 \sqcup \cdots \sqcup t_dN_0$$

where $t_1, \ldots, t_d \in N$. Therefore,

$$\begin{aligned} G &= N\langle z\rangle \\ &= (t_1N_0 \sqcup \cdots \sqcup t_dN_0)\langle z\rangle \\ &= t_1N_0\langle z\rangle \sqcup \cdots \sqcup t_dN_0\langle z\rangle \\ &= t_1H \sqcup \cdots \sqcup t_dH. \end{aligned}$$

Thus G is a union of finitely many cosets of H, so $[G : H] < \infty$. This proves that H is a poly-$\mathbb{Z}$ subgroup of G of finite index. Using Lemma 2.1.13(a), we can further shrink H to assume that it is a *normal* poly-$\mathbb{Z}$ subgroup of G of finite index, which witnesses that G is (poly-$\mathbb{Z}$)-by-finite.

"(c) $\Longrightarrow$ (a)": This statement is a tautology. If G is (poly-$\mathbb{Z}$)-by-finite, then it has a normal poly-$\mathbb{Z}$ subgroup N of finite index; in particular, N is a polycyclic subgroup of finite index. $\square$

Here are some examples of polycyclic-by-finite groups.

Example 2.1.15. Any polycyclic group is *a fortiori* virtually polycyclic.

Example 2.1.16. Any finite group is virtually polycyclic (because the trivial subgroup is polycyclic of finite index), but not necessarily polycyclic, or even solvable. For example, the symmetric group S_5 is not solvable, and therefore not polycyclic.

Example 2.1.17. If G is a polycyclic and F is any finite group acting on G by automorphisms, then the semidirect product $G \rtimes F$ is polycyclic-by-finite.

2.1.3 Noetherian Groups

Next, we set out to prove that every virtually polycyclic group is *noetherian*. Recall that a group G is **noetherian** if it satisfies the ascending chain condition on subgroups: that is, given an ascending chain of subgroups

$$H_1 \subsetneq H_2 \subsetneq H_3 \subsetneq \cdots,$$

there exists $n \geq 1$ so that $H_n = H_{n+1} = H_{n+2} = \cdots$. In fact, this ascending chain condition was our original motivation for the connection between polycyclic groups and algebraic dynamics. It is worth remarking that, at present, virtually polycyclic groups G are the *only* known examples where the group ring $\mathbb{C}[G]$ is noetherian, and it is conjectured that there are no other examples [Ivan]

It is a standard group theory exercise to show that noetherian-ness is equivalent to "every subgroup is finitely generated".

Proposition 2.1.18. *A group G is noetherian if and only if every subgroup of G is finitely generated.*

Now we show that every virtually polycyclic group is noetherian. This is apparent from the following two properties.

Proposition 2.1.19. (a) *A subgroup of a polycyclic-by-finite group is again such.*

(b) *Every virtually polycyclic group is finitely generated.*

Proof. (a) Let G be virtually polycyclic and let H be a finite index polycyclic subgroup of G. If $K \leq G$ is some subgroup, then $K \cap H$ is polycyclic (being a subgroup of H), and it is also easy to see that $K \cap H$ has finite index in K. Thus K is virtually polycyclic.

(b) Let G be a virtually polycyclic group, so that G has a polycyclic subgroup H of finite index. Then H is finitely generated by Proposition 2.1.12. Now it is a straightforward group theory exercise to show that if H is finitely generated and $[G : H] < \infty$, then G is also finitely generated. □

Corollary 2.1.20. *Every virtually polycyclic group is noetherian.*

Proof. Let G be virtually polycyclic. Then every subgroup of G is virtually polycyclic and finitely generated by Proposition 2.1.19. Thus G is noetherian by Proposition 2.1.18. □

Corollary 2.1.21 (Zassenhaus [Za69])**.** *A group is polycyclic if and only if it is solvable and noetherian.*

Proof. It is clear that a polycyclic group is solvable and noetherian. Conversely, suppose that G is solvable and noetherian: then G has a subnormal series

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = 1$$

with all factors G_i/G_{i+1} abelian. If $m = 1$ then G is a finitely generated abelian group, thus polycyclic. If $m \geq 2$, then G fits into an extension

$$1 \to G_1 \to G \to G/G_1 \to 1$$

with G/G_1 finitely generated abelian (hence polycyclic) and G_1 polycyclic by induction. Since an extension of polycyclic groups is polycyclic by Proposition 2.1.11(b), we conclude that G is polycyclic. □

To make a point later in the thesis, we note an independently interesting dynamical property of noetherian groups.

Proposition 2.1.22. *Every surjective endomorphism of a noetherian group is injective.*

Proof. Let $\varphi : G \to G$ be a surjective endomorphism of a noetherian group G. Then the kernels of iterates of φ form an ascending chain:

$$\ker(\varphi) \subseteq \ker(\varphi^2) \subseteq \ker(\varphi^3) \subseteq \cdots$$

and so the noetherian property implies that

$$\ker(\varphi^n) = \ker(\varphi^{n+1}) \quad \text{for some } n \geq 1.$$

Now we show that φ is injective by showing $\ker(\varphi) = 1$. Indeed, if $\varphi(x) = 1$, then since φ^n is surjective, we may write $x = \varphi^n(y)$ for some $y \in G$. But then

$$1 = \varphi(x) = \varphi^{n+1}(y)$$

so that $y \in \ker(\varphi^{n+1})$. This implies $y \in \ker(\varphi^n)$ by choice of n, so $x = \varphi^n(y) = 1$. Thus we have shown that φ is injective. $\square$

2.2 Hirsch Length

In this section we define the Hirsch length of a polycyclic-by-finite group, by taking a cyclic-finite series and counting the number of infinite cyclic factors. We show that this is independent of the choice of series. The Hirsch length functions as a "rank" number associated with a polycyclic-by-finite group, generalizing the usual rank of a finitely generated abelian group, so many arguments can be made by induction on the Hirsch length.

2.2.1 Schreier Refinement Theorem

Consider a subnormal series $\mathcal{A} = \{G = A_0 \trianglerighteq \cdots \trianglerighteq A_m = 1\}$ of a group G. A **refinement** of $\mathcal{A}$ is another series $\mathcal{B} = \{G = B_0 \trianglerighteq \cdots \trianglerighteq B_n = 1\}$ such that

$$\{A_0, \ldots, A_m\} \subseteq \{B_0, \ldots, B_m\};$$

i.e. some B_i terms are inserted into the first series to obtain the second. We write $\mathcal{A} \leq \mathcal{B}$ to denote that $\mathcal{B}$ refines $\mathcal{A}$.

Our goal in this section is to prove that any two subnormal series have *equivalent* refinements. To define "equivalence", consider two equally long subnormal series for a group G:

$$G = A_0 \trianglerighteq \cdots \trianglerighteq A_m = 1 \quad \text{and} \quad G = B_0 \trianglerighteq \cdots \trianglerighteq B_m = 1.$$

These series are considered **equivalent** if they have the same factors up to isomorphism; that is, there is a permutation σ of $\{1, \ldots, m\}$ so that

$$\frac{A_i}{A_{i+1}} \simeq \frac{B_{\sigma(i)}}{B_{\sigma(i)+1}} \quad \text{for all } i.$$

We write $\mathcal{A} \simeq \mathcal{B}$ to denote equivalent series.

Now we state the Schreier Refinement Theorem.

Theorem 2.2.1 (Schreier Refinement)**.** *Let G be a group. Then any two subnormal series for G have equivalent refinements.*

To prove this: given two series $\mathcal{A}$ and $\mathcal{B}$ we will insert $\mathcal{A}$ into $\mathcal{B}$ in a systematic manner; to calculate the factors of this newly constructed series, we will require the following consequence of the Second Isomorphism Theorem. This is commonly known as the Butterfly Lemma or the Zassenhaus Isomorphism Theorem.

Lemma 2.2.2 (Zassenhaus Isomorphism)**.** *Let A, B be two subgroups of a group G, and let $N_A \trianglelefteq A$, $N_B \trianglelefteq B$ be normal subgroups of A, B respectively. Then there is an isomorphism*

$$\frac{N_A(A \cap B)}{N_A(A \cap N_B)} \simeq \frac{N_B(A \cap B)}{N_B(N_A \cap B)}.$$

Proof. In fact, we show the isomorphism

$$\frac{N_A(A \cap B)}{N_A(A \cap N_B)} \simeq \frac{A \cap B}{(A \cap N_B)(B \cap N_A)} \tag{2.1}$$

and notice that group on the right-hand side of 2.1 is symmetric in A and B. To establish this isomorphism, set $H := A \cap B$ and $N := N_A(A \cap N_B)$, noting that N is a normal subgroup of H. Then we express the left-side numerator and right-side denominator of isomorphism 2.1 cleverly:

$$N_A(A \cap B) = \Big(N_A(A \cap N_B)\Big) \cdot \Big(A \cap B\Big) = NH \tag{2.2}$$

$$(A \cap N_B)(B \cap N_A) = \Big(N_A(A \cap N_B)\Big) \cap \Big(A \cap B\Big) = N \cap H \tag{2.3}$$

Now we calculate starting on the left-hand side of 2.1:

$$\begin{aligned} \frac{N_A(A \cap B)}{N_A(A \cap N_B)} &\simeq \frac{NH}{N} && \text{by 2.2} \\ &\simeq \frac{H}{N \cap H} && \text{by the Second Isomorphism Theorem} \\ &= \frac{A \cap B}{(A \cap N_B)(B \cap N_A)} && \text{by 2.3.} \end{aligned}$$

This proves 2.1. □

Now we can prove the Schreier Refinement Theorem.

Proof of Theorem 2.2.1. Let $\mathcal{A}$ and $\mathcal{B}$ be two subnormal series of a group G:

$$\mathcal{A} = \{G = A_0 \trianglerighteq \cdots \trianglerighteq A_m = 1\} \quad \text{and} \quad \mathcal{B} = \{G = B_0 \trianglerighteq \cdots \trianglerighteq B_n = 1\}.$$

First we refine $\mathcal{A}$. For $0 \leq i \leq m$ and $0 \leq j \leq n$, define a subgroup

$$A_i^j := A_{i+1}(A_i \cap B_j).$$

These subgroups refine the series $\mathcal{A}$, because all the A_i^j's fit between A_i and A_{i+1}:

$$A_i = A_i^0 \trianglerighteq A_i^1 \trianglerighteq \cdots \trianglerighteq A_i^{m-1} \trianglerighteq A_i^m = A_{i+1}.$$

These inclusions, and normality at each one, are routinely verified. Thus we have created a refinement $\widehat{\mathcal{A}}$ of $\mathcal{A}$. Now apply the same process with the roles of the A_i's and B_j's reversed: for $0 \leq i \leq m$ and $0 \leq j \leq n$, define

$$B_j^i := B_{j+1}(B_j \cap A_i).$$

So we have similarly constructed a refinement $\widehat{\mathcal{B}}$ of $\mathcal{B}$. Both new series $\widehat{\mathcal{A}}$ and $\widehat{\mathcal{B}}$ have length mn.

Finally, we will prove that $\widehat{\mathcal{A}}$ and $\widehat{\mathcal{B}}$ are equivalent by using the Zassenhaus Isomorphism Lemma 2.2.2. Indeed, for each $i \in \{0, \dots, m\}$ and $j \in \{0, \dots, n\}$, we calculate the factor A_i^j / A_i^{j+1}:

$$\begin{aligned} \frac{A_i^j}{A_i^{j+1}} &= \frac{A_{i+1}(A_i \cap B_j)}{A_{i+1}(A_i \cap B_{j+1})} \\ &\simeq \frac{B_{j+1}(A_i \cap B_j)}{B_{j+1}(A_{i+1} \cap B_j)} && \text{by Lemma 2.2.2} \\ &= \frac{B_i^j}{B_{i+1}^j}. \end{aligned}$$

Thus the (i, j) factor of $\mathcal{A}$ is isomorphic to the (j, i) factor of $\mathcal{B}$. We conclude that there is an equivalence of subnormal series $\mathcal{A} \simeq \mathcal{B}$, as required. □

2.2.2 Hirsch Length

Let G be a virtually polycyclic group. Then G is poly-{cyclic, finite} by Proposition 2.1.14, so G has a subnormal series

$$\mathcal{A} = \{G = A_0 \trianglerighteq A_1 \trianglerighteq \cdots \trianglerighteq A_m = 1\}$$

where, for each $0 \leq i < m$, the factor A_i / A_{i+1} is either finite or infinite cyclic. Let us call this a **cyclic-finite series**, and we define the **Hirsch length** of this series as the number of infinite cyclic factors.

We apply the Schreier Refinement Theorem to prove that any two cyclic-finite series have the same Hirsch length.

Theorem 2.2.3. *Let G be a virtually polycyclic group. Then any two cyclic-finite series for G have the same Hirsch length.*

Proof. The theorem follows by combining the Schreier Refinement Theorem 2.2.1 with the following observation.

Claim: When a cyclic-finite series is refined, its Hirsch length is unchanged.

To prove this, consider a cyclic-finite series

$$G = A_0 \trianglerighteq \cdots \trianglerighteq A_m = 1$$

and suppose that a subgroup B is inserted at the ith position: thus

$$A_i \trianglerighteq B \trianglerighteq A_{i+1}$$

and we assume these inclusions are proper. There are two cases: A_i / A_{i+1} is either finite or infinite cyclic. If A_i / A_{i+1} is finite, then A_i / B and B / A_{i+1} are both finite, and the refinement has not added an infinite cyclic factor. If $A_i / A_{i+1} \simeq \mathbb{Z}$ is infinite cyclic, then it contains B / A_{i+1} as a nontrivial subgroup, so $B / A_{i+1} \simeq k\mathbb{Z}$ must also be infinite cyclic. But then the factor A_i / B must be finite, because

$$\frac{A_i}{B} \simeq \frac{A_i / A_{i+1}}{B / A_{i+1}} \simeq \mathbb{Z} / k\mathbb{Z}$$

is finite. This proves that the insertion of a single subgroup B does not change the Hirsch length of the given series; inductively, the insertion of any number of terms will not change the Hirsch length. Thus we have shown the claim. □

Now we can define the **Hirsch length** of a virtually polycyclic group G as the number of infinite cyclic factors in any cyclic-finite series of G: *i.e.*

$$h(G) := |\{i \in \{0, \ldots, m-1\} : [G_i : G_{i+1}] = \infty\}$$

where $G = G_0 \trianglerighteq \cdots \trianglerighteq G_m = 1$ is any cyclic-finite series for G. By Theorem 2.2.3, any two such series have the same number of infinite cyclic factors, so $h(G)$ is well-defined.

Example 2.2.4. The Hirsch length of a finitely generated abelian group G is just its rank. To see this, write G as a direct sum:

$$G \simeq \mathbb{Z}^r \oplus T$$

where $r \geq 0$ is the rank of G and T is the torsion subgroup of G. Then it not hard to see that

$$h(G) = r = \text{rank}(G).$$

For example, the polycyclic group $\mathbb{Z}^3 \oplus \mathbb{Z}_4$ has Hirsch length 3, because it has a cyclic series obtained by removing factors from the direct sum one-by-one:

$$\mathbb{Z}^3 \oplus \mathbb{Z}_4 \geq \mathbb{Z}^3 \oplus 0 \geq \mathbb{Z}^2 \oplus 0^2 \geq \mathbb{Z} \oplus 0^3 \geq 0$$

The first factor is finite while the rest are infinite cyclic, so $h(\mathbb{Z}^3 \oplus \mathbb{Z}_4) = 3$.

Example 2.2.5. A virtually polycyclic group G is finite if and only if its Hirsch length is zero. Indeed, if G is finite then $G \trianglerighteq \{1\}$ is already a cyclic-finite series with no infinite cyclic factors, so $h(G) = 0$. Conversely, suppose G is virtually polycyclic of Hirsch length zero, so that G has a subnormal series $G = G_0 \trianglerighteq \cdots \trianglerighteq G_m = 1$ with all factors G_i/G_{i+1} finite. Since index is multiplicative along chains, we get

$$|G| = |G/\{1\}| = [G : G_m] = [G_0 : G_1] \cdots [G_{m-1} : G_m] < \infty.$$

Thus G is finite.

Example 2.2.6. Recall the Heisenberg group H from Example 2.1.7:

$$H = \langle x, y : [x, [x, y]] = [y, [x, y]] = 1 \rangle.$$

Then H has a cyclic series

$$H \trianglerighteq \langle x, [x, y] \rangle \trianglerighteq \langle x \rangle \trianglerighteq 1,$$

so H has Hirsch length 3.

Example 2.2.7. Recall the infinite dihedral group $D_\infty = \mathbb{Z} \rtimes \mathbb{Z}_2$ from Example 2.1.4, which fits in an extension

$$1 \to \mathbb{Z} \to D_\infty \to \mathbb{Z}_2 \to 1.$$

Since Hirsch length is additive along extensions (this is Proposition 2.2.8(a) below), we calculate

$$h(D_\infty) = h(\mathbb{Z}) + h(\mathbb{Z}_2) = 1.$$

We close this section with several useful properties of Hirsch length.

Proposition 2.2.8. *Let G be a virtually polycyclic group.*

(a) *Let $N \trianglelefteq G$ be a normal subgroup of G. Then $h(G) = h(G/N) + h(N)$.*

(b) *Let $A \leq G$ and $B \trianglelefteq G$. Then $h(AB) = h(A) + h(B) - h(A \cap B)$.*

(c) *Let $H \leq G$. Then $h(H) \leq h(G)$, with equality if $[G : H] < \infty$.*

Proof. (a) We use the same argument as Proposition 2.1.11(b): simply append the cyclic-finite series of N and G/N. Note that G/N is virtually polycyclic, being a quotient of such. Thus we can find a cyclic-finite series for N, which, via the quotient map, is equivalent to a series for G:

$$G = G_0 \trianglerighteq \cdots \trianglerighteq G_m = N$$

each of whose factors is either cyclic or finite. Similarly, N is also virtually polycyclic, so it has its own cyclic-finite series, say

$$N = N_0 \trianglerighteq \cdots \trianglerighteq N_n = 1.$$

Now append these two series together: the result is a cyclic-finite series for G of length $m + n$.

$$G = G_0 \trianglerighteq \cdots \trianglerighteq G_m = N = N_0 \trianglerighteq \cdots \trianglerighteq N_n = 1.$$

The Hirsch length of this series is simply the sum of Hirsch lengths of the two from which it was constructed. Therefore,

$$h(G) = h(G/N) + h(N).$$

(b) Since $A/(A \cap B) \simeq AB/B$ by the Second Isomorphism Theorem, part (a) we get

$$h(A) - h(A \cap B) = h(AB) - h(B)$$

from which the desired equation follows.

(c) Let $H \leq G$; we must show $h(H) \leq h(G)$. As in the proof of Proposition 2.1.11(a): we start with a cyclic-finite series for G, say

$$G = G_0 \trianglerighteq \cdots \trianglerighteq G_m = 1$$

and intersect with H to get a cyclic-finite series with $H_i = H \cap G_i$:

$$H = H_0 \trianglerighteq \cdots \trianglerighteq H_m = 1.$$

Since G_i/G_{i+1} contains H_i/H_{i+1} as a subgroup, the latter is infinite cyclic no more often than the former is. We conclude the inequality

$$h(H) \leq h(G).$$

Now suppose $[G : H] < \infty$. By Proposition 2.1.13(a), H has a finite index subgroup N which is normal in G. But then G/N is a finite group, so its Hirsch length is zero; using the formula from part (a) thus yields the sequence of inequalities

$$h(H) \leq h(G) = h(G/N) + h(N) = h(N) \leq h(H)$$

from which we conclude $h(H) = h(G)$. ∎

Example 2.2.9. Here is an example showing that the formula

$$h(AB) = h(A) + h(B) - h(A \cap B)$$

does not hold if neither A, B are normal in G; note that we define the product of subgroups here as $AB := \langle A \cup B \rangle$.

Take $G = D_\infty = \langle x, y : x^2 = 1, xy = y^{-1}x \rangle$ to be the infinite dihedral group, and let $A := \langle x \rangle$, $B := \langle xy \rangle$. Then A, B are each cyclic groups of order 2, and $G = \langle A \cup B \rangle$. On the other hand, $h(A) = h(B) = h(A \cap B) = 0$, so it is clear that the formula does not hold.

2.3 Automorphisms of Polycyclic Groups

2.3.1 Statement of the Main Theorem

In this section we return to dynamical systems; specifically, the dynamics of an automorphism $\varphi : G \to G$ of a polycyclic-by-finite group G. We examine the return set of the φ-orbit of a point $x \in G$ to a *normal* subgroup $N \trianglelefteq G$:

$$\mathrm{Ret}_\varphi(x, N) := \{n \geq 0 : \varphi^n(x) \in N\}.$$

Within this setting, we obtain a conclusion analogous to the "weak" Dynamical Mordell–Lang result of Bell–Ghioca–Tucker (Corollary 1.3.9).

Theorem 2.3.1. *Let G be a polycyclic-by-finite group, let $\varphi : G \to G$ be an automorphism, let $N \trianglelefteq G$ be a normal subgroup, and let $x \in G$. Define the return set*

$$E := \{n \geq 0 : \varphi^n(x) \in N\}.$$

Then E is a finite union of infinite arithmetic progressions along with a set of zero Banach density.

In the next three examples, we present some easily verified cases of this theorem. In fact, in the below three cases we only use the weaker hypothesis that φ is an *endo*morphism, and note that we get the stronger conclusion that E_N is a finite union of arithmetic progressions (no need for a set of zero density).

Example 2.3.2. Suppose that N is finite. Then the return set E is a finite union of sets of the form

$$D_g := \{n \geq 0 : \varphi^n(x) = g\} \quad \text{for } g \in G,$$

so it is enough to prove that each D_g is a finite union of arithmetic progressions. But it is easy to prove that if D_g has at least two elements then the φ-orbit of x must be preperiodic. Indeed, if $a, a+b$ are the two smallest elements of D_g, then $\varphi^a(x) = \varphi^{a+b}(x) = g$ and the φ-orbit of x is the finite set

$$\{x, \varphi(x), \ldots, \varphi^{a-1}(x)\} \cup \{g, \varphi(g), \ldots, \varphi^{b-1}(g)\}.$$

Thus D_g is equal to the infinite arithmetic progression

$$D_g = \{a, a+b, a+2b, \ldots\}.$$

Theorem 2.3.1 follows.

Example 2.3.3. If $[G : N] < \infty$, then by Lemma 2.1.13(b), N has a subgroup N' of finite index such that N' is invariant for every endomorphism of G. In particular, N' is normal in G and φ restricts to an endomorphism of N', so φ induces a well-defined endomorphism of G/N':

$$\overline{\varphi} : G/N' \to G/N', \quad \overline{\varphi}(\overline{g}) := \overline{\varphi(g)}$$

where $g \mapsto \overline{g}$ denotes the quotient map $G \to G/N'$. We thus consider the return set of $\overline{x}$ to $\overline{N} = N/N'$ under the orbit of $\overline{\varphi}$:

$$\overline{E} := \{n \geq 1 : \overline{\varphi}^n(\overline{x}) \in \overline{N}\}.$$

But it is trivial to verify that $\overline{\varphi}^n(\overline{x}) \in \overline{N}$ if and only if $\varphi^n(x) \in N$ — so in fact $\overline{E} = E$. Therefore we are in the case of an endomorphism of a finite group, so we are done by Example 2.3.2.

Example 2.3.4. If $G = \mathbb{Z}$, the only endomorphisms are $x \mapsto mx$ for some $m \in \mathbb{Z}$. So every subgroup of $\mathbb{Z}$ is invariant for every endomorphism. Thus if $\varphi^a(x) \in N$ for even a single $a \in \mathbb{N}$, then $\varphi^{a+n}(x) \in N$ for all $n \geq a$, so that E is equal to the arithmetic progression $a + \mathbb{N}$ up to a finite set.

Here is a big picture outline of the proof of Theorem 2.3.1. We show the result in two steps: (I) if $\delta^*(E) > 0$, then E contains an infinite arithmetic progression, and (II) now show that E is a finite union of arithmetic progressions up to a set of zero density. For step (I), the argument is structurally identical to that of our Theorem 1.3.11 for amenable semigroups acting on noetherian spaces: by the Poincaré Recurrence Theorem, we select $b \geq 1$ such that $E' = E \cap (E - b)$ has positive density, noting that $E' = \mathrm{Ret}_\varphi(x, N')$ is the return set of x to the smaller subgroup $N' := N \cap \varphi^{-b}(N)$. At this point it would be nice to use a minimality argument, but since there is no descending chain condition for subgroups, we must instead argue using Hirsch length: if $h(N') < h(N)$, we are done by induction; if $h(N') = h(N)$, all we can conclude is that $[N : N'] < \infty$. So most of the argument is structured around using the assumption that $[N : N'] < \infty$ to reduce to the case of Example 2.3.3, and this reduction uses a combination of Hirsch length arguments with the ascending chain condition on subgroups. Step (II) will follow from Step (I) using another straightforward induction on the Hirsch length.

2.3.2 Proof of the Theorem 2.3.1

This subsection is dedicated solely to the proof of Theorem 2.3.1; thus we maintain the following notation throughout:

- G is a polycyclic-by-finite group.
- $\varphi : G \to G$ is a group automorphism.
- $N \trianglelefteq G$ is a normal subgroup of G.
- $x \in G$.

Then we let E be the associated return set for this data:

$$E := \mathrm{Ret}_\varphi(x, N) = \{n \geq 0 : \varphi^n(x) \in N\}.$$

Our first goal is to obtain a single arithmetic progression in the case that E has positive density.

Proposition 2.3.5. *If $\delta^*(E) > 0$ then E contains an arithmetic progression.*

Let us show how Theorem 2.3.1 follows from this proposition.

Proof of Theorem 2.3.1. We proceed by induction on the Hirsch length of N. If $h(N) = 0$ then N is finite and we are done by Example 2.3.2, so we assume $h(N) \geq 1$. Also note that we are done if E already has zero density. If E has positive density, then by Proposition 2.3.5, E contains an infinite arithmetic progression $\{a + nb : n \geq 0\}$ where $0 \leq a < b$. Without loss of generality, we may assume $a = 0$ by making the replacement $x \mapsto \varphi^a(x)$, noting that this only shifts E to the set $E - a = \{n \geq 0 : n + a \in E\}$, and such a shift does not affect our desired conclusion.

Now for each $i \geq 0$, set

$$E_i := \{n \in E : n \equiv i \pmod{b}\}$$

so that E decomposes as a finite union

$$E = E_0 \sqcup \cdots \sqcup E_{b-1}.$$

Thus it is enough to prove that each E_i has the desired form. But now $E_i = i + F_i b$, where F_i is the set

$$F_i := \{m \geq 0 : i + mb \in E\}.$$

So it is enough to prove that F_i is a finite union of arithmetic progressions along with a set of zero Banach density. We fix such $i \in \{0, \dots, b-1\}$ for the remainder of the argument.

Let H be the subgroup generated by the φ^b-orbit of x:

$$H := \langle \varphi^{nb}(x) : n \geq 0 \rangle.$$

It is clear that H is a φ^b-invariant subgroup of N. If K is the normal closure of H, *i.e.* the smallest normal subgroup of G containing H, then:

Claim A: We are done if K is finite.

Indeed, if K is finite then $\{\varphi^{i+nb}(x) : n \geq 0\}$ is completely contained in the finite set $\varphi^i(K)$. Thus the sequence $\{\varphi^{i+nb}(x) : n \geq 0\}$ is preperiodic and we easily conclude that F_i has the desired form.

Thus assume $h(K) > 0$. We use the fact that $H \subseteq \varphi^{-b}(H)$ to prove:

Claim B: K is φ^b-invariant.

Indeed, $\varphi^{-b}(K)$ is a normal subgroup of G (being a preimage of one), and it contains H because $H \subseteq \varphi^{-b}(H) \subseteq \varphi^{-b}(K)$. By definition of normal closure, we must have $K \subseteq \varphi^{-b}(K)$, which is exactly what it means for K to be φ^b-invariant.

Therefore φ^b descends to a well-defined endomorphism ψ of G/K by

$$\psi : G/K \to G/K, \qquad \overline{g} \mapsto \overline{\varphi^b(g)},$$

where $g \mapsto \overline{g}$ denotes the quotient map $G \to G/K$. But now since $N \geq K$, notice that for $g \in G$ we have $g \in N$ if and only if $\overline{g} \in \overline{N}$ where $\overline{N} = N/K$. Thus, setting $y_i := \overline{\varphi^i(x)}$, our set F_i is exactly the return set of y_i to $\overline{N}$ under the orbit of ψ:

$$\begin{aligned} F_i &= \{m \geq 0 : i + mb \in E\} \\ &= \{m \geq 0 : (\varphi^b)^m(\varphi^i(x)) \in N\} \\ &= \{m \geq 0 : \psi^m(y_i) \in \overline{N}\} \\ &= \mathrm{Ret}_\psi(y_i, \overline{N}). \end{aligned}$$

So now we are in the setting of an endomorphism of G/K. Note that since φ is an automorphism, it is clear that ψ is surjective — since G/K is noetherian, Proposition 2.1.22 implies that ψ is actually an automorphism of G/K. Thus the inductive hypothesis applies to the data $(G/K, \psi, y_i, \overline{N})$. The Hirsch length of G/K is strictly smaller than that of G (because $h(K) \geq 1$) — so by induction, F_i is a finite union of arithmetic progressions along with a set of zero Banach density, as required. ☐

Now we proceed to the proof of Proposition 2.3.5. First we show that we may replace φ with some iterate φ^b without losing generality.

Lemma 2.3.6. *Let $b \geq 1$ and $a \in E$. It is enough to prove Proposition 2.3.5 with φ replaced by some iterate φ^b and x replaced by some iterate $\varphi^a(x)$ with $a \in E$.*

Proof. Clearly replacing a with $\varphi^a(x)$ does not change the conclusion of Proposition 2.3.5, because it only translates the return set E to the set $E - a$. Thus we proceed with $a = 0$.

To prove that we can make the replacement $\varphi \mapsto \varphi^b$, define a sequence of sets E_i for $i \geq 0$:

$$E_i := \{n \in E : n \equiv i \pmod{b}\}.$$

Then we can express the return set E as a union

$$E = E_0 \sqcup \cdots \sqcup E_{b-1}.$$

Since E has positive density, the same must be true for one of the sets $E_0, \ldots, E_{b-1}$; fix E_i of positive density, and fix any $c \in E_i$. It follows that the set

$$F := \{m \geq 0 : c + bm \in E\}$$

has positive density, because $E_i = c + bF$.

Now let $y := \varphi^a(x) \in N$ and $\psi := \varphi^b$. Then the corresponding return set for the data (ψ, N, y) is exactly the set F we defined above:

$$\mathrm{Ret}_\psi(y, N) = \{n \geq 0 : \psi^n(y) \in N\} = \{n \geq 0 : c + bn \in E\} = F$$

and we have already shown that F has positive density. Assuming we have proven Proposition 2.3.5 for $\psi = \varphi^b$, we conclude that F contains an infinite arithmetic progression, say $p+q\mathbb{N}$ for some $p, q \geq 1$, and it follows that E contains the arithmetic progression

$$c + b(p + q\mathbb{N}) = (c + bp) + (bq)\mathbb{N}.$$ ☐

The goal now is to reduce to the case of $[G : N] < \infty$, where we are done by Example 2.3.3. So we must find a subgroup $K \leq G$ with the following two properties:

(i) φ^b restricts to an endomorphism of K, for some $b \geq 1$; and

(ii) K contains N as a finite index subgroup.

Once we construct such K, we can complete the proof by replacing φ with φ^b (Lemma 2.3.6) so that we have an endomorphism $\varphi : K \to K$, and then applying the finite index case (Example 2.3.3).

To accomplish this, we proceed by induction on the Hirsch length of N. If $h(N) = 0$, then N is finite and we are done by Example 2.3.2. Thus assume $h(N) \geq 1$. Since $\delta^*(E) > 0$, by Lemma 1.2.31, there exists $b \geq 1$ such that

$$E \cap (E - b) = \{n \in E : n + b \in E\}$$

also has positive density. By applying Lemma 2.3.6 we assume $b = 1$ without loss of generality (this is not essential, but it simplifies the notation). But notice that $E \cap (E - 1)$ is simply the return set of x to the subgroup $N \cap \varphi^{-1}(N)$:

$$\begin{aligned} E \cap (E - 1) &= \{n \in E : n + 1 \in E\} \\ &= \{n \geq 1 : \varphi^n(x) \in N \cap \varphi^{-1}(N)\} \\ &= \operatorname{Ret}_\varphi(x, N \cap \varphi^{-1}(N)). \end{aligned}$$

If $N \cap \varphi^{-1}(N)$ has smaller Hirsch length than N, then E' must contain an infinite arithmetic progression by induction, and E contains the same progression because $E' \subseteq E$. Thus we assume $h(N) = h(N')$. But then

$$\begin{aligned} h(N) &= h(N') \\ &= h(\varphi(N')) && \text{because } N' \simeq \varphi(N') \\ &= h(N \cap \varphi(N)) && \text{because } \varphi(N \cap \varphi^{-1}(N)) = N \cap \varphi(N), \end{aligned}$$

and by the product formula for Hirsch length Proposition 2.2.8(b), we see that $N\varphi(N)/N$ has Hirsch length zero:

$$\begin{aligned} h(N\varphi(N)/N) &= h(N\varphi(N)) - h(N) \\ &= h(N) + h(\varphi(N)) - h(N \cap \varphi(N)) - h(N) \\ &= 0. \end{aligned}$$

Thus $N\varphi(N)/N$ is finite. This is the base step in the following iterative construction. Define a sequence of subgroups K_n of G:

$$K_n := N\varphi(N) \cdots \varphi^n(N), \quad \text{for } n \geq 0.$$

Then K_n is a product of normal subgroups of G, so $K_n \leq G$. We will prove that every K_n is a finite extension of N.

Lemma 2.3.7. *$[K_n : N] < \infty$ for all $n \geq 0$.*

Proof. First we prove the following Hirsch length formula:

$$h(K_n \cap \varphi^{n+1}(N)) = h(N) \quad \text{for all } n \geq 0. \tag{$\diamondsuit$}$$

We prove this by induction on n. If $n = 0$ the equation becomes $h(N \cap \varphi(N)) = h(N)$, which we have already established in the paragraphs preceding this lemma.

Assuming $n \geq 1$, we calculate

$$\begin{aligned}
h(N) &= h(\varphi^{n+1}(N)) \\
&\geq h(K_n \cap \varphi^{n+1}(N)) \\
&\geq h\Big(\varphi(K_{n-1}) \cap \varphi^{n+1}(N)\Big) && \text{because } \varphi(K_{n-1}) \subseteq K_n \\
&= h\Big(\varphi\big(K_{n-1} \cap \varphi^n(N)\big)\Big) \\
&= h(K_{n-1} \cap \varphi^n(N)) && \text{because } \varphi \text{ is an isomorphism} \\
&= h(N) && \text{by induction.}
\end{aligned}$$

This shows $h(N) \geq h(K_n \cap \varphi^{n+1}(N)) \geq h(N)$, which establishes $(\diamondsuit)$.

Now we prove the lemma, once again by induction on n, with the base case $n = 0$ following trivially since $K_0 = N$. If $n \geq 1$, then by induction we have $h(K_{n-1}) = h(N)$, and $h(K_{n-1} \cap \varphi^n(N)) = h(N)$ by $(\diamondsuit)$. So we calculate

$$\begin{aligned}
h(K_n) &= h(K_{n-1}\varphi^n(N)) \\
&= h(K_{n-1}) + h(\varphi^n(N)) - h(K_{n-1} \cap \varphi^n(N)) && \text{since } \varphi^n(N) \trianglelefteq G \\
&= h(N) + h(N) - h(N) \\
&= h(N).
\end{aligned}$$

So K_n and N have the same Hirsch length, so it follows that $[K_n : N] < \infty$ because $h(K_n/N) = h(K_n) - h(N) = 0$. □

Observe that $K_{n+1} = K_n\varphi^n(N)$, in particular $K_{n+1} \supseteq K_n$. We thus have an infinite ascending chain

$$N = K_0 \leq K_1 \leq K_2 \leq \cdots$$

Since polycyclic-by-finite groups are noetherian (Proposition 2.1.20), this chain must terminate: thus there exists $n \geq 0$ so that

$$K_n = K_{n+1} = K_{n+2} = \cdots .$$

Let $K := K_n$. Then K is φ-invariant because

$$\varphi(K) = \varphi(K_n) \subseteq K_{n+1} = K,$$

and we know that $[K : N] < \infty$ by Lemma 2.3.7.

Thus we can restrict φ to an endomorphism of K. Now apply Example 2.3.3 with the data (G, φ, x, N) replaced with $(K, \varphi|_K, \varphi^a(x), N)$, where $a \in E$ is chosen so that $\varphi^a(x) \in N$ (due to Lemma 2.3.6, this replacement does not hurt our conclusion). This completes the proof of 2.3.5.

2.3.3 Simplifications of Theorem 2.3.1 for Abelian Groups

In the case of a finitely generated abelian group, we can apply the Skolem–Mahler–Lech Theorem to obtain a cleaner result for any *endo*morphism: the return set is a finite union of arithmetic progressions. To state it, we make a general definition of linear recurrences. Let M be an R-module where R is a commutative ring. A **linear recurrence** over R is a sequence $(a_n)_{n\geq 0}$ of elements of M satisfying a recurrence relation

$$a_n = c_1 a_{n-1} + \cdots + c_d a_{n-d} \quad \text{for all } n \geq d,$$

where $c_1, \ldots, c_d \in R$ are constants. Given a submodule N of M, define the **return set** of (a_n) to M by

$$\mathrm{Ret}(a_n, N) := \{n \geq 0 : a_n \in N\}.$$

In the case $N = 0$ we obtain the **zero set**

$$Z(a_n) := \mathrm{Ret}(a_n, 0) = \{n \geq 0 : a_n = 0\}.$$

Then the Skolem–Mahler–Lech Theorem is the following statement about zeros of linear recurrences in the case $R = M = \mathbb{C}$.

Theorem 2.3.8 (Skolem–Mahler–Lech [Lec53])**.** *Let $(a_n)_{n\geq 0}$ be a linear recurrence over $\mathbb{C}$. Then $Z(a_n)$ is a finite union of arithmetic progressions.*

We can use this theorem to give an analogous conclusion for linear recurrences in abelian groups (*i.e.* $\mathbb{Z}$-modules).

Theorem 2.3.9. *Let A be an abelian group, let $B \leq A$, and let (a_n) be a sequence of elements of A satisfying a linear recurrence over $\mathbb{Z}$. Then $\mathrm{Ret}(a_n, B)$ is a finite union of arithmetic progressions.*

Proof. First we make several reductions. Noting that the image of (a_n) in A/B still satisfies a linear recurrence, we may work in A/B to assume $B = \{0\}$, so that $\mathrm{Ret}(a_n, 0) = Z(a_n)$ is the zero set. Next, if (a_n) satisfies a linear recurrence of order d, then all a_n's lie in the subgroup generated by the initial terms $a_0, \ldots, a_d$; thus we may replace A with this subgroup to assume that A is a finitely generated abelian group.

Now $A \simeq C_1 \oplus \cdots \oplus C_s$ is a direct sum of cyclic groups, and we let $\pi_i : A \twoheadrightarrow C_i$ denote the ith projection. Then $a_n = 0$ if and only if $\pi_i(a_n) = 0$ for all i, so that the zero set of a_n is obtained as the intersection

$$Z(a_n) = Z(\pi_1(a_n)) \cap \cdots \cap Z(\pi_s(a_n)).$$

Since a finite intersection of arithmetic progressions is again an arithmetic progression, we can replace A with C_i and (a_n) with its image in C_i and work in a cyclic group. This reduces to the case where A is cyclic.

If A is a finite cyclic group, then (a_n) is easily seen to be preperiodic, and the result is clear. If $A \simeq \mathbb{Z}$ is an infinite cyclic group, $Z(a_n)$ is a finite union of arithmetic progressions by the Skolem–Mahler–Lech Theorem. Either way, we are done. $\square$

Finally we obtain a simplification of Theorem 2.3.1 when $\varphi : A \to A$ is an endomorphism of a finitely generated abelian group A, by noting that the orbit $a_n := \varphi^n(x)$ is a linear recurrence for any $x \in A$.

Theorem 2.3.10. *Let $\varphi : A \to A$ be an endomorphism of a finitely generated abelian group A, and let $x \in A$. Then $a_n := \varphi^n(x)$ satisfies a linear recurrence over $\mathbb{Z}$. In particular, for any subgroup $B \leq A$, the return set $\mathrm{Ret}_\varphi(x, B)$ is a finite union of arithmetic progressions.*

Proof. Let $B_n := \langle a_0, \ldots, a_n \rangle$ be the subgroup generated by the first n terms of the sequence $(a_n)_{n \geq 0}$. These form an ascending chain of subgroups of A:

$$B_0 \leq B_1 \leq B_2 \leq \cdots$$

By the noetherian property (which holds because A is a finitely generated $\mathbb{Z}$-module), there is some $d \geq 1$ so that $B_d = B_{d-1}$, which implies that a_d is a linear combination of the previous terms $a_0, \ldots, a_{d-1}$: say

$$a_d = c_1 a_{d-1} + \cdots + c_d a_0$$

where $c_1, \ldots, c_d \in \mathbb{Z}$. But now using the fact that $\varphi(a_n) = a_{n+1}$, we can apply φ^{n-d} (for $n \geq d$) to the above relation to obtain a recurrence

$$a_n = c_1 a_{n-1} + \cdots + c_d a_{n-d} \quad \text{for all } n \geq d.$$

This proves that (a_n) is a linear recurrence over $\mathbb{Z}$.

Now it follows from Theorem 2.3.9 that $\mathrm{Ret}_\varphi(x, B) = \mathrm{Ret}(a_n, B)$ is a finite union of arithmetic progressions. $\square$

Chapter 3

Rational Orbits, S-Units, and D-Finite Power Series

Let K be a field. Given a polynomial $p(x) \in K[x]$ and a multiplicative group $G \le K^\times$, we can ask how often the orbit $p^n(a)$ of a number $a \in K$ lies in G. Thus we are interested in the return set

$$\mathrm{Ret}_{p(x)}(a, G) = \{n \ge 0 : p^n(a) \in G\}.$$

If G is finitely generated and the return set is infinite, then the orbit $(p^n(a))_{n\ge 0}$ must have some multiplicatively dependent points, so this is ultimately related to the problem of multiplicative dependence among points in polynomial orbits. Number-theoretic problems of this type have been studied previously in [BOSS, OSSZ19, BNZ99, BNZ06, BNZ08].

In this chapter, we expand this setting to higher dimensions as follows. Let $\varphi : X \dashrightarrow X$ be a rational mapping of an algebraic variety X defined over an algebraically closed field K of characteristic zero, and let $x_0 \in X$ be a point whose forward φ-orbit is well-defined, so that we have an orbit $x_0, \varphi(x_0), \varphi^2(x_0), \ldots$. Evaluating a rational function $f : X \dashrightarrow K$ along this orbit (so long as the orbit avoids the indeterminacy locus of f), we ask how often the resulting number $u_n := f(\varphi^n(x_0))$ can lay in a finitely generated multiplicative group $G \le K^\times$; thus we are interested in the return set

$$\mathrm{Ret}(u_n, G) = \{n \ge 0 : u_n \in G\}.$$

This is remarkably similar to the setup of the Skolem–Mahler–Lech Theorem, except the sequence (u_n) may not satisfy a linear recurrence. Nonetheless, we prove that the following Skolem–Mahler–Lech type result in joint work with Jason Bell and Shaoshi Chen.

Theorem 3.0.1. *Let X be an algebraic variety defined over an algebraically closed field K of charcteristic zero, let $\varphi : X \dashrightarrow X$ be a rational map, then $x_0 \in X$ be a point whose forward φ-orbit is well-defined, let $f : X \dashrightarrow K$ be a rational function defined on the forward φ-orbit of x. Let*

$$u_n := f(\varphi^n(x_0)),$$

and let $G \le K^\times$ be a finitely generated group of units. Then the return set

$$\mathrm{Ret}(u_n, G) = \{n \ge 0 : f(\varphi^n(x)) \in G\}$$

is a finite union of arithmetic progressions with a set of zero Banach density.

We note that the set of zero Banach density cannot be removed, even in a simple example: if $X = \mathbb{A}^1$, $\varphi(t) := t + 1$, $x_0 = 0$, $f(t) = t$, and $G = \langle 2 \rangle = \{2^n : n \in \mathbb{Z}\}$, then the sequence obtained is $u_n = n$, and $u_n \in G$ if and only if n is a power of 2. Thus the return set is a zero density set and contains no arithmetic progression.

If (u_n) happens to satisfy some *multiplicative* linear recurrence relation, *i.e.* a recurrence of the form $u_{n+1} = u_n^{i_0} \cdots u_{n-d}^{i_d}$ for some integers $i_0, \ldots, i_d \in \mathbb{Z}$, then this result would indeed follow directly from the Skolem–Mahler–Lech Theorem. We show that if $u_n \in G$ for all $n \geq 0$, then in fact (u_n) *must* be a multiplicative linear recurrence.

Even more strongly, we prove that if the heights of (u_n) grow slowly enough, then (u_n) actually satisfies a *bona fide* linear recurrence:

$$u_{n+1} = c_0 u_n + \cdots + c_e u_{n-e} \quad \text{for all } n \geq e$$

where $c_0, \ldots, c_e \in K$. We apply this to recover a rationality test of Bézivin [Béz86] on D-finite power series: if a formal power series $F(t) \in K[[t]]$ satisfies a homogeneous differential equation with rational function coefficients, and the coefficients of $F(t)$ all lay in $G \cup \{0\}$, then in fact $F(t)$ must be already a rational function.

3.1 Combinatorial Preliminaries

3.1.1 Rational and D-Finite Power Series

In this subsection we define two types of power series: rational functions, which are generated by linear recurrences; and D-finite power series, which are generated by polynomial recurrences. Our main dynamical result in this chapter, Theorem 3.0.1, can be applied to obtain a recurrence property for the coefficients of a D-finite power series.

Let $K[[x]]$ be the **ring of formal power series** in an indeterminate x with coefficients in a field K: the elements of $K[[x]]$ are infinite series of the form

$$F(x) := \sum_{n \geq 0} a_n x^n, \quad \text{where } a_n \in K.$$

When equipped with the expected addition and multiplication for series, it is routine to verify that $K[[x]]$ is an integral domain. In fact it is a discrete valuation ring with maximal ideal

$$(x) := \{F(x) \in K[[x]] : F(0) = 0\}.$$

Thus the units of $K[[x]]$ are precisely those power series with a nonzero constant term. One way to see this is through geometric series: the polynomial $1 - x$ is invertible in $K[[x]]$, with inverse given by

$$(1 - x)^{-1} = \sum_{n \geq 0} x^n.$$

More generally, if $q(x)$ is a polynomial with nonzero constant term, then $1/q(x)$ can be expanded as a formal power series. This shows that $K[[x]]$ contains every rational function of the form

$$\frac{p(x)}{q(x)} \quad \text{where } p(x), q(x) \in K[x] \text{ are polynomials with } q(0) \neq 0.$$

It is a routine fact that these rational functions are precisely those power series whose coefficient sequence $(a_n)_{n\geq 0}$ satisfies a linear recurrence. Recall that a sequence (a_n) of elements of K satisfies a **linear recurrence** over K if there exist $d \in \mathbb{N}$ and constants $c_0, \ldots, c_d \in K$ defining a recursive relation

$$a_{n+1} = c_0 a_n + \cdots + c_d a_{n-d}, \quad \text{for all } n \geq d.$$

Proposition 3.1.1. *Let $(a_n)_{n\geq 0}$ be a sequence of elements of a field K, and let $F(x) := \sum_{n\geq 0} a_n x^n$ denote the corresponding generating function. Then the following are equivalent:*

(a) *(a_n) satisfies a linear recurrence over K.*

(b) *$F(x)$ is a rational function of the form $p(x)/q(x)$ with $q(0) \neq 0$.*

Proof. "(a) $\Longrightarrow$ (b)": Suppose that (a_n) satisfies the recurrence

$$a_n = c_1 a_{n-1} + \cdots + c_d a_{n-d}, \quad \text{for all } n \geq d,$$

where $c_1, \ldots, c_d \in K$. Letting $q(x) := 1 - c_1 x - \cdots - c_d x^d$ be the characteristic polynomial of the recurrence, we can write $q(x)F(x)$ as

$$\begin{aligned} q(x)F(x) &= F(x) - c_1 x F(x) - \cdots - c_d x^d F(x) \\ &= \sum_{n\geq 0} a_n x^n - \sum_{n\geq 1} c_1 a_{n-1} x^n - \cdots - \sum_{n\geq d} c_d a_{n-d} x^n \\ &= a_0 + \cdots + a_{d-1} x^{d-1} + \sum_{n\geq d} (a_n - c_1 a_{n-1} - \cdots - c_d a_{n-d}) x^n \\ &= a_0 + \cdots + a_{d-1} x^{d-1}. \end{aligned}$$

Thus $F(x)$ has the form

$$F(x) = \frac{a_0 + \cdots + a_{d-1} x^{d-1}}{q(x)}.$$

"(b) $\Longrightarrow$ (a)": Suppose that $F(x)$ is a rational function; then after scalar multiplication, we may assume that $F(x)$ has the form

$$F(x) = \frac{p(x)}{1 - c_1 x - \cdots - c_d x^d}$$

for some constant $c_1, \ldots, c_d \in K$ with $d \geq 1$. Now reversing the calculation done for "(a) $\Longrightarrow$ (b)" directly shows that (a_n) satisfies the recurrence

$$a_n = c_1 a_{n-1} + \cdots + c_d a_{n-d}, \quad \text{for all } n \geq d,$$

as required. $\square$

For later use, we prove two lemmas on linear recurrences. The first characterizes linear recurrences by their subsequences along arithmetic progressions.

Lemma 3.1.2. *Let $(a_n)_{n\geq 0}$ be a sequence of elements of a field K. Suppose that there exists $q \geq 1$ so that $(a_{p+nq})_{n\geq 0}$ satisfies a linear recurrence for all $p \in \{0, \ldots, q-1\}$. Then (a_n) satisfies a linear recurrence.*

Proof. For each $p \in \{0, \ldots, q-1\}$, let $G_p(x)$ be the generating function of (a_{p+nq}):

$$G_p(x) = \sum_{n \geq 0} a_{p+nq} x^n.$$

Then $G_p(x)$ is a rational function by hypothesis. But observe that the generating function $F(x) = \sum a_n x^n$ of (a_n) can be obtained from the $G_p(x)$'s via the formula

$$F(x) = \sum_{p=0}^{q-1} x^p G_p(x^q),$$

from which it follows that $F(x)$ is also rational. $\square$

Our second lemma on linear recurrences shows that if a sequence of *integers* satisfies a linear recurrence over $\mathbb{Q}$, then in fact it satisfies a linear recurrence over $\mathbb{Z}$. This will be useful when we generalize linear recurrences to arbitrary abelian groups, where we can only work with integer coefficients.

Lemma 3.1.3 (Fatou's Lemma). *Let $(a_n)_{n\geq 0}$ be a sequence of integers. If (a_n) satisfies a linear recurrence over $\mathbb{Q}$, then it also satisfies a linear recurrence over $\mathbb{Z}$.*

This is Exercise 2 in Chapter 4 of [Sta12] and we use their solution here. For the proof of this lemma, we introduce the following terminology. The **content** of a power series $F(x) = \sum_{n\geq 0} a_n x^n$ is the greatest common divisor of its coefficients:

$$c(F) := \gcd(a_0, a_1, a_2, \ldots).$$

Let us say that $F(x)$ is **primitive** if $c(F) = 1$. It is not hard to prove that the content function $c : \mathbb{Z}[[x]] \to \mathbb{N}$ is multiplicative:

$$c(FG) = c(F)c(G) \quad \text{for all } F, G \in \mathbb{Z}[[x]].$$

Thus the product of primitive series is primitive.

Proof of Lemma 3.1.3. Let $F(x) = \sum_{n\geq 0} a_n x^n$ be the generating function of (a_n). Then $F(x)$ is a rational function by Proposition 3.1.1, so we can write

$$F(x) = \frac{p(x)}{q(x)}$$

where $p(x), q(x) \in \mathbb{Q}[x]$ are coprime polynomials with $q(0) \neq 0$. We can further assume that $p(x), q(x) \in \mathbb{Z}[x]$ by clearing denominators and cancelling any common factors. Now we are done if we show that $q(0) = \pm 1$, because then the proof of "(b) $\Longrightarrow$ (a)" in Proposition 3.1.1 shows that (a_n) satisfies a linear recurrence with coefficients in $\mathbb{Z}$.

Thus it remains prove that $q(0) = \pm 1$. Since $c(q)c(F) = c(p)$, it follows that $q(x)$ is primitive (or else $c(q)$ is a nontrivial common factor of $p(x)$ and $q(x)$ in $\mathbb{Z}[x]$). Since $p(x), q(x)$ are coprime in $\mathbb{Z}[x]$, we can write

$$a(x)p(x) + b(x)q(x) = m$$

for some $a(x), b(x) \in \mathbb{Z}[x]$ and $m \in \mathbb{Z}$, and plugging in $p(x) = q(x)F(x)$ gives

$$m = q(x)\big(a(x)F(x) + b(x)\big) = q(x)G(x)$$

where $G(x) := a(x)F(x) + b(x)$. Since $q(x)$ is primitive, it follows that the content of $G(x)$ is m — in particular m divides the constant term of G. Say $km = G(0)$ for some $k \in \mathbb{Z}$. Then $m = q(0)G(0) = q(0)km$, so $1 = q(0)k$.] The only way this is possible is if $q(0) = \pm 1$. $\square$

Rational functions are generated by linear recurrences; now we investigate the series generated by *polynomial* recurrences. First we define the **formal derivative** of a power series $F(x) = \sum_{n \geq 0} a_n x^n$ by

$$F'(x) := \sum_{n \geq 1} n a_n x^{n-1} = a_1 + 2a_2 x + 3a_3 x^2 + \cdots .$$

Let $F^{(n)}(x)$ denote the nth derivative of $F(x)$. We say that $F(x)$ is **differentiably finite**, or **D-finite** for short, if it satisfies a differential equation of the form

$$p_0(x)F(x) + p_1(x)F'(x) + \cdots + p_n(x)F^{(n)}(x) = 0$$

for some polynomials $p_0(x), \ldots, p_n(x) \in K[x]$, not all zero.

Example 3.1.4. Any rational function is D-finite: indeed, if $F(x) = p(x)/q(x)$ where the numerator has degree d, then differentiating $F(x)q(x) = p(x)$ more than d times yields the desired differential equation.

Example 3.1.5. Let $F(x) = \sum_{n \geq 0} \frac{1}{n!} x^n$ be the power series expansion of the exponential function e^x. Then $F(x)$ is D-finite because it satisfies the differential equation $F'(x) = F(x)$.

Example 3.1.6. Let $F(x) = \sum n! x^n$. The coefficients satisfy the recurrence relation $a_n = n a_{n-1}$, so the derivative of $F(x)$ is

$$F'(x) = \sum_{n \geq 1} n a_n x^{n-1} = \sum_{n \geq 1} a_{n+1} x^{n-1} = \frac{1}{x^2} \sum_{n \geq 2} a_n x^n = \frac{1}{x^2}(F(x) - 1 - x).$$

Rearranging this shows that $F(x)$ satisfies the differential equation

$$x^2 F'(x) - F(x) + (x + 1) = 0.$$

To get rid of the $x + 1$ term, we can differentiate twice.

Similar to Proposition 3.1.1, we can characterize those sequences whose generating functions are D-finite. Let $(a_n)_{n \geq 0}$ be a sequence of elements of K; then (a_n) is a **polynomial recurrence**, or **P-recurrence** for short, if there are rational functions $q_0(x), \ldots, q_d(x) \in K(x)$ defining a recurrence relation

$$a_{n+1} = q_0(n)a_n + \cdots + q_d(n)a_{n-d} \quad \text{for all } n \geq d.$$

Note that despite the terminology, we allow the coefficients $q_i(n)$ to be *rational* functions in n, not just polynomials. When the $q_i(x)$'s are constant, this is a linear recurrence — this shows that every linear recurrence is P-recursive.

Now we state the characterization of D-finite power series as the generating functions of P-recursive sequences.

Theorem 3.1.7 ([Sta80]). *Let $(a_n)_{n\geq 0}$ be a sequence of elements of a field K, and let $F(x) := \sum_{n\geq 0} a_n x^n$ denote the corresponding generating function. Then the following are equivalent:*

(a) *(a_n) is P-recursive.*

(b) *$F(x)$ is D-finite.*

The salience of P-recursive sequences to dynamics is as follows. Suppose that (a_n) satisfies a recurrence

$$a_{n+1} = q_0(n)a_n + \cdots + q_d(n)a_{n-d} \quad \text{for all } n \geq d,$$

where $q_0(x), \ldots, q_d(x) \in K(x)$ are rational functions in a variable x. Then we can define a dynamical system $\varphi : \mathbb{A}^{d+2} \dashrightarrow \mathbb{A}^{d+2}$ on the affine space $\mathbb{A}^{d+2}$ as follows: if $(t, x_0, \ldots, x_d)$ are coordinates on $\mathbb{A}^{d+2}$, then

$$\varphi(t, x_0, \ldots, x_d) := (t + 1, x_1, \ldots, x_d, q_0(t)x_0 + \cdots + q_d(t)x_d)$$

Thus t is a counter, and φ functions by shifting $x_0, \ldots, x_d$ to the right and using the recurrence to create the new coordinate in the $d + 2$ position. If we set $x := (0, a_0, \ldots, a_d) \in \mathbb{A}^{d+2}$ and $f : \mathbb{A}^{d+2} \to K$, $f(t, x_0, \ldots, x_d) := x_0$, then our original sequence (a_n) can now be obtained via

$$a_n = f(\varphi^n(x_0)).$$

3.1.2 Linear Recurrences in Abelian Groups

In this subsection we develop the necessary background on general recurrences in abelian groups. Because we will ultimately prove a result about a semigroup of morphisms, we will work with sequences indexed by monoids in this section. The proofs of these results become significantly simpler when the underlying monoid is just $(\mathbb{N}_0, +)$ (here $\mathbb{N}_0 := \mathbb{N} \sqcup \{0\}$), which is the key case needed for dealing with a single map.

Let $\mathbb{N}_0 := \mathbb{N} \sqcup \{0\}$ be the set of nonnegative integers. If A is an additive abelian group, then the set $\mathbb{Z}^{\mathbb{N}_0} = \{u : \mathbb{N}_0 \to \mathbb{Z}\}$ of sequences in A can be viewed as a module over the polynomial ring $\mathbb{Z}[x]$, where the indeterminate x acts via the shift: if $u = (u_n)_{n\geq 0}$ is a sequence in A, then $x \cdot u$ is defined by

$$(x \cdot u)_n := u_{n+1} \quad \text{for } n \geq 0.$$

Thus a linear recurrence is precisely a sequence $u \in A^{\mathbb{N}_0}$ which is annihilated by a monic polynomial: there exists a monic $f(x) \in \mathbb{Z}[x]$ so that $f(x) \cdot u = 0$.

Let us generalize this by replacing $\mathbb{N}_0$ by an arbitrary indexing set Z equipped with the action of a multiplicative monoid S. Then the space of functions

$$A^Z := \{u : Z \to A\}$$

is an additive abelian group under pointwise addition, and we extend the action $S \curvearrowright Z$ to a $\mathbb{Z}[S]$-module structure on A^Z, where $\mathbb{Z}[S]$ is the monoid algebra[1] with

[1] $\mathbb{Z}[S]$ consists of formal $\mathbb{Z}$-linear combinations of elements of S, with multiplication extending the multiplication on S.

coefficients in $\mathbb{Z}$. Thus for $s \in S$ and a sequence $u = (u_z)_{z\in Z} \in A^Z$, the product $s \cdot u$ is given by

$$(s \cdot u)_z := u_{sz} \quad \text{for all } z \in Z.$$

The **annihilator** of (u_z) is defined to be

$$\mathrm{Ann}(u) := \{f \in \mathbb{Z}[S] : f \cdot u = 0\}.$$

It is not hard to check that $\mathrm{Ann}(u)$ is a two-sided ideal of $\mathbb{Z}[S]$.

Now we say that $u = (u_z)_{z\in Z}$ satisfies an **S-linear recurrence** if $\mathbb{Z}[S]/\mathrm{Ann}(u)$ is finitely generated as a $\mathbb{Z}$-module. If S is further assumed to be finitely generated as a monoid, then u satisfies an **S-quasilinear recurrence** if there are a set of generators $s_1, \dots, s_d$ of S and a natural number M such that whenever $s_{i_1} \cdots s_{i_M}$ is an element of S that is a product of M elements of $s_1, \dots, s_d$, there is an element in I of the form

$$\sum_{j=1}^{M} c_j s_{i_j} \cdots s_{i_M}$$

with $c_1, \dots, c_M \in \mathbb{Z}$ are coprime, *i.e.* $\gcd(c_1, \dots, c_M) = 1$.

The reason for introducing the notion of quasilinear recurrences is for later convenience, as it is often easier to demonstrate that a sequence satisfies a quasilinear recurrence than a linear one.

Example 3.1.8. In general, a quasilinear recurrence may not be linear. To see this, let $S = \mathbb{N}_0$ and let A be the additive group $(\mathbb{Q}, +)$. Then if we consider the sequence $a_n = 1/2^n$ and identify $\mathbb{Z}[S]$ with $\mathbb{Z}[x]$, then this sequence is annihilated by the primitive polynomial $f(x) = 2x - 1$, but it does not satisfy an S-linear recurrence since a_{n+1} is never in the additive group generated by the initial terms $a_1, \dots, a_n$.

To prove a simple statement such as "the sum of $\mathbb{N}_0$-linear recurrences is again an $\mathbb{N}_0$-linear recurrences", it is enough to take the product of the monic annihilating polynomials for each recurrence, and in this case it is trivial to verify that this product is still monic. To generalize this to the sum of S-linear recurrences where S is a finitely generated monoid, we need the following well-known ring-theoretic fact.

Lemma 3.1.9. *Let R be a finitely generated T-algebra, where T is a noetherian integral domain. Suppose that I, J are ideals of R such that R/I and R/J are finitely generated T-modules. Then:*

(a) *R/IJ is also a finitely generated T-module.*

(b) *I and J are finitely generated as left ideals of R.*

Proof. (a) Let $U = \{u_1, \dots, u_d\}$ be elements of R with $u_1 = 1$ whose images span both R/I and R/J as T-modules and that generate R as a T-algebra. We prove that every finite product of elements from $u_1, \dots, u_d$ is congruent to a T-linear combination of elements of the form $u_i u_j u_k u_\ell$ modulo IJ. (Since $u_1 = 1$, this includes products of smaller length.) We prove this by induction on the length of the product, with the case for products of length at most four following by construction. Suppose now that the result holds for all products of elements from $u_1, \dots, u_d$ of length less than M with $M \geq 5$, and consider a product $u_{i_1} \cdots u_{i_M}$. Then by our choice of U we have

$$u_{i_1} \cdots u_{i_{M-2}} \equiv \sum a_i u_i \pmod{I}$$

and

$$u_{i_{M-1}} u_{i_M} \equiv \sum b_i u_i \pmod{J}$$

for $a_i, b_i \in T$. Hence

$$\left(u_{i_1} \cdots u_{i_{M-2}} - \sum a_i u_i\right)\left(u_{i_{M-1}} u_{i_M} - \sum b_i u_i\right) \in IJ.$$

Then expanding the product, we see that $u_{i_1} \cdots u_{i_M}$ is congruent to a T-linear combination of products of $u_1, \ldots, u_d$ of length at most $\max(M-1, 3) = M-1$, and so by the induction hypothesis it is in the span of products of length at most 4. Thus (a) now follows by induction.

(b) suffices to prove that I is finitely generated as a left ideal. Then since U spans R/I as a T-module, there exist elements $c_{i,j,k} \in T$ such that $\alpha_{i,j} := u_i u_j - \sum_k c_{i,j,k} u_k \in I$ for $1 \leq i, j, k \leq d$. Next, consider the submodule M of T^d consisting of $(t_1, \ldots, t_d) \in T^d$ such that $\sum t_i u_i \in I$. Then since T is noetherian, M is finitely generated as a T-module and we pick elements $\beta_k = \sum t_{i,k} u_i$ for $k = 1, \ldots, s$ such that $(t_{1,k}, \ldots, t_{d,k})$ with $k = 1, \ldots, s$ generate M. Then let L denote the finitely generated left ideal in R generated by the $\alpha_{i,j}$ and β_k. By construction $L \subseteq I$ and so to complete the proof of (b) it suffices to show that $I \subseteq L$. Since the $\alpha_{i,j}$ are in L, a straightforward induction gives that every finite product of $u_1, \ldots, u_d$ is congruent modulo L to a T-linear combination of $u_1, \ldots, u_d$. It follows that if $f \in I$ then $f \equiv \sum t_i u_i \pmod{L}$ for some $t_1, \ldots, t_d \in T$. But since $L \subseteq I$, $t_1 u_1 + \cdots + t_d u_d \in I$ and so by construction, $t_1 u_1 + \cdots + t_d u_d$ is a T-linear combination of the β_k and hence it is in L. It then follows that $f \in L$, giving us that $I \subseteq L$ and showing that $I = L$ and so I is finitely generated as a left ideal. $\square$

Corollary 3.1.10. *Let S be a finitely generated monoid acting on a set Z, let A and B be abelian groups, and let $u \in A^Z$ and $v \in B^Z$ be sequences satisfying S-linear recurrences. Then $(u, v) = (u_z, v_z)_{z \in Z} \in (A \oplus B)^Z$ also satisfies an S-linear recurrence.*

Proof. Let I and J be respectively the annihilators of u and v. Then $\mathbb{Z}[S]/I$ and $\mathbb{Z}[S]/J$ are finitely generated $\mathbb{Z}$-modules and since S is finitely generated, we have that $\mathbb{Z}[S]/IJ$ is a finitely generated $\mathbb{Z}$-module. Since IJ annihilates both u and v, it also annihilates (u, v). The result follows. $\square$

The following lemma generalizes the classical Fatou's Lemma 3.1.3 on rational power series in $\mathbb{Z}[[x]]$.

Lemma 3.1.11. *Let A be a finitely generated abelian group, let S be a finitely generated monoid acting on a set Z. Then every S-quasilinear recurrence is also an S-linear recurrence.*

Proof. Let u be an S-quasilinear recurrence and let I denote the annihilator of u in $\mathbb{Z}[S]$. By Corollary 3.1.10, it suffices to prove this in the case when A is a cyclic group. We first consider the case when $A = \mathbb{Z}$. Then quasilinearity gives that $\mathbb{Z}[S]/I \otimes_{\mathbb{Z}} \mathbb{Q}$ is finite-dimensional as a $\mathbb{Q}$-vector space, as there is some natural number M such that it is spanned by the images of all words of a set of generators of length at most M. We pick $t_1, \ldots, t_d \in S$ such that their images span $\mathbb{Z}[S]/I \otimes_{\mathbb{Z}} \mathbb{Q}$ as a vector space and we let $R = \mathbb{Z}[S]/I$. Consider the $\mathbb{Z}$-submodule N of $\mathbb{Z}^d = A^d$ spanned by elements of the form $v_z := (u(t_1 \cdot z), \ldots, u(t_d \cdot z))$ with $z \in Z$. Then N is finitely generated and hence there exist $z_1, \ldots, z_m \in Z$ such that N is generated by $v_{z_1}, \ldots, v_{z_m}$.

Then we define a homomorphism of additive abelian groups $\Psi : \mathbb{Z}[S] \to A^m$ given by

$$s \mapsto (u(s \cdot z_1), \ldots, u(s \cdot z_m)).$$

We claim that $f \in \mathbb{Z}[S]$ is in the kernel of Ψ if and only if f annihilates u. It is clear that if f annihilates u then it is in the kernel of Ψ. Conversely, suppose that f is in the kernel of Ψ. Then since the images of $t_1, \ldots, t_d$ span $R \otimes_{\mathbb{Z}} \mathbb{Q}$, there are some positive integer m and some integers $c_1, \ldots, c_d$ such that $mf - c_1 t_1 - \cdots - c_d t_d \in I$. Then for $z \in Z$,

$$mf \cdot u_z = (c_1 t_1 + \cdots + c_d t_d) \cdot u_z = \sum_{i=1}^{d} c_i u(t_i \cdot z).$$

Observe that the right-hand side is zero if $\sum_{i=1}^{d} c_i u(t_i z_j) = 0$ for $j = 1, \ldots, m$. But

$$\sum_{i=1}^{d} c_i u(t_i z_j) = mf \cdot u_{z_j} = 0$$

since f is in the kernel of Ψ. It follows that $m \cdot f$ annihilates u and since A is torsion-free we have f is in I, giving us the claim. It follows that Ψ induces an injective map from R into A^m, and so R is a finitely generated abelian group, and so u satisfies an S-linear recurrence.

Next suppose that $A = \mathbb{Z}/n\mathbb{Z}$ with $n > 0$. We suppose towards a contradiction that there exists a sequence $u \in A^Z$ that satisfies an S-quasilinear recurrence but not an S-linear recurrence. We may also assume that n is minimal among all positive integers for which there exists such a sequence in $(\mathbb{Z}/n\mathbb{Z})^Z$. We note that n cannot be prime. To see this, observe that there are generators $s_1, \ldots, s_e$ of S and some M such that for every M-fold product $s_{i_1} \cdots s_{i_M}$ of elements from $s_1, \ldots, s_e$ we have an element in I of the form

$$\sum_{j=1}^{M} c_j s_{i_j} \cdots s_{i_M}$$

with $c_1, \ldots, c_M \in \mathbb{Z}$ satisfying that $\gcd(c_1, \ldots, c_M) = 1$. In particular, there is some smallest j_0 for which n does not divide c_{j_0}. If n is a prime number, then c_{j_0} is invertible modulo n. Then by construction

$$s_{i_1} \cdots s_{i_m} \equiv -c_{j_0}^{-1} \sum_{\ell=j_0+1}^{M} c_\ell s_{i_1} \cdots s_{i_{j_0-1}} s_{i_\ell} \cdots s_{i_M} \pmod{I},$$

where we take $c_{j_0}^{-1}$ to be an integer that is a multiplicative inverse of c_{j_0} modulo n. Then $\mathbb{Z}[S]/I$ is a $\mathbb{Z}/n\mathbb{Z}$-module spanned by words of length at most M in this case. This contradicts our assumption, and so n has a prime factor p and $n = pn_0$ with $n_0 > 1$. Now let $A_0 = \{x \in A : px = 0\}$. Then $\bar{u} := (u_z + A_0)_{z \in Z}$ satisfies an

S-quasilinear recurrence and since A/A_0 is cyclic of order $n_0 < n$, we have that $\bar{u}$ satisfies an S-linear recurrence by induction. Hence if J denotes the annihilator of $\bar{u}$ then $\mathbb{Z}[S]/J$ is a finitely generated $\mathbb{Z}$-module. Then for $f \in J$, we have $f \cdot u \in A_0^Z$ and satisfies an S-quasilinear recurrence and since $|A_0| = p$, it satisfies an S-linear recurrence by minimality of n. In particular, for $f \in J$, if we let J_f denote the annihilator of $f \cdot u$ then $\mathbb{Z}[S]/J_f$ is a finitely generated $\mathbb{Z}$-module. Since $\mathbb{Z}[S]/J$ is a finitely generated $\mathbb{Z}$-module and S is a finitely generated monoid, we have that J is finitely generated as a left ideal. We let $f_1, \ldots, f_q$ denote a set of generators of J as a left ideal. Then by construction the ideal $J' := J_{f_1} f_1 + \cdots + J_{f_q} f_q$ annihilates u. We claim that $\mathbb{Z}[S]/J'$ is a finitely generated $\mathbb{Z}$-module, from which it will follow that u satisfies an S-linear recurrence. Since each $\mathbb{Z}[S]/J_{f_i}$ is a finitely generated $\mathbb{Z}$-module, $L := J_{f_1} \cdots J_{f_q}$ has the property that $\mathbb{Z}[S]/L$ is a finitely generated $\mathbb{Z}$-module. By construction $I \supseteq L f_1 + \cdots + L f_q = LJ$ and since $\mathbb{Z}[S]/L$ and $\mathbb{Z}[S]/I$ are both finitely generated $\mathbb{Z}$-modules, so is $\mathbb{Z}[S]/LI$ and thus so is $\mathbb{Z}[S]/I$. It now follows that u satisfies an S-linear recurrence. $\square$

We require a few more basic facts about recurrences.

Lemma 3.1.12. *Let A be an abelian group, let S be a finitely generated monoid, and let $u = (u_s)_{s \in S}$ be a sequence in A^S. Suppose there is a surjective semigroup homomorphism $\Psi : S \to G$ where G is a finite group and let T be the semigroup $\Psi^{-1}(1)$. Then T acts on the sets $Z_g := \Psi^{-1}(g)$ for each $g \in G$. Suppose that T is finitely generated as a monoid and that for each $g \in G$ $u_g := (u_z)_{z \in Z_g}$ satisfies a T-linear recurrence. Then (u_s) satisfies an S-linear recurrence.*

Proof. For $g \in G$, we let $I_g \subseteq \mathbb{Z}[T]$ denote the annihilator of u_g. Then by assumption $\mathbb{Z}[T]/I_g$ is a finitely generated $\mathbb{Z}$-module and hence $\mathbb{Z}[T]/J$ is also a finitely generated $\mathbb{Z}$-module by Lemma 3.1.9, where $J := \prod_{g \in G} I_g$. By construction, if $f \in J$ then f annihilates each u_g and so, since T acts on each Z_g, we have that f annihilates u. It follows that the ideal $I := \mathbb{Z}[S]J\mathbb{Z}[S] \subseteq \mathbb{Z}[S]$ is contained in the annihilator of u. To finish the proof, it suffices to show that $\mathbb{Z}[S]/I$ is a finitely generated $\mathbb{Z}$-module. We claim that there is a finite subset U of S such that every element of S can be expressed in the form $u_1 t_1 u_2 t_2 \cdots u_{m-1} t_m u_m$, with $m \leq |G|$. To see this, we pick a set of generators $s_1, \ldots, s_d$ of S and let U denote the set of elements of S that can be expressed as a product of elements in $s_1, \ldots, s_d$ of length at most m. Then it is immediate that if s is element of S, then s has an expression of the form $u_1 t_1 u_2 \cdots u_{p-1} t_{p-1} u_p$ for some p. For this element s, we pick such an expression with p minimal. If $p \leq |G|$, there is nothing to prove, so we may assume that $p > |G|$. Then $\Psi(u_1), \Psi(u_1 u_2), \ldots, \Psi(u_1 \cdots u_p)$ are p elements of G and hence two of them must be the same. So there exist i, j with $1 \leq i < j \leq p$ such that $\Psi(u_1 \cdots u_i) = \Psi(u_1 \cdots u_j)$ and so $\Psi(u_{i+1} \cdots u_j) = 1$. In particular, $t := u_{i+1} t_{i+1} \cdots u_{j-1} t_{j-1} u_j \in T$ and thus we can rewrite s as $u_1 t_1 \cdots u_{i-1} (t_i t t_j) u_{j+1} \cdots t_{p-1} u_p$, which contradicts the minimality of p in our expression for s. The claim now follows.

Since $\mathbb{Z}[T]/J$ is a finitely generated $\mathbb{Z}$-module, there exists a finite subset V of T such that $\mathbb{Z}[T]/J$ is spanned by images of elements of V. It follows that $\mathbb{Z}[S]/I$ is spanned as a $\mathbb{Z}$-module by images of elements of the form $u_1 t_1 u_2 t_2 \cdots u_{m-1} t_m u_m$ with $u_i \in U$ and $t_i \in V$ and $m \leq |G|$. Thus $\mathbb{Z}[S]/I$ is a finitely generated $\mathbb{Z}$-module and so (u_s) satisfies an S-linear recurrence, as required. $\square$

Recall from Theorem 2.3.10 that if $(a_n)_{n\geq 0}$ is a sequence satisfying a linear recurrence in an abelian group A, and $B \leq A$ is any subgroup, then

$$\mathrm{Ret}(a_n, B) = \{n \geq 0 : a_n \in B\}$$

is a finite union of arithmetic progressions. If A is finitely generated, then the same conclusion is true if $(a_n)_{n\geq 0}$ is an $\mathbb{N}_0$-quasilinear recurrence (because all such sequences are automatically $\mathbb{N}_0$-linear by Lemma 3.1.11). If A is not finitely generated, we may not enjoy such a conclusion. However, in the case that A is the multiplicative group of units in a finitely generated field extension of $\mathbb{Q}$, we can make the following argument.

Proposition 3.1.13. *Let K be a finitely generated extension of $\mathbb{Q}$, and let $(u_n) \in (K^\times)^{\mathbb{N}_0}$ be a sequence satisfying a multiplicative $\mathbb{N}_0$-quasilinear recurrence. Then in fact (u_n) satisfies a (multiplicative) linear recurrence. Thus if H is a finitely generated multiplicative subgroup of $K^\times$, then $\{n \geq 0 \colon u_n \in H\}$ is a finite union of arithmetic progressions.*

This is not true without the hypothesis that K is finitely generated as an extension of $\mathbb{Q}$. For example if $K = \mathbb{C}$ and $u_n = \exp(2\pi i/2^n)$, then $u_n^2 = u_{n-1}$ and so (u_n) satisfies a quasilinear recurrence. But since u_n is never in the subfield generated by $u_1, \ldots, u_{n-1}$, it follows that u_n does not satisfy a linear recurrence.

Proof of Proposition 3.1.13. The assumption that (u_n) is a quasilinear recurrence means that there are some $d \geq 0$ and integers $i_0, \ldots, i_d$ with $\gcd(i_0, \ldots, i_d) = 1$ so that the following relation holds for all $n \geq 0$:

$$u_n^{i_0} \cdots u_{n+d}^{i_d} = 1.$$

Then if G is the subgroup generated by $u_0, \ldots, u_d$, it follows that u_n lies in the *radical* of G for all $n \geq 0$:

$$\sqrt{G} := \{g \in K^\times : g^m \in G \text{ for some } m \geq 1\}.$$

We will show that $\sqrt{G}$ is finitely generated, from which the desired conclusion follows from Lemma 3.1.11.

To see that $\sqrt{G}$ is finitely generated: since $K/\mathbb{Q}$ is finitely generated, K is a finite extension of a function field $L = \mathbb{Q}(t_1, \ldots, t_m)$. Now let $R = \mathbb{Z}[G, t_1, \ldots, t_d]$ be the subring of K generated by $t_1, \ldots, t_d$ and G, and let $F := \mathrm{Frac}(R)$ so that K/F is finite. Finally let $\overline{R}$ denote the integral closure of R in K. Then R is a finitely generated $\mathbb{Z}$-algebra, so the same is true for $\overline{R}$ [Eis95, Corollary 13.13]. It follows that the group of units $\overline{R}^*$ is finitely generated by Roquette's Theorem [Roq57]. But $\sqrt{G} \leq \overline{R}^*$ since every element of $\sqrt{G}$ is integral over R. Thus $\sqrt{G}$ is finitely generated.

Now let $H_0 := H \cap \sqrt{G}$. Then by Theorem 2.3.9, the set $\{n \geq 0 \colon u_n \in H_0\}$ is a finite union of arithmetic progressions, and since $u_n \in H$ if and only if $u_n \in H_0$ we obtain the result. $\square$

3.2 Multiplicative Dependence

The goal of this section is to establish a key lemma which converts the statement of Theorem 3.0.1 into a problem about quasilinear recurrences. Thus we may apply our results on quasilinear recurrences to obtain the main theorem.

Let K be a field and let k be a subfield of K. Elements $a_1, \ldots, a_n \in K^\times$ are *multiplicatively dependent modulo* $k^\times$ if there are integers $i_1, \ldots, i_n \in \mathbb{Z}$, not all zero, such that $a_1^{i_1} \cdots a_n^{i_n} \in k^\times$. If $a_1, \ldots, a_n \in K^\times$ are not multiplicatively dependent modulo $k^\times$ then they are *multiplicatively independent modulo* $k^\times$.

Observe that if k is algebraically closed in K, the integers $i_0, \ldots, i_d$ in this definition can be chosen to satisfy $\gcd(i_0, \ldots, i_d) = 1$. Indeed, if $m = \gcd(i_0, \ldots, i_d)$, then $(i_0, \ldots, i_d) = (mj_0, \ldots, mj_d)$ for some $j_0, \ldots, j_d$, and set $g := f_0^{j_0} \cdots f_d^{j_d}$. Then g^m is in $k^\times$. But then $g \in k^\times$ as k is algebraically closed. Since $\gcd(j_0, \ldots, j_d) = 1$, this is the required multiplicative dependence modulo $k^\times$.

Let K be an algebraically closed field and let X be an irreducible quasiprojective variety over K. For a group $G \leq K^*$ and rational functions $f_1, \ldots, f_n \in K(X)$, we set

$$X_G(f_1, \ldots, f_n) := \{x \in X : f_1(x), \ldots, f_n(x) \in G\} = \bigcap_{i=1}^{n} f_i^{-1}(G). \tag{3.1}$$

Notice that if $X = \mathbb{A}^n$ and $f_i(x_1, \ldots, x_n) := x_i$ is a coordinate function, then $X_G(f_1, \ldots, f_n)$ is the set $X(G)$ of affine points with coordinates in G. The set X_G has been studied in [BOSS] in the case $X = \mathbb{P}^1$ and $f_0 = f_1 = f : \mathbb{P}^1 \to \mathbb{P}^1$ is a rational function; they determine exactly the form of such f so that X_G is infinite. Similarly, multiplicative dependence of values of rational functions has been studied in [OSSZ19].

Now we state our key lemma.

Lemma 3.2.1. *Let K be an algebraically closed field of characteristic zero, let G be a finitely generated multiplicative subgroup of K^*, let X be an irreducible quasiprojective variety over K of dimension d, and let $f_0, \ldots, f_d \in K(X)$ be $d+1$ rational functions on X. If $X_G(f_0, \ldots, f_d)$ is Zariski dense in X, then $f_0, \ldots, f_d$ are multiplicatively dependent modulo $K^\times$.*

Proof. Since the field extension $K(X)/K$ has transcendence degree d, the functions $f_0, \ldots, f_d$ must be algebraically dependent over K. Thus there is a polynomial relation

$$\sum_{i_0, \ldots, i_d} c_{i_0 \cdots i_d} f_0^{i_0} \cdots f_d^{i_d} = 0$$

where $c_{i_0 \cdots i_d} \in K$ and the sum is over a finite set of indices in $\mathbb{N}_0^{d+1}$; this holds on some open subset of X. To simplify notation, let I be the (finite) set of those indices $\alpha = (i_0, \ldots, i_d) \in \mathbb{N}_0^{d+1}$ where $c_{i_0 \cdots i_d}$ is nonzero. For $\gamma = (i_0, \ldots, i_d) \in \mathbb{Z}^{d+1}$, we set

$$f^\gamma := f_0^{i_0} \cdots f_d^{i_d}.$$

Then for every $y \in X_G$, the I-tuple $(c_\alpha f^\alpha(y))_{\alpha \in I}$ is a solution to the S-unit equation

$$\sum_{\alpha \in I} X_\alpha = 0$$

in the group $\overline{G}$ generated by $G \cup \{c_\alpha : \alpha \in I\}$. This tuple may be *degenerate* in the sense that some subsum vanishes, so we partition it into nondegenerate subtuples. Thus, for each partition $\pi \vdash I$, say $\pi = \{I_1, \ldots, I_m\}$, we let $X_{G,\pi}$ be the set of points $y \in X_G$ such that, for each $s = 1, \ldots, m$, the I_s-tuple $(c_\alpha f^\alpha(y))_{\alpha \in I_s}$ is nondegenerate (*i.e.* its sum vanishes, but no subsum vanishes). Note that there is a decomposition $X_G = \bigcup_{\pi \vdash I} X_{G,\pi}$ and hence there is some partition π of I such that $X_{G,\pi}$ is Zariski dense in X. Notice $X_{G,\pi}$ is empty if π has some part of size 1, and hence if $\pi = (I_1, \ldots, I_m)$ then each I_k has size at least two since $c_\alpha f^\alpha(y) \neq 0$ for $\alpha \in I$ and $y \in X_G$. Thus there exist α, β, two distinct indices in the same component I_s of π.

By the Main Theorem on S-unit equations [ESS02], an S-unit equation in characteristic zero has only finitely many nondegenerate solutions up to scalar multiplication [ESS02]. Let $(t_{1,\mu})_{\mu \in I_s}, \ldots, (t_{n,\mu})_{\mu \in I_s}$ be all solutions to the equation

$$\sum_{\mu \in I_s} t_\mu = 0$$

up to scaling. Then for each $y \in X_{G,\pi}$, we know that $(c_\mu f^\mu(y))_{\mu \in I_s}$ is a multiple of some $(t_{j,\mu})_{\mu \in I_s}$, so there is some $g \in \overline{G}$ such that

$$c_\mu f^\mu(y) = g t_{j,\mu} \qquad \text{for all } \mu \in I_s.$$

Here g, j may depend on y. But then for $\alpha, \beta \in I_s$, we can take quotients to get

$$f^{\alpha - \beta}(y) = \frac{c_\beta t_{j,\alpha}}{c_\alpha t_{j,\beta}}$$

and there are only finitely many possible values for the right-hand side of this equation, independent of y. Taking $\gamma = \alpha - \beta$, we have $f^\gamma(y)$ takes only finitely many values for $y \in X_{G,\pi}$. Since X is irreducible and f^γ is constant on $X_{G,\pi}$, which is Zariski dense in X, we have $f^\gamma \in K^\times$, which completes the proof. □

3.2.1 Interpolation of G-Valued Orbits as Recurrences

In this section we prove the following result:

Proposition 3.2.2. *Let $\varphi : X \to X$ be a rational mapping of a quasiprojective variety X defined over an algebraically closed field K of characteristic zero, and let $f : X \dashrightarrow K$ be a dominant rational map. Suppose that $x \in X$ is a point whose forward φ-orbit is defined and avoids the indeterminacy locus of f. Suppose that there is a finitely generated multiplicative subgroup G of $K^\times$ such that*

$$f(\varphi^n(x)) \in G \quad \text{for all } n \geq 0.$$

Then there are integers p and L with $p \geq 0$ and $L > 0$ such that if $h_1, \ldots, h_m$ generate G then there are integer valued linear recurrences $b_{j,1}(n), \ldots, b_{j,m}(n)$ for $j \in \{0, \ldots, L\}$ such that

$$f \circ \varphi^{Ln+j}(x) = \prod_i h_i^{b_{j,i}(n)}$$

for $n \geq p$.

In fact we prove a more general version for semigroups of maps. We find it convenient to fix the following assumptions and notation for the remainder of this section.

- Let K be an algebraically closed field of characteristic zero.
- Let G be a finitely generated multiplicative subgroup of $K^\times$.
- Let X be an irreducible quasiprojective variety over K.
- Let $\varphi_1, \ldots, \varphi_m : X \dashrightarrow X$ be rational maps, and let S denote the monoid generated by these maps under composition;
- Let S^{op} denote the *opposite semigroup*, which is, as a set, just S but with multiplication $\star$ given by $\mu_1 \star \mu_2 = \mu_2 \circ \mu_1$.
- Let $f : X \dashrightarrow K$ be a non-constant rational function.
- Let $x_0 \in X$ be a point whose forward S-orbit under S is Zariski dense, and each point avoids the indeterminacy loci of the maps $\varphi_1, \ldots, \varphi_m$ and f.

With these data fixed, we may thus define a sequence u in K^S by

$$u_\varphi := f(\varphi(x_0)).$$

Notice that the semigroup algebra $\mathbb{Z}[S^{\mathrm{op}}]$ acts on K^S via the rule

$$\varphi \cdot (v_\mu)_{\mu \in S} = (v_{\mu \circ \varphi})_{\mu \in S}$$

for $\varphi \in S$. In this section, we analyze the case when $u_\varphi \in G$ for every $\varphi \in S$.

Proposition 3.2.3. *Adopt that assumptions and notation of Notation 3.2.1. If $f(\varphi(x_0)) \in G$ for every $\varphi \in S$, then $(f(\varphi(x_0)))_{\varphi \in S^{\mathrm{op}}}$ satisfies a multiplicative S^{op}-linear recurrence.*

Proof. We let $C \subseteq (K^\times)^S$ denote the set of constant sequences and let v denote the image of u in K^S/C. We first show that v satisfies an S^{op}-quasilinear recurrence. Let d denote the dimension of X and let $\varphi_{i_1} \circ \cdots \circ \varphi_{i_{d+1}}$ be a $(d+1)$-fold composition of $\varphi_1, \ldots, \varphi_m$, let $\mu_j := \varphi_{i_j} \circ \cdots \circ \varphi_{i_{d+1}}$ for $j = 1, 2, \ldots, d+1$, and let $f_j = f \circ \mu_j$. Then we take $X_G := X_G(f_1, \ldots, f_{d+1})$, as in Equation (3.1). The assumption that $u_\varphi \in G$ for $\varphi \in S$ implies that X_G contains the orbit of x_0 under S, which is dense. Thus $\overline{X_G} = X$ and it follows from Lemma 3.2.1 that $f_1, \ldots, f_{d+1}$ are multiplicatively dependent modulo $K^\times$. Hence

$$f_1^{p_1} \cdots f_{d+1}^{p_{d+1}} \equiv c$$

where $c \in K^\times$ is a constant and $p_1, \ldots, p_{d+1} \in \mathbb{Z}$ with $\gcd(p_1, \ldots, p_{d+1}) = 1$. Now evaluating this at $\varphi(x_0)$ gives

$$u_{\varphi \star \mu_1}^{p_1} \cdots u_{\varphi \star \mu_{d+1}}^{p_{d+1}} = c \quad \text{for all } \varphi \in S.$$

In particular, $p_1\mu_1 + \cdots + p_{d+1}\mu_{d+1} \in \mathbb{Z}[S^{\mathrm{op}}]$ annihilates v. It follows that v satisfies an S^{op}-quasilinear recurrence and it now follows from Lemma 3.1.11 that it satisfies an S^{op}-linear recurrence. We now claim that u satisfies an S^{op}-linear recurrence. To see this, let $I \subseteq \mathbb{Z}[S^{\mathrm{op}}]$ denote the annihilator of v. Then we have shown that $R := \mathbb{Z}[S^{\mathrm{op}}]/I$ is a finitely generated $\mathbb{Z}$-module. In particular, there exists some M such that R is spanned as a $\mathbb{Z}$-module by compositions of $\varphi_1, \ldots, \varphi_m$ of length at most M. Now let J denote the annihilator of u. We claim that $\mathbb{Z}[S^{\mathrm{op}}]/J$ is spanned as a $\mathbb{Z}$-module by compositions of length at most $M+1$, which will complete the proof that u satisfies an S^{op}-linear recurrence. So to show this, let φ be a composition of length $\ell \geq M+1$. We shall show by induction on ℓ that φ is equivalent mod J to a $\mathbb{Z}$-linear combination of compositions of $\varphi_1, \ldots, \varphi_m$ of length $M+1$, with the base case $\ell = M+1$ being immediate. So suppose that the claim holds whenever $\ell < q$ and consider the case when $\ell = q$. Then we can write $\varphi = \mu \circ \varphi_j$ for some μ that is a composition of length $q-1$ and some $j \in \{1, \ldots, m\}$. Then $\mu \equiv \sum m_j \mu_j \pmod{I}$, where the m_j are integers and the μ_j are all compositions of $\varphi_1, \ldots, \varphi_m$ of length at most M. In particular, $(\mu - \sum m_j \mu_j) \cdot u \in C$ and so $(\varphi_j - 1) \star (\mu - \sum m_j \mu_j) \cdot u = 0$. Hence

$$\mu \circ \varphi_j \equiv \mu - \sum_j m_j(\mu_j \circ \varphi_j - \mu_j) \pmod{J}.$$

By the induction hypothesis the right-hand side is equivalent mod J to a $\mathbb{Z}$-linear combination of compositions of $\varphi_1, \ldots, \varphi_m$ of length $M+1$, and so we now obtain the result. $\square$

Proposition 3.2.3 gives a combinatorial description of the sequence $(u_\phi)_{\phi \in S}$. We now give a more geometric interpretation of this result.

Corollary 3.2.4. *Adopt the assumptions and notation of Notation 3.2.1. Suppose that*

$$f(\varphi(x_0)) \in G \quad \textit{for all } \varphi \in S.$$

Then there exists a dominant rational map $\Theta : X \dashrightarrow \mathbb{G}_m^d$ that is defined at each point in the orbit $\mathcal{O}_\varphi(x_0)$, and endomorphisms $\Phi_1, \ldots, \Phi_m : \mathbb{G}_m^d \to \mathbb{G}_m^d$ such that the following diagram commutes

$$\begin{tikzcd} X \arrow[r, dashed, "\varphi_1, \ldots, \varphi_m"] \arrow[d, dashed, "\Theta"'] & X \arrow[d, dashed, "\Theta"] \\ \mathbb{G}_m^d \arrow[r, "\Phi_1, \ldots, \Phi_m"'] & \mathbb{G}_m^d. \end{tikzcd}$$

Moreover, $f = g \circ \Theta$, where $g : \mathbb{G}_m^d \to \mathbb{G}_m$ is a map of the form

$$g(t_1, \ldots, t_d) = C t_1^{i_1} \cdots t_d^{i_d}$$

for some $i_1, \ldots, i_d \in \mathbb{Z}$.

Proof. We let S^{op} denote the opposite monoid of S. Then by Proposition 3.2.3 the sequence $u := (f \circ \varphi(x_0))_{\varphi \in S} \in G^S$ satisfies a multiplicative S^{op}-linear recurrence. It follows that there is some M such that every M-fold composition of $\varphi_1, \ldots, \varphi_m$ is congruent, modulo the annihilator of u, to a $\mathbb{Z}$-linear combination of j-fold compositions of these endomorphisms, as j ranges over numbers $< M$. Let W denote the set of j-fold compositions of $\varphi_1, \ldots, \varphi_m$ with $j < M$. Then we construct a rational map $\Theta : X \dashrightarrow \mathbb{G}_m^L$, where $L = |W|$, given by $\Theta(x) = (f \circ \varphi(x))_{\varphi \in W}$. Now let $i \in \{1, \ldots, m\}$ and consider $\Theta(\varphi_i(x)) = (f \circ \varphi \circ \varphi_i(x))_{\varphi \in W}$. By construction $f = \pi \circ \Theta$, where π is a suitable projection.

Then for $\varphi \in W$ and $i \in \{1, \ldots, m\}$, $\varphi \circ \varphi_i$ either remains in W or it is an M-fold composition of $\varphi_1, \ldots, \varphi_m$, in which case the fact that u satisfies an S^{op}-linear recurrence gives that there exist integers p_μ for each $\mu \in W$ such that

$$f \circ \varphi \circ \varphi_i(x) = \prod_{\mu \in W} (f \circ \mu(x))^{p_w}$$

for all x in the S-orbit of x_0. In particular, since the S-orbit of x_0 is Zariski dense in X, $\Theta \circ \varphi_i = \Psi_i \circ \Theta$ for some self-map Ψ_i of $\mathbb{G}_m^L$ of the form

$$(u_1, \ldots, u_L) \mapsto \left(\prod_j u_j^{p_{1,j}}, \ldots, \prod_j u_j^{p_{L,j}} \right).$$

In particular, each Ψ_i is a group endomorphism of the multiplicative torus. Now let Y denote the Zariski closure of the S-orbit of x_0 under Θ. Then by construction Y has a Zariski dense set of points in $G^L \leq \mathbb{G}_m^L$ and is irreducible. Then a theorem of Laurent [Lau84, Théorème 2] gives that Y is a translate of a subtorus of $\mathbb{G}_m^L$. In particular, $Y \cong \mathbb{G}_m^d$ for some $d \leq \dim(X)$ and $\Psi_1, \ldots, \Psi_d$ restrict to endomorphisms of Y. Moreover, since Y is a translation of a subtorus, the restriction of π to Y induces a map $g : \mathbb{G}_m^d \to \mathbb{G}_m$ of the form $g(u_1, \ldots, u_d) \mapsto C u_1^{q_1} \cdots u_d^{q_d}$. The result now follows. $\square$

In fact, it can be observed that $\Theta(x_0) \in G^d$ and that Ψ_i induce maps of $\mathbb{G}_m^d$ of the form

$$(x_1, \ldots, x_d) \mapsto (\lambda_1 x_1^{p_{1,1}} \cdots x_d^{p_{1,d}}, \ldots, \lambda_d x_1^{p_{d,1}} \cdots x_d^{p_{d,d}})$$

with $\lambda_1, \ldots, \lambda_d \in G$; finally, $g(x_1, \ldots, x_d) \mapsto C x_1^{q_1} \cdots x_d^{q_d}$ with $C \in G$.

The following example shows that the conclusion to Corollary 3.2.4 does not necessarily hold if K has positive characteristic.

Example 3.2.5. Let $K = \bar{\mathbb{F}}_p(u)$ and let $X = \mathbb{P}^1_K$. Then we have a map $\varphi : X \to X$ given by $t \mapsto t^p + 1$ and let $f : X \to \mathbb{P}^1$ be the map $f(t) = t$. Notice that if we take $x_0 = u$ then $f \circ \varphi^n(u) = u^{p^n} + n = u^{p^n}(1 + n/u)^{p^n}$ and hence $\varphi^n(u)$ lies in the finitely generated subgroup G of K generated by u and $1 + n/u$ for $n = 1, 2, \ldots, p-1$. Then if the conclusion to Corollary 3.2.4 held, we would necessarily have $d = 1$ since Θ is dominant and $f \circ \varphi^n(u)$ has infinite orbit. Thus the function fields of $\mathbb{P}^1$ and $\mathbb{G}_m^d$ are both isomorphic to $K(t)$ and the commutative diagram given in the statement of Corollary 3.2.4 would give rise to a corresponding diagram at the level of functions fields:

$$\begin{tikzcd} K(t) \arrow[r, dashed, "\Phi^*"] \arrow[d, dashed, "\Theta^*"'] & K(t) \arrow[d, dashed, "\Theta^*"] \\ K(t) \arrow[r, dashed, "\varphi^*"'] & K(t) \end{tikzcd}$$

with $\varphi^*(t) = t^p + 1$ and $\Phi^*(t) = Ct^a$ for some integer a and some $C \in K$. Moreover, $f^* = \Theta^* \circ g^*$ and since f^* is the identity map of $K(t)$, Θ^* and g^* are automorphisms of $K(t)$; since $g^*(t) = C' t^b$ for some integer a and some $C' \in K$, we have $b = \pm 1$, and so $\Theta^*(t) = C'^{-b} t^b$. But now $\Theta^* \circ \Phi^*(t) = (C')^{-ab} C t^{ab}$ and $\varphi^* \circ \Theta^*(t) = (C')^{-b}(t^p + 1)^{-b}$, and so the two sides do not agree.

Proof of Proposition 3.2.2. For each $n \geq 1$, we let $X_{\geq n}$ denote the Zariski closure of $\{\varphi^m(x_0) \colon m \geq n\}$. Since the $X_{\geq i}$ form a descending chain of closed sets and since X endowed with the Zariski topology is a noetherian topological space, there is some m such that $X_{\geq m} = X_{\geq m+1} = \cdots$. We let $Y = X_{\geq m}$ and we let $Z_1, \ldots, Z_r$ denote the irreducible components of Y. By our choice of m, φ induces a dominant rational self-map of Y and in particular there is some permutation σ of $\{1, \ldots, r\}$ such that $\varphi(Z_i)$ is Zariski dense in $Z_{\sigma(i)}$. It follows that there is some L such that φ^L maps each Z_i into itself. Let $j \in \{m, \ldots, m+L-1\}$. Then $\varphi^j(x_0) \in Z_i$ for some i. Then by the above, we have $\{\varphi^{Ln+j}(x_0) \colon n \geq 0\}$ is Zariski dense in Z_i. Moreover, $f(\varphi^{Ln+j}(x_0)) \in G$ for every $n \geq 0$ and so there are some $e \geq 0$ and some endomorphism $\Psi : \mathbb{G}_m^e \to \mathbb{G}_m^e$ and a map $g : \mathbb{G}_m^e \to \mathbb{G}_m$ such that $f(\varphi^{Ln+j}(x_0)) = g \circ \Psi^n(z_0)$ for some $z_0 \in \mathbb{G}_m^e$ whose coordinates lie in G. Let $h_1, \ldots, h_m$ be a set of generators for G. Then

$$\Psi^n(z_0) = (h_1^{a_{1,1}(n)} \cdots h_m^{a_{1,m}(n)}, \ldots, h_1^{a_{e,1}(n)} \cdots h_m^{a_{e,m}(n)})$$

for some integer-valued sequence $a_{i,j}(n)$. (There may be several choices for the sequences $a_{i,j}(n)$ if the h_i are not multiplicatively independent.) Since

$$\Psi(x_1, \ldots, x_e) = (h_1^{p_{1,1}} \cdots h_m^{p_{1,m}} x_1^{q_{1,1}} \cdots x_e^{q_{1,e}}, \ldots, h_1^{p_{e,1}} \cdots h_m^{p_{e,m}} x_1^{q_{e,1}} \cdots x_e^{q_{e,e}}),$$

there is a choice of sequences $a_{i,j}(n)$ such that there are an integer matrix A and an integer vector $\mathbf{p}$ such that

$$\mathbf{v}(n+1) = A\mathbf{v}(n) + \mathbf{p}$$

for every $n \geq 0$, where $\mathbf{v}(n)$ is the column vector whose entries are $a_{i,j}(n)$ for $i = 1, \ldots, e$, and $j = 1, \ldots, m$ in some fixed ordering of the indices that does not vary with n. In particular, if $Q(x) = q_0 + q_1 x + \cdots + q_r x^r \in \mathbb{Z}[x]$ then

$$Q(A)\mathbf{v}(n) = q_0\mathbf{v}(n) + q_1\mathbf{v}(n+1) + \cdots + q_r\mathbf{v}(n+r) + \mathbf{b}_Q$$

for $n \geq 0$, where $\mathbf{b}_Q$ is an integer vector that depends upon Q but not upon n. In particular, if we take $Q(x)$ to be the characteristic polynomial of A, the Cayley–Hamilton theorem gives that the vectors $\mathbf{v}(n)$ satisfy a non-trivial affine linear recurrence of the form

$$0 = q_0\mathbf{v}(n) + q_1\mathbf{v}(n+1) + \cdots + q_r\mathbf{v}(n+r) + \mathbf{b}_Q$$

for $n \geq 0$. In particular, substituting $n+1$ for n into this equation and subtracting from our original equation gives a recurrence

$$0 = q_0\mathbf{v}(n) + (q_1 - q_0)\mathbf{v}(n+1) + \cdots + (q_r - q_{r-1})\mathbf{v}(n+r) - q_r\mathbf{v}(n+r+1).$$

It follows that each $a_{i,j}(n)$ satisfies a linear recurrence. Then applying the map g and using the fact that a sum of sequences satisfying a linear recurrence also satisfies a linear recurrence now gives the result. $\square$

3.3 Return Sets to a Group of Units

In this section we prove Theorem 3.0.1. The set up is as follows: X is a quasiprojective variety defined over a field K of characteristic zero, $\varphi : X \dashrightarrow X$ is a rational map, $x_0 \in X$ is a point whose forward φ-orbit is well-defined, $f : X \dashrightarrow K$ is a rational function defined on this orbit, and G is a finitely generated subgroup of $K^\times$. Finally, we let

$$E := \{n \in \mathbb{N}_0 : f(\varphi^n(x_0)) \in G\}.$$

We prove:

Theorem 3.3.1. *E is a finite union of arithmetic progressions and a set of zero Banach density.*

We first show that if E has a positive Banach density then it must contain an infinite arithmetic progression. Once a single arithmetic progression is obtained, we then use noetherian induction to show that E is a union of finitely many arithmetic progressions together with a set of Banach density zero.

3.3.1 A Single Arithmetic Progression

With notation as above, in this section we will prove:

Proposition 3.3.2. *Let X be a quasiprojective variety over an algebraically closed field K of characteristic zero, let $\varphi : X \dashrightarrow X$ be a rational map, let $f : X \dashrightarrow K$ be a rational function, and let $G \leq K^\times$ be a finitely generated group. Suppose that $x_0 \in X$ is a point with well-defined forward φ-orbit that also avoids the indeterminacy locus of f. Then if the set*

$$E := \{n \in \mathbb{N}_0 : f(\varphi^n(x_0)) \in G\}$$

has a positive Banach density then it contains an infinite arithmetic progression.

To prove this result, we require a lemma.

Lemma 3.3.3. *Let K be an algebraically closed field, let X be a quasiprojective variety over K, let $\varphi : X \dashrightarrow X$ and $f : X \dashrightarrow K$ be rational maps, and let x_0 be a point whose forward orbit under φ is defined and is Zariski dense and avoids the indeterminacy locus of f. If $\{n \geq 0 : f(\varphi^n(x_0)) = 0\}$ has Banach density zero and if $u_n := f(\varphi^n(x_0))$ has the property that there exist $C \neq 0$ and integers $i_0, \ldots, i_d$ with $i_0 i_d \neq 0$ and $\gcd(i_0, \ldots, i_d) = 1$ such that $u_n^{i_0} \cdots u_{n+d}^{i_d} = C$ for every $n \geq 0$, then:*

(a) *$u_n \in K^\times$ for all $n \geq 0$; and*

(b) *for all finitely generated subgroups $G \leq K^\times$, the set $\{n \geq 0 : u_n \in G\}$ is a finite union of arithmetic progressions.*

Proof. Since $u_n^{i_0} \cdots u_{n+d}^{i_d} = C$ and since x_0 has a Zariski dense orbit, we have $f^{i_0} = C \prod_{j=1}^{d} (f \circ \varphi^j)^{-i_j}$. In particular, if f has a zero at $\varphi^n(x_0)$ for some n, then there is some $j \in \{1, 2, \ldots, d\}$ for which $f \circ \varphi^j$ has a zero or a pole at $\varphi^n(x_0)$. But since the orbit of x_0 under φ avoids the indeterminacy locus of f, $f(\varphi^{j+n}(x_0)) = 0$ for some $j \in \{1, 2, \ldots, d\}$. Hence if $u_n = 0$ then $u_{n+j} = 0$ for some $j \in \{1, 2, \ldots, d\}$. In particular, $\{n \colon u_n = 0\}$ has a positive Banach density, a contradiction. Thus $u_n \in K^\times$. In fact, there is a finitely generated extension of $\mathbb{Q}$, $K_0 \subseteq K$, such that $x_0 \in X(K_0)$ and such that φ and f are defined over K_0. It follows that $u_n \in K_0^\times$ for all n and using the equation $u_n^{i_0} \cdots u_{n+d}^{i_d} = C$ and substituting $n+1$ for n and taking quotients, we have

$$u_{n+d+1}^{i_d} u_{n+d}^{i_{d-1}-i_d} \cdots u_{n+1}^{i_0 - i_1} u_n^{-i_0} = 1.$$

Moreover, it is straightforward to show that $\gcd(i_0, i_0 - i_1, \ldots, i_{d-1} - i_d, i_d) = 1$ and so (u_n) satisfies an $\mathbb{N}_0$-quasilinear recurrence. But that means it satisfies a linear recurrence by Lemma 3.1.11. In particular, the u_i are all contained in a subfield K_0 of K that is finitely generated over $\mathbb{Q}$ and so the result follows from Proposition 3.1.13. $\square$

Proof of Proposition 3.3.2. By [BGT15, Theorem 1.4] there is some positive integer L such that for $j \in \{0, \ldots, L-1\}$ we have $\mathcal{Z}_j := \{n \colon f \circ \varphi^{Ln+j}(x_0) = 0\}$ is a either a set of Banach density zero or contains all sufficiently large natural numbers. If $\delta(E) > 0$ then there is some j such that $E \cap (L\mathbb{N}_0 + j)$ has a positive Banach density and such that $\mathcal{Z}_j$ has Banach density zero. Then we can replace φ by φ^L and x_0 by $\varphi^j(x_0)$ and we may assume without loss of generality that the set of n for which $f \circ \varphi^n(x_0) = 0$ has Banach density zero.

Let $\mathcal{S}$ denote the collection of Zariski closed subsets Y of X for which there exists a rational self-map $\Psi : Y \dashrightarrow Y$ and $y_0 \in Y$ whose forward orbit under Ψ is well-defined and avoids the indeterminacy locus of f and such that the following hold:

(i) $E(Y, y_0, \Psi, f, G) := \{n \colon f \circ \Psi^n(y_0) \in G\}$ has a positive Banach density but does not contain an infinite arithmetic progression;

(ii) $\{n \colon f \circ \Psi^n(y_0) = 0\}$ has Banach density zero.

If $\mathcal{S}$ is empty, then we are done. Thus we may assume $\mathcal{S}$ is non-empty and since X is a noetherian topological space, there is some minimal element Y in $\mathcal{S}$. By assumption, there exists a rational self-map $\Psi : Y \dashrightarrow Y$ and $y_0 \in Y$ such that conditions (i) and (ii) hold.

Observe that the orbit of y_0 under Ψ must be Zariski dense in Y, since otherwise, we could replace Y with the Zariski closure of this orbit and construct a smaller counterexample. We also note that Y is necessarily irreducible. To see this, suppose towards a contradiction, that this is not the case and let $Y_1, \ldots, Y_r$ denote the irreducible components of Y, with $r \geq 2$. Then since the orbit of y_0 is Zariski dense, Ψ is dominant and hence it permutes the irreducible components of Y in the sense that there is a permutation σ of $\{1, \ldots, r\}$ with the property that $\Psi(Y_i)$ is Zariski dense in $Y_{\sigma(i)}$. It follows that there is some $M > 1$ such that Ψ^M maps Y_i into Y_i for every i. Now there must be some $j \in \{0, \ldots, M-1\}$ such that $(M\mathbb{N} + j) \cap E_Y$ has a positive Banach density. Then $\Psi^j(y_0) \in Y_i$ for some i, and so by construction $E(Y_i, \Psi^j(y_0), \Psi^M, f, G)$ has a positive Banach density. Since Y_i is a proper closed subset of Y, by minimality of Y, the set $E(Y_i, \Psi^j(y_0), \Psi^M, f, G)$ must contain an infinite arithmetic progression. But $E(Y_i, \Psi^j(y_0), \Psi^L, f, G) \subseteq E(Y, y_0, \Psi, f, G)$ and so $E(Y, y_0, \Psi, f, G)$ contains an infinite arithmetic progression, a contradiction. Thus Y is irreducible.

Let $d := \dim(Y)$. Since the Banach density of $E(Y, y_0, \Psi, f, G)$ is positive, a version of Szemerédi's Theorem [Sze75] due to Furstenberg [Fur79, Theorem 1.4] gives that there is a set A of positive Banach density and a fixed integer $b \geq 1$ such that E contains the finite progression

$$a, a+b, a+2b, \ldots, a+db$$

for every $a \in A$. Setting, $f_n := f \circ \Psi^{bn}$ for $n \geq 0$, we have defined $d+1$ rational functions $f_0, \ldots, f_d$, so by Lemma 3.2.1 either the set

$$Y_G := Y_G(f_0, \ldots, f_d) = \{x \in Y : f_0(x), \ldots, f_d(x) \in G\}$$

is contained in a proper subvariety of Y, or the functions $f_0, \dots, f_d$ satisfy some multiplicative dependence relation. We proceed by ruling out the first possibility. Suppose that $\overline{Y_G} \subsetneq Y$. Since $\Psi^a(y_0) \in \overline{Y_G}$ for every $a \in A$, the set

$$P := \{n \in \mathbb{N}_0 : \Psi^n(y_0) \in \overline{Y_G}\}$$

has a positive Banach density. Hence [BGT15, Theorem 1.4] gives that P is a union of infinite arithmetic progressions $A_1, \dots, A_r$ and a set of density zero. In particular, since P has a positive Banach density, P contains an infinite arithmetic progression. But since $P \subseteq E(Y, y_0, \Psi, f, G)$, we then see $E(Y, y_0, \Psi, f, G)$ contains an infinite arithmetic progression, a contradiction. It follows that Y_G is Zariski dense in Y.

Combining this with Lemma 3.2.1, we conclude that there is a multiplicative dependence relation

$$\prod_{s=0}^{d} f(\Psi^{sb}(x))^{i_s} = C \in K^\times, \tag{3.2}$$

where $i_0, \dots, i_d \in \mathbb{Z}$ with $\gcd(i_0, \dots, i_d) = 1$. Then for $a \in \{0, \dots, b-1\}$ we let $u_a(n) := f(\Psi^{a+bn}(y_0))$. Evaluating Equation (3.2) at $x = \Psi^{a+bn}(y_0)$ then gives the relation

$$u_a(n)^{i_0} \cdots u_a(n+d)^{i_d} = C.$$

and so Lemma 3.3.3 gives that $u_a(n) \in K^\times$ for all $n \geq 0$ and that $u_a(n)$ satisfies a multiplicative $\mathbb{N}_0$ linear recurrence and that the set of n for which $u_a(n) \in G$ is eventually periodic. In particular, since there is some a for which the set $\{n \colon u_a(n) \in G\}$ has a positive Banach density, for this a, $\{n \colon u_a(n) \in G\}$ contains an infinite arithmetic progression $c + e\mathbb{N}_0$. This then gives that E contains the infinite arithmetic progression $a + b(c + e\mathbb{N}_0) = (a + bc) + be\mathbb{N}_0$, as required. □

3.3.2 A Union of Arithmetic Progressions

We now use Proposition 3.3.2 to prove Theorem 3.3.1.

Proof of Theorem 3.3.1. First, by [BGT15, Theorem 1.4] there is some positive integer L such that for $j \in \{0, \dots, L-1\}$ we have $\mathcal{Z}_j := \{n \colon f \circ \varphi^{Ln+j}(x_0) = 0\}$ is either a set of Banach density zero or contains all sufficiently large natural numbers. Then to prove the result, it suffices to prove that for every natural number $j \in \{0, \dots, L-1\}$, the set of n for which $f \circ \varphi^{Ln+j}(x_0) \in G$ is a finite union of arithmetic progressions along with a set of Banach density zero. In the case that $\mathcal{Z}_j$ contains all sufficiently large natural numbers, this is immediate; hence we may replace φ by φ^L and x_0 by some point in the orbit under φ and assume without loss of generality that the set $\mathcal{Z}$ of n for which $f \circ \varphi^n(x_0) = 0$ has Banach density zero. We now let $X_{\geq i}$ denote the Zariski closure of $\{\varphi^n(x_0) \colon n \geq i\}$. Then as in the proof of Corollary 3.2.2, we have that there is some m such that $X_{\geq m} = X_{\geq m+1} = \cdots$ and without loss of generality we may replace X with $X_{\geq m}$ and x_0 with $\varphi^m(x_0)$ and assume that the orbit of x_0 is Zariski dense in X. Now let $X_1, \dots, X_r$ denote the irreducible components of X. Then there is some positive integer M such that $\varphi^M(X_i)$ is Zariski dense in X_i for $i = 1, \dots, r$. Then it suffices to prove that for $j \in \{0, \dots, M-1\}$ we have $\{n \colon f \circ \varphi^{Mn+j}(x_0) \in G\}$ is a finite union of arithmetic progressions along with a set of Banach density zero. Since $\{\varphi^{Mn+j}(x_0) \colon n \geq 0\}$ is Zariski dense in some component X_i, we may replace X by X_i, x_0 by $\varphi^j(x_0)$ and φ with φ^M and we may assume that X is irreducible and that $\{\varphi^n(x_0) \colon n \geq 0\}$ is

Zariski dense in X. Now let $E := \{n\colon f(\varphi^n(x_0)) \in G\}$. If E has Banach density zero, then there is nothing to prove. Thus we may assume that E has a positive Banach density, and hence it contains an infinite arithmetic progression, say $a\mathbb{N}_0 + b$ with $a > 0$.

We point out that the Zariski closure, Y, of the set $\{\varphi^{an+b}(x_0)\colon n \geq 0\}$ must be Zariski dense in X, since the union of the closures Y_i of $\varphi^i(Y)$ for $i = 0, 1, \ldots, a-1$ contains all but finitely many points in the orbit of x_0 and hence is dense in X. Since X is irreducible, we then see that Y_i must be X for some i, which then gives that $Y = X$.

Now for each $i \geq 0$, define a rational function $f_i := f \circ \varphi^{ai}$, and set

$$X_G := \{x \in X : f_0(x), \ldots, f_d(x) \in G\},$$

where d is the dimension of X. Then X_G contains $\{\varphi^{an+b}(x_0)\colon n \geq 0\}$, which is Zariski dense in X and so Lemma 3.2.1 gives that the functions $f_0, \ldots, f_d$ satisfy some multiplicative dependence of the form

$$f_0^{i_0} \cdots f_d^{i_d} = c$$

with c nonzero and $i_0, \ldots, i_d$ integers with $\gcd(i_0, \ldots, i_d) = 1$. It follows that if we set $u_n = f(\varphi^n(x_0))$ then $u_n^{i_0} u_{n+a}^{i_1} \cdots u_{n+ad}^{i_d} = c$ for every $n \geq 0$. Moreover, by assumption the set of n for which $u_n = 0$ has Banach density zero and thus by Lemma 3.3.3, the set

$$\{n \in \mathbb{N}_0 : u_n \in G\}$$

is eventually periodic. This completes the proof. $\square$

3.4 Heights of Points in Orbits

Corollary 3.2.2 gives an interesting "gap" about heights of points in the forward orbit of a self-map φ for varieties and maps defined over $\mathbb{Q}$.

First we define the Weil height. Let K be a number field and let M_K be the set of places of K. For a place v, let $|\cdot|_v$ be the corresponding absolute value, normalized so that $|p|_v = p^{-1}$ when v lies over the p-adic valuation on $\mathbb{Q}$. Let K_v be the completion of K at a place v and let $n_v := [K_v : \mathbb{Q}_v]$. Now define a function $H : \overline{\mathbb{Q}} \to [1, \infty)$ as follows: for $x \in \overline{\mathbb{Q}}^{\times}$, choose any number field K containing x, and set

$$H(x)^{[K:\mathbb{Q}]} := \prod_{v \in M_K} \max\{|x|_v^{n_v}, 1\}.$$

This is independent of choice of K and defines a function $H : \overline{\mathbb{Q}} \to [1, \infty)$ called the *absolute Weil height*. We let $h : \overline{\mathbb{Q}} \to [0, \infty)$ be its logarithm; i.e., $h(x) := \log H(x)$. For further background on height functions, we refer the reader to [BG06, Chapter 2] and [Sil07, Chapter 3]. We have the following result.

Theorem 3.4.1. *Let X be an irreducible quasiprojective variety with a dominant self-map $\varphi : X \to X$ and let $f : X \to \mathbb{P}^1$ be a rational map, all defined over $\bar{\mathbb{Q}}$. Suppose that $x \in X$ has the following properties:*

1. *every point in the orbit of x under φ avoids the indeterminacy loci of φ and f;*

2. *there is a finitely generated multiplicative subgroup G of $\bar{\mathbb{Q}}^\times$ such that $f \circ \varphi^n(x) \in G$ for every $n \in \mathbb{N}_0$.*

Then if $h(f \circ \varphi^n(x)) = \mathrm{o}(n^2)$ then the sequence $(f \circ \varphi^n(x))_n$ satisfies a linear recurrence. More precisely, there exists an integer $L \geq 1$ such that for each $j \in \{0, \dots, L-1\}$ there are $\alpha_j, \beta_j \in G$ such that

$$f(\varphi^{Ln+j}(x)) = \alpha_j \beta_j^n. \quad \textit{for all sufficiently large } n \geq 0.$$

To prove this result, we first require an elementary estimate.

Lemma 3.4.2. *Let K be a number field and let G be a finitely generated free abelian subgroup of $K^\times$ with multiplicative basis $g_1, \dots, g_r$ for G. Then there exists a real constant $C > 0$ such that for each $a = g_1^{k_1} \cdots g_r^{k_r} \in G$ with $k_1, \dots, k_r \in \mathbb{Z}$, we have the estimate*

$$h(a) \geq \max_{1 \leq i \leq s} C|k_i|.$$

Proof. Since G is a finitely generated subgroup of $K^\times$ there exists a finite set S of places of K such that $|g|_v = 1$ for every $g \in G$ whenever $v \notin S$. Let $v_1, \dots, v_s$ denote the elements of S. Then for $i \in \{1, \dots, s\}$ we have a group homomorphism

$$\Psi_i : G \to \mathbb{R}$$

given by $g \mapsto \log |g|_{v_i}$. Then there is a linear form $L_i(x_1, \dots, x_r)$ such that for $a = g_1^{k_1} \cdots g_r^{k_r} \in G$,

$$\Psi_i(a) = L_i(k_1, \dots, k_r).$$

We claim that $h(a) \geq |L_i(k_1, \dots, k_s)|$ for $i = 1, \dots, s$. To see this, fix $i \in \{1, \dots, s\}$. Since $\Psi(a^{-1}) = -\Psi(a)$ and since $h(a) = h(a^{-1})$, we may assume without loss of generality that $|a|_{v_i} \geq 1$ and so $L_i(k_1, \dots, k_s) \geq 0$. Then

$$\begin{aligned} h(a) &= \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} \log \max\{|a|_v^{n_v}, 1\} \\ &\geq \frac{1}{[K:\mathbb{Q}]} \log \max\{|a|_{v_i}^{n_{v_i}}, 1\} \\ &= \frac{n_{v_i}}{[K:\mathbb{Q}]} L_i(k_1, \dots, k_s). \end{aligned}$$

Thus there is a positive constant κ such that $h(a) \geq \kappa \cdot |L_i(k_1, \dots, k_s)|$ for $i = 1, \dots, s$ and so

$$h(a) \geq \kappa \cdot \max_{1 \leq i \leq s} (|L_i(k_1, \dots, k_s)|).$$

By construction, the homomorphism $\Psi : G \to \mathbb{R}^s$ given by $g \mapsto (\Psi_i(g))_{1 \leq i \leq s}$ is injective and so the image has rank r. Thus after reindexing, we may assume that $L_1, \dots, L_r$ are linearly independent over $\mathbb{Q}$ and so there exist real constants $c_{i,j}$ for $1 \leq i, j \leq r$ such that

$$\sum_{j=1}^{r} c_{i,j} L_j(x_1, \dots, x_s) = x_i$$

for $i = 1, \dots, r$. In particular, since for a given i the $c_{i,j}$ cannot all be zero, there is some $C > 0$ such that

$$0 \neq \sum_{j=1}^{r} |c_{i,j}| \kappa^{-1} < C^{-1}$$

for $i = 1, \ldots, r$. Then for $a = g_1^{k_1} \cdots g_r^{k_r}$, we have

$$\begin{aligned}
|k_i| &= \left| \sum_{j=1}^{r} c_{i,j} L_j(k_1, \ldots, k_s) \right| \\
&\leq \sum_{j=1}^{r} |c_{i,j}| \cdot |L_j(k_1, \ldots, k_s)| \\
&\leq \left(\sum_{j=1}^{r} |c_{i,j}| \kappa^{-1} \right) h(a)
\end{aligned}$$

Thus $h(a) \geq C|k_i|$ for $i = 1, \ldots, r$, as required. $\square$

Proof of Theorem 3.4.1. Since G is finite direct product of cyclic subgroups, we can find a multiplicative generating $g_1, \ldots, g_d, g_{d+1}, \ldots, g_m$ for G so that $g_1, \ldots, g_d$ generate a free abelian group and $g_{d+1}, \ldots, g_m$ are roots of unity. By Corollary 3.2.2, there are a positive integer L and integer-valued sequences $b_{i,j}(n)$ for $j = 0, \ldots, L-1$ and $i = 1, \ldots, m$, each of which satisfies a linear recurrence, such that

$$f \circ \varphi^{Ln+j}(x) = \prod_i g_i^{b_{i,j}(n)}$$

for $n \geq p$. Then multiplication by a root of unity does not affect the height of a number and so

$$h(f \circ \varphi^{Ln+j}(x)) = h \left(\prod_{i=1}^{d} g_i^{b_{i,j}} \right).$$

Then if $h(f \circ \varphi^{Ln+j}(x)) = \mathrm{o}(n^2)$ then by Lemma 3.4.2 we must have $b_{i,j}(n) = \mathrm{o}(n^2)$ for $j = 0, \ldots, L-1$ and $i = 1, \ldots, d$. Since it also is an integer-valued sequence satisfying a linear recurrence, we have that it is in fact $\mathrm{O}(n)$ and is "piecewise linear"; *i.e.* it has the form $A + Bn$ on progressions of a fixed gap [BNZ, Proposition 3.6]. Formally, this means that there exists a fixed $M \geq 1$ and integers $A_{i,j}, B_{i,j}$ for $j \in \{0, \ldots, M-1\}$ and $i \in \{1, \ldots, d\}$, and integer-valued sequences $c_{i,j}(n)$, which satisfy a linear recurrence for $i = d+1, \ldots, m$ and $j = 0, \ldots, M-1$, such that for n sufficiently large we have

$$f \circ \varphi^{Mn+j}(x) = \prod_{i=1}^{d} g_i^{A_{i,j} + B_{i,j} n} \prod_{i=d+1}^{m} g_i^{c_{i,j}(n)}.$$

Since the g_i are roots of unity for $i = d+1, \ldots, m$ and since integer-valued sequences satisfying a linear recurrence are eventually periodic modulo N for every positive integer N, we see that for n sufficiently large, $f \circ \varphi^{Mn+j}(x)$ has the form

$$\alpha_j \beta_j^n \omega^{t_j(n)},$$

where ω is a fixed N-th root of unity for some $N \geq 1$, $t_j(n)$ is eventually periodic, and $\alpha_j, \beta_j \in G$ and depend only on j and not on n. Since we only care about what holds for n sufficiently large, it is no loss of generality to assume that each $t_j(n)$ is periodic and we let p be a positive integer that is a common period for each of $t_0, \ldots, t_{M-1}$. Then for $j \in \{0, \ldots, M-1\}$ and $i \in \{0, \ldots, p-1\}$ we have

$$f \circ \varphi^{pMn+Mi+j}(x) = \left(\alpha_j \omega^{t_j(i)} \beta_j^i \right) (\beta_j^p)^n.$$

The result now follows. $\square$

3.5 Applications to D-Finite Power Series

In this section we apply our results to D-finite power series, showing how Theorem 3.3.1 generalizes a result of Methfessel [Met00] and Bézivin [Béz89]. We also look at classical results of Pólya [Pól21] and Bézivin [Béz86] through a dynamical lens.

3.5.1 Methfessel's Theorem

In this subsection, we use Theorem 3.0.1 to recover a result of Methfessel on the periodicity of G-coefficients in a D-finite power series. Recall that a formal power series $F(t) = \sum_{n\geq 0} a_n t^n$ is **differentiably finite**, or **D-finite**, if it satisfies a differential equation of the form

$$p_0(t)F(t) + p_1(t)F'(t) + \cdots + p_d(t)F^{(d)}(t) = 0,$$

where the coefficients $p_0(t), \ldots, p_d(t) \in K[t]$ are polynomials, not all zero. By Proposition 3.1.7, it is equivalent to require that the coefficient sequence $(a_n)_{n\geq 0}$ satisfies a **polynomial recurrence relation** of the form

$$a_{n+1} = q_0(n)a_n + \cdots + q_d(n)a_{n-d} \quad \text{for all } n \geq d,$$

where $q_0(t), \ldots, q_d(t) \in K(t)$ are rational functions in t.

By interpolating the sequence (a_n) dynamically, we obtain the following theorem of Methfessel.

Theorem 3.5.1. *Let $F(t) = \sum_{n\geq 0} a_n t^n$ be a D-finite power series with coefficients a_n in a field K of characteristic zero, and let $G \leq K^\times$ be a finitely generated multiplicative group. Then*

$$E := \{n \geq 0 : a_n \in G \cup \{0\}\}$$

is a finite union of arithmetic progressions along with a set of zero Banach density.

Proof. Since $F(x)$ is D-finite, its coefficient sequence is P-recursive: there is a recurrence relation

$$a_{n+1} = \sum_{i=0}^{d} r_i(n)a_{n-i},$$

valid for all sufficiently large n, where the $r_i(x) \in K(x)$ are rational functions [Sta80]. Thus we may define a rational map $\varphi : \mathbb{A}^{d+1} \dashrightarrow \mathbb{A}^{d+1}$ as follows:

$$(t, t_1, \ldots, t_d) \mapsto \left(t+1, t_2, \ldots, t_d, \sum_{i=0}^{d} r_i(t)t_i\right).$$

Here $(t, t_1, \ldots, t_d)$ are coordinates on $\mathbb{A}^{d+1}$. Now there is some $p > 0$ such that none of the $r_i(x)$ have a pole at $x = n$ when $n \geq p$. Now take the initial point to be $x_0 := (p, a_p, \ldots, a_{p+d-1})$ and the rational function $f(t, t_1, \ldots, t_d) := t_1$. Then the sequence $(a_n)_{n\geq 0}$ can be recovered as

$$a_{n+p} = f(\varphi^n(x_0)) \qquad \text{for } n \geq 0. \tag{3.3}$$

After taking a suitable shift of the sequence $(a_n)_{n\geq 0}$, it can be recovered as

$$a_n = f(\varphi^n(x_0)).$$

Thus the desired sets N and N_0 are just

$$N = \{n \in \mathbb{N}_0 : f(\varphi^n(x_0)) \in G\} \text{ and } N_0 = \{n \in \mathbb{N}_0 : f(\varphi^n(x_0)) \in G \cup \{0\}\}.$$

Then we obtain the desired decomposition of N from Theorem 3.3.1; since $N_0 = N \cup Z$, where $Z = \{n \in \mathbb{N}_0 : f(\varphi^n(x_0)) = 0\}$, applying [BGT15, Theorem 1.4] then gives that Z is a finite union of arithmetic progressions along with a set of Banach density zero. Then since both N and Z are expressible as a finite union of infinite arithmetic progressions along with a set of Banach density zero, so is their union. The result follows. □

3.5.2 Theorems of Pólya and Bézivin

Pólya [Pól21] showed that, given a fixed set of prime numbers S, if $F(x) = \sum a_n x^n \in \mathbb{Z}[[x]]$ is the power series of a rational function and the prime factors of a_n lie inside of S for every n, then there is some natural number L such that for n sufficiently large

$$a_{Ln+j} = \frac{A_j}{B_j} \cdot \beta_j^n$$

where A_j, B_j, and β_j are integers whose prime factors lie inside of S for $j = 0, \ldots, L-1$ and B_j divides $A_j \beta_j^m$ for some positive integer m. This result was later extended by Bézivin [Béz86], who showed that if K is a field of characteristic zero and $G \leq K^\times$ is a finitely generated group then if $F(x) = \sum a_n x^n$ is a D-finite power series such that there is some fixed m such that each a_n is a sum of at most m elements of G, then $F(x)$ is rational; moreover, he gave a precise form of these rational functions. We show how to recover Bézivin's theorem in the case that $m = 1$ from the dynamical results we obtained in the preceding sections. In particular, this recovers Pólya's theorem. We conclude by showing the relationship between these classical theorems and the dynamical results developed in the preceding sections. More precisely, we give a dynamical proof of the following result.

Theorem 3.5.2 (Bézivin [Béz86]). *Let K be a field of characteristic zero and let $F(x) = \sum a_n x^n \in K[[x]]$ be a D-finite power series such that $a_n \in G \cup \{0\}$ for every n, where G is a finitely generated subgroup of $K^\times$. Then $F(x)$ is rational.*

To do this, we require a basic result on orders of zeros and poles of coefficients in a D-finite series. We recall that if X is a smooth irreducible projective curve over an algebraically closed field k, and if $k(X)$ is the field of rational functions on X, then to each $p \in X$ we have a discrete nonarchimedean valuation $\nu_p : k(X)^\times \to \mathbb{Z}$ that gives the order of vanishing of a function at p (when the function has a pole at p then this valuation is negative). Then for a function $f \in k(X)^\times$ we have a divisor $\mathrm{div}(f) = \sum_{p \in X} \nu_p(f)[p]$, which is a formal $\mathbb{Z}$-linear combination of points of X. The *support* of $\mathrm{div}(f)$ is the (finite) set of points p for which $\nu_p(f) \neq 0$; that is, it is the set of points where f has a zero or a pole. We make use of the fact $\sum_p \nu_p(f) = 0$ [Har77, II, Corollary 6.10].

Lemma 3.5.3. *Let E be an algebraically closed field of characteristic zero and let K be the field of rational functions of a smooth projective curve C over E. Suppose that $F(x) = \sum a_n x^n \in K[[x]]$ is D-finite, $a_n \neq 0$ for every n, and that there is a finite subset S of C such that $\mathrm{div}(a_n)$ is supported on S for every n. Then for each $p \in S$, $\nu_p(a_n) = \mathrm{O}(n)$.*

Proof. We have a polynomial recurrence

$$R_M(n)a_{n+M} + \cdots + R_0(n)a_n = 0$$

for n sufficiently large. Since each $R_i(n) = \sum_{j=0}^{L} r_{i,j}n^j$, we claim there is a fixed number C_i such that $\nu_p(R_i(n)) = C_i$ for sufficiently large n for each nonzero polynomial R_i. To see this, pick a uniformizing parameter u for the local ring $\mathcal{O}_{X,p}$ and suppose that $Q(x) = q_0 + \cdots + q_L x^L$ is a nonzero polynomial in $K[x]$. Then we can rewrite it as $\sum_{i=0}^{N} u^{m_i} q_i' x^L$ where $m_i = \nu_p(q_i)$ and $q_i' \in \mathcal{O}_{X,p}^{\times}$. Let s denote the minimum of $m_0, \ldots, m_N$. Then $Q(x)/u^s = \sum_{i=0}^{N} u^{m_i - s} q_i' x^L$ and by construction

$$\sum_{i=0}^{N} u^{m_i - s}(p) q_i'(p) x^L$$

is a nonzero polynomial in $E[x]$ and hence it is nonzero for n sufficiently large, which shows that $\nu_p(Q(n)) = s$ for all n sufficiently large. Thus in particular if C is the maximum of the C_i as i ranges over the indices for which $R_i(x)$ is nonzero, then for n sufficiently large

$$\begin{aligned}
\nu_p(a_{n+M}) &= \nu_p(R_M(n)a_{n+M}) - C \\
&= \nu_p(\sum_{i=0}^{M-1} R_i(n)a_{n+i}) - C \\
&\geq -2C + \min(\nu_p(a_{n+i} : i = 0, \ldots, M-1).
\end{aligned}$$

It follows that $\nu_p(a_n) \geq -2Cn + B$ for some constant B for all sufficiently large n. It follows that there is a fixed constant C_0 such that $\nu_p(a_n) \geq -C_0 n$ for every $p \in S$, for all n sufficiently large. To get an upper bound, observe that $\sum_{p \in S} \nu_p(a_n) = 0$ [Har77, II, Corollary 6.10] and so for n sufficiently large we have

$$\nu_p(a_n) = \sum_{q \in S \setminus \{p\}} -\nu_q(a_n) \leq (|S| - 1)C_0 n,$$

which now gives $\nu_p(a_n) = \mathrm{O}(n)$.

□

We now give a quick overview of how one can recover Theorem 3.5.2 from the above dynamical framework.

Proof of Theorem 3.5.2. By Theorem 3.5.1, the set $\{n \geq 0 : a_n \in G\}$ is a finite union of arithmetic progressions along with a set of Banach density zero. Since $F(x) = \sum a_n x^n$ is D-finite if and only if for each $L \geq 1$ and each $j \in \{0, \ldots, L-1\}$, the series $\sum a_{Ln+j} x^n$ is D-finite, it suffices to consider the case when $a_n \in G$ for every n. The fact that the coefficients are P-recursive gives that there is a finitely generated field extension K_0 of $\mathbb{Q}$ such that $F(x) \in K_0[[x]]$. We prove the result by induction on $\mathrm{trdeg}_{\mathbb{Q}}(K_0)$. If $[K_0 : \mathbb{Q}] < \infty$ then K_0 is a number field. Then by [BNZ, Theorem 1.6], $h(a_n) = \mathrm{O}(n \log n)$ and by Equation (3.3) and Theorem 3.4.1, we then get a_n satisfies a linear recurrence, giving the result when K_0 has transcendence degree zero over $\mathbb{Q}$.

We now suppose the the result holds whenever K_0 has transcendence degree less than m, with $m \geq 1$, and consider the case when $\mathrm{trdeg}_{\mathbb{Q}}(K_0) = m$. Then there is subfield E of K_0 such that K_0 has transcendence degree 1 over E and such that E is algebraically closed in K_0. Since K_0 has characteristic zero and E is algebraically closed in K_0, K_0 is a regular extension of E, and so $R := K_0 \otimes_E \bar{E}$ is an integral domain. Then the field of fractions of R is the field of regular functions of a smooth projective curve X over $\bar{E}$. Now let $g_1, \ldots, g_d, g_{d+1}, \ldots, g_m$ be generators for G so that $g_1, \ldots, g_d$ generate a free abelian group and $g_{d+1}, \ldots, g_m$ are roots of unity and let $\{p_1, \ldots, p_\ell\} \in X$ denote the collection of points at which some element from $g_1, \ldots, g_d$ has a zero or a pole. Then there are integers $b_{i,j}$ such that

$$\mathrm{div}(g_i) = \sum b_{i,j}[p_j]$$

for $i = 1, \ldots, d$. Now we have $a_n = g_1^{e_1(n)} \cdots g_m^{e_m(n)}$ and so

$$\mathrm{div}(a_n) = \sum_{j=1}^{\ell} \left(\sum_{i=1}^{d} b_{i,j} e_i(n) \right) [p_j].$$

In particular, by Lemma 3.5.3,

$$\sum_{i=1}^{d} b_{i,j} e_i(n) = \mathrm{O}(n)$$

and since the left-hand side satisfies a linear recurrence, we have that it is piecewise linear in the sense of having the form $A + Bn$ on progressions of a fixed gap [BNZ, Proposition 3.6]. It then follows that there exist some $r \geq 1$ and some fixed $h_0, \ldots, h_{r-1} \in K_0^\times$ such that for $j \in \{0, \ldots, r-1\}$, $a_{r(n+1)+j}/a_{rn+j} = C_{j,n} h_j$, where $C_{j,n} \in E^\times$. It follows that for $a_{rn+j} = C_{j,n} h_j^n P_j$, where $P_j \in K_0$ is constant. Then since the series $\sum P_j^{-1} h_n^{-n} x^n$ is D-finite and since D-finite series are closed under Hadamard product,

$$G_j(x) := \sum C_{j,n} x^n \in \bar{E}[[x]]$$

is D-finite and takes values in a finitely generated multiplicative group. Thus $G_j(x)$ is rational and then it is straightforward to show that

$$F_j(x) := \sum a_{rn+j} x^n = \sum C_{j,n} P_j h_j^n x^n$$

must also be rational and thus $F(x) = \sum_{j=0}^{r-1} x^j F_j(x^r)$ is also rational, as required. □

Bibliography

[AW] L. N. Argabright and C. O. Wilde, *Semigroups Satisfying a Strong Følner Condition. Proceedings of the American Mathematical Society*, Vol. **18**, No. 4 (Aug., 1967), pp.587–591.

[Bell] J. P. Bell, *A generalised Skolem-Mahler-Lech theorem for affine varieties.* J. London Math. Soc. (2) 73 (2006), no. 2, 367—379.

[Ber] J. Bertrand, *Mémoire sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme. Journal de l'Ecole Royale Polytechnique*, Cahier **30**, Vol. 18 (1845), 123–140.

[Berg03] V. Bergelson, *Minimal idempotents and ergodic Ramsey theory.* Topics in dynamics and ergodic theory, 8–39, *London Math. Soc. Lecture Note Ser.*, **310**, Cambridge Univ. Press, Cambridge, 2003.

[Berg00] V. Bergelson, *The multifarious Poincaré recurrence theorem.* Descriptive set theory and dynamical systems (Marseille-Luminy, 1996), 31–57, *London Math. Soc. Lecture Note Ser.*, **277**, Cambridge Univ. Press, Cambridge, 2000.

[BGS] J. P. Bell, D. Ghioca, and M. Satriano, *Dynamical uniform bounds for fibers and a gap conjecture.* To appear in *Int. Math. Res. Not. IMRN*, DOI: https://doi.org/10.1093/imrn/rnz257, 2019.

[BGT15] J. P. Bell, D. Ghioca, and T. J. Tucker, The dynamical Mordell–Lang problem for Noetherian spaces. *Funct. Approx. Comment. Math.* **53** (2015), no. 2, 313–328.

[BGT16] J. P. Bell, D. Ghioca, and T. J. Tucker, *The Dynamical Mordell–Lang Conjecture.* Mathematical Surveys and Monographs, vol. 210, American Mathematical Society, Providence, RI, 2016.

[BGT10] J. P. Bell, D. Ghioca, and T. J. Tucker, *The dynamical Mordell-Lang problem for étale maps. Amer. J. Math.* **132** (2010), no. 6, 1655–1675.

[BHS] J. P. Bell, F. Hu, and M. Satriano, *Height gap conjectures, D-finiteness, and weak dynamical Mordell-Lang.* Preprint available on arXiv, arXiv:2003.01255.

[BNZ] J. P. Bell, K. D. Nguyen, and U. Zannier, D-finiteness, rationality, and height. To appear in *Trans. Amer. Math. Soc.*, DOI: https://doi.org/10.1090/tran/8046, 2019.

[BOSS] A. Bérczes, A. Ostafe, I. Shparlinski, and J. H. Silverman, *Multiplicative dependence among iterated values of rational functions modulo finitely generated groups.* To appear in *Int. Math. Res. Not. IMRN*, DOI: https://doi.org/10.1093/imrn/rnz091, 2019.

[Béz86] J.-P. Bézivin, *Sur un théorème de G. Pólya. J. Reine Angew. Math.* **364** (1986), 60–68.

[Béz89] J.-P. Bézivin, Une généralisation du théorme de Skolem-Mahler-Lech. *Quart. J. Math. Oxford Ser.* (2) **40** (1989), 133–138.

[BG06] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry.* New Mathematical Monographs, vol. 4, Cambridge University Press, Cambridge, 2006.

[BNZ99] E. Bombieri, D. Masser, U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups. Internat. Math. Res. Notices* no. **20** (1999) 1119–1140.

[BNZ06] E. Bombieri, D. Masser, U. Zannier, *Intersecting curves and algebraic subgroups: conjectures and more results. Trans. Amer. Math. Soc.* **358** (2006), no. 5, 2247–2257.

[BNZ08] E. Bombieri, D. Masser, U. Zannier, *Intersecting a plane with algebraic subgroups of multiplicative groups. Ann. Sc. Norm. Super. Pisa Cl. Sci.* (5) **7** (2008), no. 1, 51–80.

[Che52] P. Chebyshev, *Mémoire sur les nombres premiers.* Journal de mathématiques pures et appliquées, Sér. **1** (1852), 366-390.

[Den94] L. Denis, *Géométrie et suites récurrentes. Bull. Soc. Math. France* **122** (1994), 13–27.

[DHRS18] T. Dreyfus, C. Hardouin, Charlotte, J. Roques, and M. Singer, *On the nature of the generating series of walks in the quarter plane. Invent. Math.* **213** (2018), no. 1, 139–203.

[Ell] R. Ellis, Distal transformation groups. *Pacific J. Math.* **8** (1958), 401–405.

[Eis95] D. Eisenbud, *Commutative Algebra. With a View toward Algebraic Geometry.* Graduate Texts in Mathematics, **150**. Springer-Verlag, New York, 1995.

[ESS02] J.-H. Evertse, H. P. Schlickewei, and W. M. Schmidt, Linear equations in variables which lie in a multiplicative group. *Ann. of Math.* (2) **155** (2002), 807–836.

[Fal] G. Faltings, The general case of S. Lang's conjecture. *Barsotti Symposium in Algebraic Geometry* (Abano Terme, 1991), 175–182.

[Fur79] H. Furstenberg, Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *J. Analyse Math.* **31** (1977), 204–256.

[Fur81] H. Furstenberg, Recurrence in ergodic theory and combinatorial number theory. *M. B. Porter Lectures.* Princeton University Press, Princeton, N.J., 1981.

[Gar09] S. Garoufalidis, G-functions and multisum versus holonomic sequences. *Adv. Math.* **220** (2009), no. 6, 1945–1955.

[GP17] S. Garrabrant and I. Pak, Words in linear groups, random walks, automata and P-recursiveness. *J. Comb. Algebra* **1** (2017), 127–144.

[GN17] D. Ghioca and K. Nguyen, The orbit intersection problem for linear spaces and semiabelian varieties. *Math. Res. Lett.* **24** (2017), no. 5, 1263–1283.

[GK] R. D. Gray and M. Kambites. Amenability and geometry of semigroups. *Trans. Amer. Math. Soc.* **369** (2017), no. 11, 8087–8103.

[GT] D. Ghioca and T. Tucker, Periodic points, linearizing maps, and the dynamical Mordell-Lang problem. *J. Number Theory* **129** (2009), no. 6, 1392—1403.

[Gig14] W. Gignac, Measures and dynamics on Noetherian spaces. *J. Geom. Anal.* **24** (2014), no. 4, 1770–1793.

[GoTs13] G. Golan and B. Tsaban, Hindman's coloring theorem in arbitrary semigroups. *Journal of Algebra* **395** (2013), 111-120.

[Had] J. Hadamard, Sur la distribution des zéros de la fonction zeta(s) et ses conséquences arithmétiques. *Bull. Soc. math. France* **24**, 199-220, 1896.

[Har77] R. Hartshorne, *Algebraic Geometry.* Graduate Texts in Mathematics **52**, Springer-Verlag, New York-Heidelberg, 1977.

[Lau84] M. Laurent, Équations diophantiennes exponentielles. *Invent. Math.* **78** (1984), 299–327.

[Hin74] N. Hindman, Finite sums from sequences within cells of a partition of N. *J. Combinatorial Theory Ser. A* **17** (1974), 1–11.

[HS] N. Hindman, D. Strauss, Algebra in the Stone-Cech compactification. Theory and applications. De Gruyter Textbook. Walter de Gruyter & Co., Berlin, 2012. xviii+591 pp. ISBN: 978-3-11-025623-9

[Ivan] S. V. Ivanon, Group rings of Noetherian groups. *Translation in Math. Notes* **46** (1989), no. 5-6, 929–933 (1990).

[Lec53] C. Lech, A note on recurring series. *Ark. Mat.* **2** (1953), 417–421.

[Lip88] L. Lipshitz, The diagonal of a D-finite power series is D-finite. *J. Algebra* **113** (1988), no. 2, 373–378.

[Mal] A. L. Malcev, On certain classes of infinite solvable groups. *Amer. Math. Soc. Transl.* **(2) 2** (1956), 1–21.

[Mann] A. Mann, How Groups Grow. *London Mathematical Society Lecture Note Series*, **395**. Cambridge University Press, Cambridge, 2012.

[Met00] C. Methfessel, On the zeros of recurrence sequences with non-constant coefficients. *Arch. Math. (Basel)* **74** (2000), 201–206.

[Mis20] M. Mishna, *Analytic Combinatorics: A Multidimensional Approach.* Discrete Mathematics and Its Applications, CRC Press, 2020.

[Nam] I. Namioka, Følner's conditions for amenable semi-groups. *Math. Scand.* **15** (1964), 18–28.

[Num] K. Numakura, On bicompact semigroups. *Math. J. Okayama Univ.* **1** (1952), 99–108.

[OSSZ19] A. Ostafe, M. Sha, I. Shparlinski, and U. Zannier, On multiplicative dependence of values of rational functions and a generalization of the Northcott theorem. *Michigan Math. J.* **68** (2019), no. 2, 385–407.

[Pak18] I. Pak, Complexity problems in enumerative combinatorics. In *Proc. ICM Rio de Janeiro*, Volume 3(2018), 3319–3166.

[Pet15] C. Petsche, On the distribution of orbits in affine varieties. *Ergodic Theory Dynam. Systems* **35** (2015), no. 7, 2231–2241.

[Pól21] G. Pólya, Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen. *J. Reine Angew. Math.* **151** (1921), 1–31.

[Roq57] P. Roquette, Einheiten und Divisorklassen in endlich erzeugbaren Körpern. *Jber. Deutsch. Math.-Verein.* **60** (1957), no. Abt., Abt. 1, 1–21.

[Sil07] J. H. Silverman, *The Arithmetic of Dynamical Systems.* Graduate Texts in Mathematics, vol. 241, Springer, New York, 2007.

[Sal17] B. Salvy, Linear differential equations as a data structure. *Found. Comput. Math* 19 (2019), 1071¨C1112.

[Sta80] R. P. Stanley, Differentiably finite power series. *European J. Combin.* **1** (1980), no. 2, 175–188.

[Sta12] R. P. Stanley. *Enumerative combinatorics. Volume 1.* Second edition. Cambridge Studies in Advanced Mathematics, 49. Cambridge University Press, Cambridge, 2012.

[Sta96] R. P. Stanley. *Enumerative Combinatorics. Vol. 2.* Cambridge Studies in Advanced Mathematics, 62. Cambridge University Press, Cambridge, 1999.

[Ste] B. Steinberg (https://mathoverflow.net/users/15934/benjamin-steinberg), Are semigroups with finite-to-one right multiplication "moving"?, URL (version: 2014-05-02): https://mathoverflow.net/q/164429

[Swan] R. G. Swan, Representations of polycyclic groups. *Proc. Amer. Math. Soc.* **18** (1967), 573–574.

[Sze75] E. Szemerédi, On sets of integers containing k elements in arithmetic progression. *Acta Arith.* **27** (1975), no 1, 199–245.

[WZ92] H. S. Wilf and D. Zeilberger, An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities. *Invent. Math.* **108** (1992), no. 3, 575–633.

[Xie] J. Xie, The dynamical Mordell-Lang conjecture for polynomial endomorphisms of the affine plane. *Astérisque* No. **394** (2017), vi+110 pp. ISBN: 978-2-85629-869-5.

[Za69] H. Zassenhaus, On linear noetherian groups. *J. Number Theory* **1** (1969), 70–89.