EXPANSIVE DYNAMICS ON PROFINITE GROUPS

MICHAEL WIBMER

Abstract. A profinite group equipped with an expansive endomorphism is equivalent to a one-sided group shift. We show that these groups have a very restricted structure. More precisely, we show that any such group can be decomposed into a finite sequence of full one-sided group shifts and two finite groups.

1. Introduction

An endomorphism $\sigma\colon G \to G$ of a profinite group G is *expansive* if there exists an open subgroup U of G with $\bigcap_{n\in\mathbb{N}} \sigma^{-n}(U) = 1$. There are two obvious examples: A (discrete) finite group with an arbitrary endomorphism (choose $U = 1$) and a full one-sided group shift on a finite group $\mathcal{G}$, i.e., $G = \mathcal{G}^{\mathbb{N}}$ with $\sigma(g_0, g_1, \ldots) = (g_1, g_2, \ldots)$ (choose $U = 1 \times \mathcal{G} \times \mathcal{G} \times \ldots$). Our main result shows that any profinite group with an expansive endomorphism is build up from these two examples. More precisely, we have (Theorem 4.6):

Theorem A. *Let G be a profinite group equipped with an expansive endomorphism σ. Then there exists a subnormal series*

$$G \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n$$

of closed σ-stable subgroups G_i of G such that

- *G_i/G_{i+1} is isomorphic to a full one-sided group shift on a finite simple group $\mathcal{G}_i$ for $i = 1, \ldots, n-1$,*
- *G/G_1 is a finite group and $\sigma\colon G/G_1 \to G/G_1$ is an automorphism,*
- *G_n is a finite group and some power of $\sigma\colon G_n \to G_n$ is the trivial endomorphism $g \mapsto 1$.*

Moreover, the length n of such a series, the group G_1 and the isomorphism classes of the finite simple groups $\mathcal{G}_i$ are uniquely determined by G.

A continuous map $\sigma\colon X \to X$ on a metric space (X, d) is *expansive* if there exists an $\varepsilon > 0$ such that for any two distinct points $x, y \in X$ there is an $n \in \mathbb{N}$ with $d(\sigma^n(x), \sigma^n(y)) > \varepsilon$. In the context of a continuous group homomorphism $\sigma\colon G \to G$ on a topological group G, this condition translates to the existence of a neighborhood U of 1 such that for any two distinct $g, h \in G$ there is an $n \in \mathbb{N}$ with $\sigma^n(g) \notin \sigma^n(h)U$, or equivalently, $h^{-1}g \notin \sigma^{-n}(U)$. Thus, σ is expansive if and only if there is a neighborhood U of 1 with $\bigcap_{n\in\mathbb{N}} \sigma^{-n}(U) = 1$. Similarly, an *automorphism* σ of a topological group is an *expansive automorphism* if there exists a neighborhood U of 1 such that $\bigcap_{n\in\mathbb{Z}} \sigma^{-n}(U) = 1$.

Expansive automorphisms of topological groups have been studied extensively under varying restrictions on the group (e.g., profinite, compact or locally compact). See [Kit87], [Fag96], [KS89], [BS08], [GR17], [Sha20], [Sch95, Chapter 3] and the references given there.

Date: August 4, 2020.

2010 *Mathematics Subject Classification.* 37B10, 37B05, 22C05, 20E18, 12H10.

Key words and phrases. Symbolic dynamics, group shift, Markov subgroup, expansive automorphism, expansive dynamical system, Babbitt's decomposition.

This work was supported by the NSF grants DMS-1760212, DMS-1760413, DMS-1760448 and the Lise Meitner grant M 2582-N32 of the Austrian Science Fund FWF.

A fundamental result, concerning expansive automorphisms of profinite groups, due to B. Kitchens (see [Kit87] or [Kit98, Section 6.3]), is that any such group is topologically conjugate to a direct product of a finite set equipped with a bijection and a full two-sided shift. See [BS08] for a discussion of higher dimensional analogs and [Sob07] for a generalization to quasi-groups.

In this article, we also establish a one-sided analog of Kitchens' result (Theorem 5.2): If G is a profinite group equipped with an expansive endomorphism $\sigma\colon G \to G$, then there exists an integer $n \geq 0$ such that $\sigma^n(G)$ is topologically conjugate to a finite set equipped with a bijection and a full one-sided shift.

Despite its beautiful simplicity, Kitchens' result is not fully satisfactory since the topological conjugacy in general does not respect the group structure. In fact, it appears that the problem, set forth by Kitchens in [Kit87], to classify all expansive automorphisms of profinite groups up to isomorphism is still wide open.

We also establish a version of Theorem A for expansive automorphisms (Theorem 6.13), i.e., a two-sided version. The statement is very similar. The only significant difference is that the group G_n does not occur in the two-sided version. One can think of our two-sided version of Theorem A as a variant of Kitchens' result that respects the group structure. It reduces the problem of classifying all expansive automorphisms of profinite groups to the study of the group extension problem for profinite groups with an expansive automorphism. This is somewhat similar to how the Jordan-Hölder theorem reduces the study of finite groups to the study of finite simple groups and the group extension problem for finite groups. Our proof of the uniqueness part of Theorem A is actually modeled on the proof of the Jordan-Hölder theorem.

There is no direct connection between profinite groups equipped with an expansive endomorphism and profinite groups equipped with an expansive automorphism. Indeed, if G is a profinite group and $\sigma\colon G \to G$ is a map that is simultaneously an expansive endomorphism and an expansive automorphism, then G must be finite (Corollary 3.17). However, there is a universal construction $G \rightsquigarrow G^*$ that associates to any profinite group G equipped with an expansive endomorphism, a profinite group G^* equipped with an expansive automorphism. We use this universal construction to deduce the two-sided version of Theorem A from Theorem A.

We also present an application of Theorem A to difference algebra. Babbitt's decomposition theorem ([Lev08, Theorem 5.4.13]) is an important classical theorem in difference algebra that elucidates the structure of Galois extensions of difference fields. Here a difference field is a field equipped with an endomorphism. The connection to expansive endomorphisms is that the Galois group of an extension of difference fields is naturally a profinite group equipped with an endomorphism. If the extension of difference fields is finitely generated, then the endomorphism on the Galois group is expansive. Indeed, one can think of Theorem A as a group version of Babbitt's decomposition theorem. Based on Theorem A, we present a new proof of Babbitt's decomposition theorem that yields additional information concerning the uniqueness of the decomposition (Theorem 7.5).

A certain connection between difference algebra and symbolic dynamics, to be detailed in a forthcoming paper, was discovered by Ivan Tomašić. While we do not use or even explain this connection here, this paper would not have happened without it and the author is grateful to Ivan Tomašić for sharing his discovery. In the light of this connection, the results of this article could also be interpreted as results about a certain class of affine difference algebraic groups.

We conclude this introduction with an overview of the article: In Section 2 we discuss one-sided group shifts and show that they are always of finite type. In Section 3 we first explain the equivalence of categories between the category of one-sided group shifts and the category of profinite groups equipped with an expansive endomorphism. We then study the latter category in more detail. In particular, we discuss quotients and analogs of the isomorphism theorems and the Schreier refinement theorem. We also introduce the σ-identity component that has properties somewhat similar to the identity component of an algebraic group. Section 4 contains

the technical heart of the paper and establishes Theorem A. In Section 5 the one-sided analog of Kitchens' result is proved. Then the two-sided version of Theorem A is established in Section 6. Finally, Section 7 contains the application to Babbitt's decomposition theorem.

2. One-sided group shifts

In this section we provide some basic results concerning one-sided group shifts. In particular, we show that every one-sided group shift is of finite type. We begin by fixing the notation and recalling some basic definitions from symbolic dynamics. See [Kit98] or [LM95]. As general conventions, the set $\mathbb{N}$ of natural numbers contains zero and a subset Y of a set X equipped with a map $\sigma\colon X \to X$ is *σ-stable* if $\sigma(Y) \subseteq Y$.

Let $\mathcal{A}$ be a finite set. We consider $\mathcal{A}^{\mathbb{N}}$ as a topological space via the product topology of the discrete topology on $\mathcal{A}$. The topological space $\mathcal{A}^{\mathbb{N}}$ together with the continuous map $\sigma\colon \mathcal{A}^{\mathbb{N}} \to \mathcal{A}^{\mathbb{N}}$, given by $\sigma(a_0, a_1, \ldots) = (a_1, a_2, \ldots)$ is the *full one-sided shift* on the alphabet $\mathcal{A}$. A *one-sided shift space* or *one-sided shift* on $\mathcal{A}$ is a closed subset X of $\mathcal{A}^{\mathbb{N}}$ such that $\sigma(X) \subseteq X$. A morphism between two one-sided shifts X and Y (possibly on different alphabets) is a continuous map $\phi\colon X \to Y$ such that

$$\begin{array}{ccc} X & \xrightarrow{\phi} & Y \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ X & \xrightarrow{\phi} & Y \end{array}$$

commutes. A *word* or *block* of length i is a sequence of i elements from $\mathcal{A}$. A one-sided shift X on $\mathcal{A}$ is a (one-sided) *subshift of finite type* if there exists a finite set $\mathcal{F}$ of blocks such that X consists of all elements of $\mathcal{A}^{\mathbb{N}}$ that do not contain any blocks from $\mathcal{F}$.

An important class of subshifts of finite type is formed by those coming from directed graphs, also called 1-step subshifts of finite type. Let Γ be a directed graph with set of vertices equal to $\mathcal{A}$. Then the set $X_\Gamma \subseteq \mathcal{A}^{\mathbb{N}}$ of all sequences in $\mathcal{A}$ that trace out the vertices of an infinite directed path in Γ, is a subshift of finite type.

The *topological entropy* of a one-sided shift X on $\mathcal{A}$ is

$$h(X) = \lim_{i\to\infty} \frac{\log(d_i)}{i},$$

where d_i denotes the cardinality of the image of $X \to \mathcal{A}^i,\ (a_0, a_1, \ldots) \mapsto (a_0, a_1, \ldots, a_{i-1})$, i.e., the cardinality of all blocks of length i that occur in elements of X.

In this article, we are mainly interested in the situation when the alphabet is a finite group. If $\mathcal{G}$ is a finite group, then $\mathcal{G}^{\mathbb{N}}$ inherits a group structure via componentwise multiplication. Indeed $\mathcal{G}^{\mathbb{N}}$ is a profinite group and $\sigma\colon \mathcal{G}^{\mathbb{N}} \to \mathcal{G}^{\mathbb{N}}$ is a continuous group homomorphism. In this situation, the pair $(\mathcal{G}^{\mathbb{N}}, \sigma)$ is called the *full one-sided group shift* on $\mathcal{G}$. A *one-sided group shift* G on $\mathcal{G}$ is a one-sided shift on $\mathcal{G}$ such that G is a subgroup of $\mathcal{G}^{\mathbb{N}}$. A morphism between two one-sided group shifts is a morphism between one-sided shifts that is a group homomorphism. We note that (in the two-sided context) group shifts are called Markov subgroups in [Kit98, Section 6.3]. Here we follow the nomenclature from [LM95] and [BS08].

Let G be a one-sided group shift on the finite group $\mathcal{G}$. The following notation will be useful: For $i \in \mathbb{N}$, let $G[i]$ denote the image of the group homomorphism $G \to \mathcal{G}^{i+1},\ (g_0, g_1, \ldots) \mapsto (g_0, g_1, \ldots, g_i)$. Then $G[i]$ is the subgroup of $\mathcal{G}^{i+1}$ consisting of all blocks of length $i+1$ that occur in elements of G. For $i \geq 1$, the map

$$\pi_i\colon G[i] \to G[i-1],\ (g_0, \ldots, g_i) \mapsto (g_0, \ldots, g_{i-1})$$

is a surjective group homomorphism.

Every two-sided group shift is a subshift of finite type ([Kit98, Section 6.3]). As we now show, a similar result holds for one-sided group shifts. The proof has some important consequences.

Proposition 2.1. *Every one-sided group shift is a subshift of finite type.*

Proof. Let $\mathcal{G}$ be a finite group and $G \leq \mathcal{G}^{\mathbb{N}}$ a one-sided group shift on $\mathcal{G}$. Set $\mathcal{G}_0 = G[0]$ and for $i \geq 1$, let $\mathcal{G}_i \subseteq \mathcal{G}$ denote the follower set of $(1, \ldots, 1) \in \mathcal{G}^i$, i.e., $\ker(\pi_i) = \{(1, \ldots, 1, g) \in \mathcal{G}^{i+1} |\ g \in \mathcal{G}_i\}$. So $\mathcal{G}_i$ is a subgroup of $\mathcal{G}$. As G is stable under the shift map $\sigma\colon \mathcal{G}^{\mathbb{N}} \to \mathcal{G}^{\mathbb{N}}$, we also have group homomorphisms $\sigma_i\colon G[i] \to G[i-1]$, $(g_0, \ldots, g_i) \mapsto (g_1, \ldots, g_i)$. Since σ_i maps $\ker(\pi_i)$ injectively into $\ker(\pi_{i-1})$, we see that $\mathcal{G}_{i-1} \subseteq \mathcal{G}_i$. We thus have a descending chain $\mathcal{G}_0 \supseteq \mathcal{G}_1 \supseteq \mathcal{G}_2 \supseteq \ldots$ of subgroups of $\mathcal{G}$ that must eventually stabilize. Let $\mathcal{G}' = \bigcap_{i \in \mathbb{N}} \mathcal{G}_i$ denote the eventual value and let $n \in \mathbb{N}$ be minimal with the property that $\mathcal{G}_i = \mathcal{G}'$ for all $i \geq n$. Set $\mathcal{H} = G[n]$ and let $G' \subseteq \mathcal{G}^{\mathbb{N}}$ denote the subshift of finite type that avoids all blocks from $\mathcal{F} = G[n] \setminus \mathcal{H}$. In other words, G' is the subgroup of $\mathcal{G}^{\mathbb{N}}$ consisting of all elements that have all their blocks of length $n+1$ inside $\mathcal{H}$. By construction $G \subseteq G'$.

We claim that $G = G'$. We have $G[i] \leq G'[i]$ for $i \in \mathbb{N}$. To show that $G = G'$ it suffices to show that $G[i] = G'[i]$ for $i \in \mathbb{N}$. This is clear for $i = 0, \ldots, n$ and we will prove the general case by induction on i. So we assume that $i \geq n$ and that $G[i] = G'[i]$. We have to show that $G[i+1] = G'[i+1]$. There is a commutative diagram

$$\begin{array}{ccc} G[i+1] & \hookrightarrow & G'[i+1] \\ \downarrow{\scriptstyle \pi_{i+1}} & & \downarrow{\scriptstyle \pi'_{i+1}} \\ G[i] & = & G'[i] \end{array}$$

where the vertical maps π_{i+1} and π'_{i+1} are the surjective group homomorphisms given by projection onto the first $i+1$ coordinates. It suffices to show that $\ker(\pi_{i+1}) = \ker(\pi'_{i+1})$. Clearly $\ker(\pi_{i+1}) \subseteq \ker(\pi'_{i+1})$. Moreover, $\ker(\pi_{i+1}) = \{1\}^{i+1} \times \mathcal{G}' \leq \mathcal{G}^{i+2}$ since $i+1 \geq n$. Let $h = (1, \ldots, 1, g) \in \ker(\pi'_{i+1}) \leq \mathcal{G}^{i+2}$. By definition of G', the element $(1, \ldots, 1, g) \in \mathcal{G}^{n+1}$ lies in $\mathcal{H} = G[n]$ and so it lies in the kernel of $\pi_n\colon \mathcal{H} = G[n] \to G[n-1]$. We conclude that $g \in \mathcal{G}'$ and $h \in \ker(\pi_{i+1})$ as desired. □

Corollary 2.2. *Let G be a one-sided group shift. Then $h(G) = \log(d)$ for some integer $d \geq 1$.*

Proof. We use the notation of the proof of Proposition 2.1 and furthermore set $d = |\mathcal{G}'|$. For $i \geq 1$ we have $|G[i]| = |G[i-1]| \cdot |\mathcal{G}_i|$ and so inductively,

$$|G[i]| = |\mathcal{G}_0| \cdot |\mathcal{G}_1| \ldots |\mathcal{G}_i| = |\mathcal{G}_0| \ldots |\mathcal{G}_{n-1}| \cdot |\mathcal{G}_n|^{i-n+1} = |\mathcal{G}_0| \ldots |\mathcal{G}_{n-1}| \cdot d^{i-n+1}$$

for $i \geq n$. Thus

$$h(G) = \lim_{i \to \infty} \frac{\log |G[i]|}{i+1} = \lim_{i \to \infty} \frac{\log(|\mathcal{G}_0| \ldots |\mathcal{G}_{n-1}| \cdot d^{-n})}{i+1} + \lim_{i \to \infty} \frac{\log(d^{i+1})}{i+1} = \log(d).$$

□

Definition 2.3. *Let $G \leq \mathcal{G}^{\mathbb{N}}$ be a one-sided group shift on the finite group $\mathcal{G}$ and $n \geq 1$. Then G is an* n-step group shift of finite type *if there exists a subgroup $\mathcal{H}$ of $\mathcal{G}^{n+1}$ such that G consists of exactly those elements of $\mathcal{G}^{\mathbb{N}}$ that have all blocks of length $n+1$ inside $\mathcal{H}$.*

The following corollary is immediate from the proof of Proposition 2.1.

Corollary 2.4. *Every one-sided group shift is an n-step group shift of finite type for some $n \geq 1$.* □

1-step subshifts of finite type are described by directed graphs. The following definition provides a group version of this well-known fact.

Definition 2.5. *Let $\mathcal{G}$ be a finite group. A* directed group graph *on $\mathcal{G}$ is a directed graph Γ such that the set of vertices of Γ equals $\mathcal{G}$ and such that the set of directed edges of Γ is a subgroup of $\mathcal{G} \times \mathcal{G}$.*

For a directed group graph Γ on $\mathcal{G}$ let

$$G_\Gamma = X_\Gamma \subseteq \mathcal{G}^{\mathbb{N}}$$

denote the subshift of finite type defined by Γ. Then G_Γ is a 1-step group shift of finite type. Conversely, every 1-step group shift $G \subseteq \mathcal{G}^{\mathbb{N}}$ is of the form $G = G_\Gamma$ for some directed group graph Γ.

In a directed group graph the set of directed edges is a group. The same is true for the set of directed paths of a fixed length (finite or infinite): Two directed paths are multiplied by multiplying the vertices and the directed edges. We will see later (Lemma 3.16) that every one-sided group shift is isomorphic to some G_Γ.

3. Expansive profinite groups

If G is a one-sided group shift, then G is a profinite group and $\sigma\colon G \to G$ is an expansive endomorphism. Conversely, we will see that every profinite group with an expansive endomorphism is isomorphic to a one-sided group shift. It is sometimes beneficial to work inside this larger category of expansive profinite groups. For example, if G and N are one-sided group shifts on a finite group $\mathcal{G}$ such that N is a normal subgroup of G, then the quotient G/N is not a one-sided group shift on the nose as there is no canonical choice of the alphabet for G/N. On the other hand, it is clear that G/N is a profinite group equipped with an endomorphism (which can be shown to be expansive).

In this section we provide some basic definitions and results concerning expansive profinite groups that will then be used in the next section to establish the main decomposition theorem (Theorem 4.6). In particular, we define the σ-identity component and the limit degree of an expansive profinite group.

3.1. **Expansive profinite groups versus one-sided group shifts.** Let G be a profinite group. A continuous group homomorphism $\sigma\colon G \to G$ is called an *expansive endomorphism* if there exists a neighborhood U of $1 \in G$ such that $\bigcap_{n\in\mathbb{N}} \sigma^{-n}(U) = 1$. Since the open normal subgroups of G are a neighborhood basis for 1 ([RZ10, Theorem 2.1.3]), we can assume that U is an open normal subgroup of G.

Definition 3.1. *An* expansive profinite group *is a profinite group G together with an expansive endomorphism $\sigma\colon G \to G$.*

We will usually omit σ from the notation and simply refer to G as an expansive profinite group. A morphism between expansive profinite groups G and H is a continuous group homomorphism $\phi\colon G \to H$ such that

$$\begin{array}{ccc} G & \xrightarrow{\phi} & H \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ G & \xrightarrow{\phi} & H \end{array}$$

commutes.

Example 3.2. Let $G \leq \mathcal{G}^{\mathbb{N}}$ be a one-sided group shift on the finite group $\mathcal{G}$. Then G is an expansive profinite group. Indeed, we can choose $U = \{(g_0, g_1, \ldots) \in G |\ g_0 = 1\}$.

See Lemma 7.1 for an explanation how expansive profinite groups naturally occur in the study of Galois extensions of difference fields. The following lemma provides a converse to Example 3.2.

Lemma 3.3. *Every expansive profinite group is isomorphic to a one-sided group shift.*

Proof. Let G be an expansive profinite group and let U be an open normal subgroup of G such that $\bigcap_{n\in\mathbb{N}} \sigma^{-n}(U) = 1$. Then $\mathcal{G} = G/U$ is a finite group and

$$\phi\colon G \to \mathcal{G}^{\mathbb{N}},\ g \mapsto (g, \sigma(g), \sigma^2(g), \ldots)$$

is a group homomorphism that commutes with σ. It is injective because $\bigcap_{n\in\mathbb{N}} \sigma^{-n}(U) = 1$.

The inverse image of a basic open subset

$$V = V(h_0, \ldots, h_n) = \{(g_0, g_1, \ldots) \in \mathcal{G}^{\mathbb{N}} |\ g_0 = h_0, \ldots, g_n = h_n\}$$

of $\mathcal{G}^{\mathbb{N}}$, where $h_1, \ldots, h_n \in \mathcal{G}$ are U-cosets in G, equals $h_0 \cap \sigma^{-1}(h_1) \cap \ldots \cap \sigma^{-n}(h_n)$, which is open G. Thus ϕ is continuous.

A continuous group homomorphism between profinite groups is closed ([FJ08, Remark 1.2.1 (e)]). In particular, $\phi(G) \subseteq \mathcal{G}^{\mathbb{N}}$ is closed. As $\phi(G)$ is stable under σ, we see that $\phi(G)$ is a one-sided group shift. Because ϕ is closed it follows that $\phi\colon G \to \phi(G)$ is a homeomorphism and thus an isomorphism. □

From the above lemma and example we see that the concepts "expansive profinite group" and "one-sided group shift" are interchangeable. More precisely we have:

Corollary 3.4. *The category of one-sided group shifts is equivalent to the category of expansive profinite groups.*

Proof. Every one-sided group shift is an expansive profinite group (Example 3.2). Since in both categories the morphisms are defined in the same fashion, it suffices to know that every expansive profinite group is isomorphic to a one-sided group shift. This is exactly Lemma 3.3. □

We can thus think of expansive profinite groups as a "coordinate free" version of one-sided group shifts. One advantage of working with the larger category of expansive profinite groups is that certain constructions, such as quotients by normal closed σ-stable subgroups, are more naturally performed in this category.

3.2. **Group theory for expansive profinite groups.** The isomorphism theorems for abstract groups carry over without difficulty to the category of expansive profinite groups. The same holds for the Schreier refinement theorem, which will be the key for establishing the uniqueness in our main decomposition theorem (Theorem 4.6).

The following lemma shows that subgroups and quotients of expansive profinite groups are well-behaved.

Lemma 3.5. *Let G be an expansive profinite group.*

(i) *If H is a closed σ-stable subgroup of G, then H (with the induced topology and endomorphism) is an expansive profinite group.*

(ii) *If N is a normal closed σ-stable subgroup of G, then G/N (with the quotient topology and induced endomorphism) is an expansive profinite group and the canonical map $G \to G/N$ is a morphism of expansive profinite groups.*

Proof. A closed subgroup of a profinite group is a profinite group ([RZ10, Proposition 2.2.1]). If U is an open subgroup of G such that $\bigcap_{n\in\mathbb{N}} \sigma^{-n}(U) = 1$, then $U' = H \cap U$ is an open subgroup of H and $\bigcap_{n\in\mathbb{N}} \sigma'^{-n}(U') = 1$, where $\sigma'\colon H \to H$ is the restriction of $\sigma\colon G \to G$. This proves (i).

The quotient of a profinite group by a closed normal subgroup is a profinite group ([RZ10, Proposition 2.2.1]). Because $\sigma(N) \subseteq N$ we have a well-defined continuous group homomorphism $\overline{\sigma}\colon G/N \to G/N,\ gN \mapsto \sigma(g)N$.

To show that $\overline{\sigma}$ is expansive, we may assume that G is a one-sided group shift on a finite group $\mathcal{G}$ (Lemma 3.3). Then, it follows from Corollary 2.4 that $N \leq \mathcal{G}^{\mathbb{N}}$ is an n-step group shift of finite type for some $n \geq 1$. Note that because N is normal in G, $N[i]$ is normal in $G[i]$ for every $i \in \mathbb{N}$. In particular, $N[n]$ is normal in $G[n]$. Set $\mathcal{H} = G[n]/N[n]$ and

$\phi\colon G \to \mathcal{H}^{\mathbb{N}}$, $(g_0, g_1, \ldots) \mapsto (\overline{(g_i, g_{i+1}, \ldots, g_{i+n})})_{i\in\mathbb{N}}$. Then ϕ is a morphism of expansive profinite groups with kernel N. Set $U = \phi^{-1}(1 \times \mathcal{H} \times \mathcal{H} \times \ldots)$ and $\overline{U} = U/N \subseteq G/N$. Then $\overline{U}$ is an open subgroup of G/N and if $g \in G$ is such that $\overline{g} \in \bigcap_{i\in\mathbb{N}} \overline{\sigma}^{-i}(\overline{U})$, i.e., $\sigma^i(g) \in U$ for all $i \in \mathbb{N}$, then $\sigma^i(\phi(g)) \in 1 \times \mathcal{H} \times \mathcal{H} \times \ldots$ for all i and thus $\phi(g) = (1, 1 \ldots)$. Therefore $g \in N$ and $\bigcap_{i\in\mathbb{N}} \overline{\sigma}^{-i}(\overline{U}) = 1$. □

Definition 3.6. *An* expansive subgroup *of an expansive profinite group is a closed σ-stable subgroup.*

By Lemma 3.5 (i) an expansive subgroup H of an expansive profinite group G is an expansive group in its own right. If H is normal in G we will speak of a normal expansive subgroup.

Proposition 3.7 (Isomorphism theorems for expansive profinite groups)**.**

(i) *Let $\phi\colon G \to H$ be a morphism of expansive profinite groups. Then $\phi(G)$ is an expansive subgroup of H, $\ker(\phi)$ is a normal expansive subgroup of G and the canonical map $G/\ker(\phi) \to \phi(G)$ is an isomorphism of expansive profinite groups.*

(ii) *Let N be a normal expansive subgroup of an expansive group G and $\pi\colon G \to G/N$ the canonical map. Then the map*

$$\{\text{expansive subgroups of } G \text{ containing } N\} \longrightarrow \{\text{expansive subgroups of } G/N\},$$

$H \mapsto \pi(H) = H/N$ is a bijection with inverse $H' \mapsto \pi^{-1}(H')$. Moreover H is normal in G if and only if H/N is normal in G/N and in that case $G/H \simeq (G/N)/(H/N)$.

(iii) *Let H and N be expansive subgroups of an expansive profinite group G such that H normalizes N. Then HN is an expansive subgroup of G, $H \cap N$ is a normal expansive subgroup of H and $HN/N \simeq H/H \cap N$.*

Proof. The isomorphism theorems hold for profinite groups. See e.g., [FJ08, Section 1.2]. (The key observation here is that any morphism of profinite groups is a closed map.) One immediately verifies that the relevant constructions are compatible with the endomorphism σ. □

Definition 3.8. *A* subnormal series *of an expansive profinite G is a sequence*

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = 1 \tag{1}$$

of expansive subgroups G_i of G such that G_{i+1} is a normal expansive subgroup of G_i for $i = 0, \ldots, n-1$. Another subnormal series

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_m = 1 \tag{2}$$

is a refinement *of (1) if $\{H_0, \ldots, H_m\} \subseteq \{G_0, \ldots, G_n\}$.*

Two subnormal series (1) and (2) are equivalent *if $m = n$ and there exists a permutation π such that G_i/G_{i+1} is isomorphic to $H_{\pi(i)}/H_{\pi(i)+1}$ for $i = 0, \ldots, n-1$.*

We will sometimes omit the first group $G = G_0$ and the last group $G_n = 1$ in our notations for a subnormal series for G.

Similarly to the isomorphism theorems, the Schreier refinement theorem carries over in a straight forward fashion from the category of abstract groups to the category of expansive profinite groups. For the sake of completeness we include a sketch of the proof (see e.g., [Rot95, Theorem 5.11]).

Lemma 3.9. *Let N_1, H_1, N_2, H_2 be expansive subgroups of an expansive profinite group such that N_i is a normal subgroup of H_i for $i = 1, 2$. Then $N_1(H_1 \cap N_2)$ is a normal expansive subgroup of $N_1(H_1 \cap H_2)$, $N_2(N_1 \cap H_2)$ is a normal expansive subgroup of $N_2(H_1 \cap H_2)$ and*

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \simeq \frac{N_2(H_1 \cap H_2)}{N_2(N_1 \cap H_2)}.$$

Proof. The statement about normality holds for abstract groups ([Rot95, Lemma 5.10]), so it also holds in our context. As $H_1 \cap H_2$ normalizes $N_1(H_1 \cap N_2)$ it follows from Proposition 3.7 (iii) that

$$\frac{(H_1 \cap H_2)N_1(H_1 \cap N_2)}{N_1(H_1 \cap N_2)} \simeq \frac{H_1 \cap H_2}{(H_1 \cap H_2) \cap N_1(H_1 \cap N_2)} \tag{3}$$

as expansive profinite groups. But $(H_1 \cap H_2)N_1(H_1 \cap N_2) = N_1(H_1 \cap H_2)$ and $(H_1 \cap H_2) \cap N_1(H_1 \cap N_2) = (H_1 \cap N_2)(N_1 \cap H_2)$. Thus (3) simplifies to

$$\frac{N_1(H_1 \cap H_2)}{N_1(H_1 \cap N_2)} \simeq \frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)}.$$

By symmetry (exchanging the indices 1 and 2) also

$$\frac{N_2(H_1 \cap H_2)}{N_2(N_1 \cap H_2)} \simeq \frac{H_1 \cap H_2}{(H_1 \cap N_2)(N_1 \cap H_2)}$$

and the claim follows. □

Proposition 3.10. *Any two subnormal series of an expansive profinite group have equivalent refinements.*

Proof. Let

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = 1 \tag{4}$$

and

$$G = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_m = 1 \tag{5}$$

be subnormal series for an expansive profinite group G. Setting $G_{i,j} = G_{i+1}(G_i \cap H_j)$ for $i = 0, \ldots, n-1$ and $j = 0, \ldots, m$ yields a refinement of (4). Similarly, setting $H_{j,i} = H_{j+1}(G_i \cap H_j)$ for $j = 0, \ldots, m-1$ and $i = 0, \ldots, n$ yields a refinement of (5). By Lemma 3.9 we have $G_{i,j}/G_{i,j+1} \simeq H_{j,i}/H_{j,i+1}$ and so the two refinements are equivalent. □

3.3. **The limit degree of an expansive profinite group.** The limit degree of an expansive profinite group is the topological entropy but conveniently transformed so that it always is an integer. It is a rough measure for the "seize" of an expansive profinite group. In this section we provide some basic properties of this numerical invariant. The main decomposition theorem (Theorem 4.6) will be proved by induction on the limit degree.

Definition 3.11. *Let G be an expansive profinite group. As the topological entropy of subshifts of finite type is invariant under isomorphism, we can define* $\mathrm{ld}(G)$*, the* limit degree *of G as* $\exp(h(G'))$*, where G' is any one-sided group shift isomorphic to G.*

Note that by Corollary 2.2 the limit degree is a positive integer. Moreover, it has the following interpretation:

Lemma 3.12. *Let G be a one-sided group shift on a finite group $\mathcal{G}$. Then the sequence $(|\ker(G[i] \xrightarrow{\pi_i} G[i-1])|)_{i \geq 1}$ is non-increasing and stabilizes with value $\mathrm{ld}(G)$. If n is the smallest integer such that $|\ker(G[i] \xrightarrow{\pi_i} G[i-1])| = \mathrm{ld}(G)$, then G is n-step.*

Proof. This is clear from the proof of Proposition 2.1 and Corollary 2.2. □

Example 3.13. Let $G = \mathcal{G}^{\mathbb{N}}$ be the full one-sided group shift on a finite simple group, then $\mathrm{ld}(G) = |\mathcal{G}|$.

Note that the limit degree of a one-sided group shift G can also be describes as $\mathrm{ld}(G) = \lim_{i \to \infty} \frac{|G[i]|}{|G[i-1]|}$. The smallest value $\mathrm{ld}(G)$ can take is 1. The following lemma shows that this happens if and only if G is finite.

Lemma 3.14. *Let G be an expansive profinite group. Then $\mathrm{ld}(G) = 1$ if and only if G is finite.*

Proof. If G is finite, we can consider the underlying finite group $\mathcal{G}$ obtained from G by forgetting σ. Then $\phi\colon G \to \mathcal{G}^{\mathbb{N}},\ g \mapsto (g, \sigma(g), \sigma^2(g), \dots)$ identifies G with a one-sided group shift of finite type with limit degree 1.

Conversely, assume that G is an expansive profinite with $\mathrm{ld}(G) = 1$. We may assume that G is a one-sided group shift on a finite group $\mathcal{G}$. Then, using the notation of the proof of Proposition 2.1 and Corollary 2.2, we have $|G[i]| = |\mathcal{G}_0| \cdot |\mathcal{G}_1| \dots |\mathcal{G}_i| = |\mathcal{G}_0| \dots |\mathcal{G}_{n-1}|$ for $i \geq n$. In particular, $m := |G[i]|$ is independent of i for $i \gg 0$. Since G is the projective limit of the $G[i]$'s, it follows that $|G| = m$. □

The following lemma shows that the limit degree is multiplicative.

Lemma 3.15. *Let G be an expansive profinite group and N a normal expansive subgroup. Then* $\mathrm{ld}(N)$ *divides* $\mathrm{ld}(G)$ *and* $\mathrm{ld}(G/N) = \frac{\mathrm{ld}(G)}{\mathrm{ld}(N)}$.

Proof. By Lemma 3.3 we may assume that G is a one-sided group shift on a finite group $\mathcal{G}$. Let $n \in \mathbb{N}$ be such that N is an n-step group shift of finite type (Corollary 2.4). The morphism

$$\phi\colon G \to (G[n]/N[n])^{\mathbb{N}},\ (g_0, g_1, \dots) \mapsto (\overline{(g_i, g_{i+1}, \dots, g_{i+n})})_{i \in \mathbb{N}}$$

of expansive profinite groups has kernel N and induces, for every $i \in \mathbb{N}$, an isomorphism $G[n+i]/N[n+i] \simeq \phi(G)[i]$. Therefore

$$\mathrm{ld}(G/N) = \mathrm{ld}(\phi(G)) = \lim_{i\to\infty} \frac{|\phi(G)[i]|}{|\phi(G)[i-1]|} = \lim_{i\to\infty} \frac{\frac{|G[n+i]|}{|N[n+i]|}}{\frac{|G[n+i-1]|}{|N[n+i-1]|}} = \lim_{i\to\infty} \frac{\frac{|G[n+i]|}{|G[n+i-1]|}}{\frac{|N[n+i]|}{|N[n+i-1]|}} = \frac{\mathrm{ld}(G)}{\mathrm{ld}(N)}.$$

□

Every expansive profinite group is isomorphic to G_Γ for some directed group graph Γ (Definition 2.5). For later use, we record a slightly more precise statement.

Lemma 3.16. *Let G be an expansive profinite group. Then there exists a finite group $\mathcal{H}$ and a 1-step group shift $H \subseteq \mathcal{H}^{\mathbb{N}}$ such that G is isomorphic to H, $H[0] = \mathcal{H}$ and* $\mathrm{ld}(G) = |\ker(H[1] \xrightarrow{\pi_1} H[0])|$. *In particular, $G \simeq G_\Gamma$, for some directed group graph Γ.*

Proof. It is well-known ([Kit98, p. 27]) that every one-sided subshift of finite type is isomorphic to a 1-step subshift of finite type (via a higher block representation). We follow a similar idea here.

By Lemma 3.3 we can assume that G is a one-sided group shift on a finite group $\mathcal{G}$. Let n be the smallest integer such that $|\ker(G[n] \xrightarrow{\pi_n} G[n-1])| = \mathrm{ld}(G)$. Then $G \leq \mathcal{G}^{\mathbb{N}}$ consists of exactly those sequences in $\mathcal{G}^{\mathbb{N}}$ that have all blocks of length $n+1$ inside $\mathcal{H} = G[n]$ (Lemma 3.12). Define a map $\phi\colon G \to \mathcal{H}^{\mathbb{N}}$ by $\phi(g) = (g_i, g_{i+1}, \dots, g_{i+n})_{i\in\mathbb{N}}$ for $g = (g_0, g_1, \dots) \in G$. Then ϕ is an injective morphism of group shifts. The image $H = \phi(G)$ of ϕ is the 1-step group shift on $\mathcal{H}$ defined by the directed group graph with directed edges $E \leq \mathcal{H} \times \mathcal{H}$ given by

$$E = \{((g_0, \dots, g_n), (g'_0, \dots, g'_n)) \in \mathcal{H} \times \mathcal{H} |\ g_1 = g'_0, \dots, g_n = g'_{n-1}\}.$$

So $\phi\colon G \to H$ is an isomorphism. As the projection $G \to G[n]$ is surjective, we see that $H[0] = \mathcal{H}$. Moreover, the kernel of $\pi_1\colon H[1] = E \to H[0] = \mathcal{H},\ (h_0, h_1) \mapsto h_0$ equals $\{1\} \times \ker(G[n] \xrightarrow{\pi_n} G[n-1]) \leq \mathcal{H} \times \mathcal{H}$ and thus has cardinality $\mathrm{ld}(G)$. □

The following corollary shows that an expansive endomorphism is rarely injective.

Corollary 3.17. *Let G be an expansive profinite group with $\sigma\colon G \to G$ injective. Then G is finite.*

Proof. By Lemma 3.16 we can assume that $G = G_\Gamma$ for some directed group graph Γ. Without loss of generality, we can assume that every vertex of Γ is contained in an infinite directed path. Then σ is injective on G if and only if there is no vertex with more than one incoming directed edge. This implies that Γ is a disjoint union of directed cycles. But then G is finite. □

We will have use for a version of Lemma 3.16 that simultaneously works for an expansive subgroup.

Lemma 3.18. *Let G be an expansive profinite group and $H \leq G$ an expansive subgroup. Then there exists a finite group $\mathcal{G}$ and an injective morphism $\phi\colon G \to \mathcal{G}^{\mathbb{N}}$ of expansive profinite groups such that $\phi(G) \leq \mathcal{G}^{\mathbb{N}}$ and $\phi(H) \leq \mathcal{G}^{\mathbb{N}}$ are 1-step group shifts of finite type.*

Proof. By Lemma 3.3 we can assume that G is a one-sided group shift on a finite group $\mathcal{H}$. By Corollary 2.4 there exists an $n_G \in \mathbb{N}$ such that G is n_G-step. Similarly, there exists an $n_H \in \mathbb{N}$ such that H is n_H-step. Let n be the maximum of n_G and n_H. Then G and H are both n-step.

Set $\mathcal{G} = G[n]$. Then $\phi\colon G \to \mathcal{G}^{\mathbb{N}}$, $(g_0, g_1, \ldots) \mapsto ((g_i, g_{i+1}, \ldots, g_{i+n}))_{i\in\mathbb{N}}$ has the desired property (cf. proof of Lemma 3.16). □

3.4. **The σ-identity component.** Since profinite groups are totally disconnected, the connected component containing the identity is always trivial. However, requiring the closed sets of an expansive profinite group to also be σ-stable, leads to an interesting notion of identity component with properties somewhat analogous to the identity component of an algebraic group. The σ-identity component is important for the main decomposition theorem (Theorem 4.6) because it yields the first group in the subnormal series.

Some considerations in this section have some similarity with [Kit98, Section 5.1] and [LM95, Section 4.4]. However, our approach is different and guided by topology.

Let X be a topological space equipped with a continuous map $\sigma\colon X \to X$. Then the closed σ-stable subsets of X satisfy the axioms for the closed sets of a topology. We call this topology on X the *σ-topology*.

Recall that a connected component of a topological space is a maximal connected subset. The connected components are closed and the whole space is the disjoint union of its connected components. A subset of X that is connected or irreducible with respect to the σ-topology is called *σ-connected* or *σ-irreducible* respectively. The connected components with respect to the σ-topology are called the *σ-connected components*.

An infinite subshift of finite type has infinitely many connected components as the connected components are in fact the singletons. However, the following lemma shows that it only has finitely many σ-connected components.

Lemma 3.19. *Let X be a one-sided subshift of finite type. Then X has only finitely many σ-connected components.*

Proof. Every one-sided subshift of finite type is isomorphic to a 1-step subshift of finite type (cf. [LM95, Proposition 2.3.9]). We can thus assume that $X = X_\Gamma$ for a directed graph Γ. Without loss of generality, we assume that every vertex of Γ lies on an infinite directed path.

Let $\Gamma_1, \ldots, \Gamma_r$ denote the strongly connected components of Γ whose associated subshift X_{Γ_i} is non-empty. Note that the subshift associated to a strongly connected component is empty only if the component has a unique vertex and no directed edge (from the vertex to itself), and this only happens for vertices that do not lie on any directed circuit in Γ.

We define an undirected graph Δ with set of vertices $\{\Gamma_1, \ldots, \Gamma_r\}$ and an edge between Γ_i and Γ_j if there exists a directed path in Γ that connects a vertex in Γ_i to a vertex in Γ_j. Let $\Delta_1, \ldots, \Delta_s$ denote the connected components of Δ. For $i = 1, \ldots, s$ let Θ_i denote the full directed subgraph of Γ whose vertices are all vertices of Γ that can be connected with a directed path to a vertex belonging to some Γ_j, such that Γ_j is a vertex of Δ_i.

An infinite directed path in Γ might traverse from one strongly connected component to another. However, in that case, it can never return to this strongly connected component. Therefore, every infinite directed path in Γ eventually stays in one Γ_i. This shows that every infinite directed path in Γ lives inside a unique Θ_i. Therefore $X = X_{\Theta_1} \uplus \ldots \uplus X_{\Theta_s}$. To complete the proof it suffices to show that X_{Θ_i} is σ-connected for $i = 1, \ldots, s$.

The closure of a σ-orbit is σ-irreducible. It follows that X_Γ is σ-irreducible if Γ is strongly connected because then X_Γ contains a point with dense σ-orbit. To find such a point one constructs a directed path in Γ that traverses every finite directed path in Γ (cf. [Kit98, Theorem 1.4.1 (i)]).

It follows that X_{Γ_j} is σ-irreducible and a fortiori σ-connected for every $j = 1, \ldots, r$. Note that $X_{\Gamma_j} \subseteq X_{\Theta_i}$ for every Γ_j that is a vertex of Δ_i. For every Γ_j that is a vertex of Δ_i there exists a unique σ-connected component X_j of X containing X_{Γ_j} because X_{Γ_j} is σ-connected. We will show that $X_j = X_{j'}$ for any j, j' such that Γ_j and $\Gamma_{j'}$ are vertices of Δ_i. Because Δ_i is connected, it suffices to show this under the additional assumption that there exists a directed path in Γ from a vertex in $\Gamma_{j'}$ to a vertex in Γ_j.

Note that if a point $x \in X$ is such that $\sigma^m(x) \in X_j$ for some $m \in \mathbb{N}$, then $x \in X_j$ because the σ-connected component containing x also contains $\sigma^m(x)$. Using this, we see that a given point $y \in X_{\Gamma_{j'}}$ can be approximated arbitrarily well with a point in X_j: Choose a directed path in $X_{\Gamma_{j'}}$ that agrees with the directed path corresponding to y up to an arbitrary large index and then continue this directed path to an infinite directed path in Γ that eventually stays in Γ_j. Because X_j is closed, it follows that $y \in X_j$. So $y \in X_j \cap X_{j'}$ and therefore $X_j = X_{j'}$ as desired.

Thus there exists a σ-connected component Y of X such that $X_{\Gamma_j} \subseteq Y$ for every j such that Γ_j a vertex of Δ_i. Since every infinite directed path in Θ_i eventually stays in some Γ_j, with Γ_j a vertex of Δ_i, we see that for every $x \in X_{\Theta_i}$ there exists an $m \in \mathbb{N}$ with $\sigma^m(x) \in Y$. This shows that $X_{\Theta_i} \subseteq Y$. From $X = X_{\Theta_1} \uplus \ldots \uplus X_{\Theta_s}$ we deduce that $X_{\Theta_i} = Y$ is σ-connected. □

We now return to groups:

Lemma 3.20. *Let G be an expansive profinite group. Then:*

(i) *There are only finitely many σ-connected components in G.*
(ii) *The σ-connected component $G^{\sigma o}$ of G that contains 1 is a normal expansive subgroup of G such that $G/G^{\sigma o}$ is finite and $\sigma\colon G/G^{\sigma o} \to G/G^{\sigma o}$ is bijective.*
(iii) *If $G = G_\Gamma$ for a directed group graph Γ, then the σ-connected component containing 1 equals G_{Γ^o}, where Γ^o is the full directed subgraph of Γ whose set of vertices consists of all vertices of Γ that can be connected to 1 with a directed path.*

Proof. Since every expansive profinite group is isomorphic to a group shift of finite type, (i) follows from Lemma 3.19. To establish (ii), by Lemma 3.16, we may assume that $G = G_\Gamma$ for some directed group graph Γ on a finite group $\mathcal{G}$. Without loss of generality we assume that every vertex of Γ is contained in an infinite directed path.

Let $\mathcal{G}^o \subseteq \mathcal{G}$ denote the set of all vertices g of Γ such that there exists a directed path in Γ starting at g and ending at 1. If $g_1, g_2 \in \mathcal{G}^o$, then a directed path from g_i to 1 can be extended by adding the vertex 1 at the end a certain number of times. The product of two such directed paths then yields a directed path from $g_1 g_2$ to 1. This shows that $\mathcal{G}^o$ is a subgroup of $\mathcal{G}$.

To show that $\mathcal{G}^o$ is normal in $\mathcal{G}$, let $g \in \mathcal{G}^o$ and fix a directed path γ from g to 1. Let $h \in \mathcal{G}$ and choose a directed path δ starting at h with the same length as γ. Then $\delta\gamma\delta^{-1}$ is a directed path in Γ from hgh^{-1} to 1. Thus $hgh^{-1} \in \mathcal{G}^o$ and $\mathcal{G}^o$ is normal in $\mathcal{G}$.

Let Γ^o denote the full directed subgraph of Γ with vertex set $\mathcal{G}^o$. Because $\mathcal{G}^o$ is a normal subgroup of $\mathcal{G}$, we see that G_{Γ^o} is a normal expansive subgroup of $G = G_\Gamma$. If $g \in \mathcal{G}$ is such that there exists a directed edge from g to an element of $\mathcal{G}^o$, then $g \in \mathcal{G}^o$. This shows that $\sigma^{-1}(G_{\Gamma^o}) = G_{\Gamma^o}$ and therefore $\sigma\colon G/G_{\Gamma^o} \to G/G_{\Gamma^o}$ is injective. It thus follows from Corollary 3.17 that G/G_{Γ^o} is finite and so $\sigma\colon G/G_{\Gamma^o} \to G/G_{\Gamma^o}$ is bijective. Thus G/G_{Γ^o} is

the disjoint union of σ-orbits $o_1, \dots, o_r$. If $\pi\colon G \to G/G^{\sigma o}$ is the canonical map, then G is the disjoint union of the closed σ-stable subsets $\pi^{-1}(o_1), \dots, \pi^{-1}(o_r)$. Note that the identity element of $G/G^{\sigma o}$ is a σ-orbit, say o_1. Then $\pi^{-1}(o_1) = G_{\Gamma^o}$. From the proof of Lemma 3.19 it is clear that G_{Γ^o} is σ-connected. From $G = \pi^{-1}(o_1) \uplus \dots \uplus \pi^{-1}(o_r)$ it follows that G_{Γ^o} is the σ-connected component of G containing 1, i.e., $G^{\sigma o} = G_{\Gamma^o}$. This completes the proof of (ii) and (iii). □

Definition 3.21. *Let G be an expansive profinite group. The σ-connected component $G^{\sigma o}$ of G containing 1 is called the* σ-identity component *of G.*

By Lemma 3.20 we know that $G^{\sigma o}$ is a normal expansive subgroup of G such that $G/G^{\sigma o}$ is finite and $\sigma\colon G/G^{\sigma o} \to G/G^{\sigma o}$ is bijective. Note that an expansive profinite group is σ-connected if and only if it equals its σ-identity component.

Example 3.22. A full one-sided group shift is σ-connected by Lemma 3.20 (iii).

Example 3.23. Let G be an expansive profinite group that is finite. We claim that $G^{\sigma o} = \{g \in G |\ \exists\, n \in \mathbb{N}\colon \sigma^n(g) = 1\}$. Let N denote the right hand side of this equation. Then N is a normal σ-connected expansive subgroup of G. Moreover, $\sigma^{-1}(N) = N$, so $\sigma\colon G/N \to G/N$ is injective and therefore bijective. It follows that G is the disjoint union of the σ-stable sets $\pi^{-1}(o)$, where o is an orbit of σ on G/N and $\pi\colon G \to G/N$ the canonical map. From this we deduce that N is the σ-connected component of G containing 1.

The following simple example shows that a σ-connected expansive profinite group need not be σ-irreducible. However, it follows from Corollary 5.3 that a σ-connected expansive profinite group G with $\sigma\colon G \to G$ surjective is σ-irreducible.

Example 3.24. Let $G = \{1, h, h^2\}$ be the cyclic group with three elements and $\sigma\colon G \to G,\ g \mapsto 1$ the trivial endomorphism. Then G is σ-connected but not σ-irreducible because G is the union of the σ-closed sets $\{1, h\}$ and $\{1, h^2\}$.

For the proof of the main decomposition theorem we need the following:

Lemma 3.25. *Let G be an expansive profinite group and N a normal expansive subgroup of G. Then $N^{\sigma o}$ is normal in G.*

Proof. By Lemma 3.18 we may assume that $G \leq \mathcal{G}^{\mathbb{N}}$ such that G and N are 1-step group shifts of finite type. Let Γ be the directed group graph on $\mathcal{G}$ such that $G = G_\Gamma$. Then there is a directed subgraph Γ' of Γ such that $N = G_{\Gamma'}$. The set $\mathcal{N}' = N[0]$ of vertices of Γ' is a normal subgroup of $G[0] \leq \mathcal{G}$ because N is normal in G. Moreover, $N^{\sigma o} = G_{\Gamma''}$, where Γ'' is the full directed subgraph of Γ' whose set of vertices $\mathcal{N}''$ consists of all elements of $\mathcal{N}'$ that can be connected with 1 through a directed path inside Γ' (Lemma 3.20 (iii)).

We will show that $\mathcal{N}''$ is normal in $G[0]$. Let $n \in \mathcal{N}''$ and $g \in G[0]$. Consider an infinite directed path γ in Γ starting at g and an infinite directed path δ in Γ' that starts at n, goes to 1 and then stabilizes at 1. Because N is normal in G, the directed path $\gamma\delta\gamma^{-1}$ lies inside Γ'. Moreover it starts at gng^{-1} and ends at 1. Therefore $gng^{-1} \in \mathcal{N}''$ and $\mathcal{N}''$ is normal in $G[0]$. This implies that $N^{\sigma o} = G_{\Gamma''}$ is normal in $G = G_\Gamma$. □

Lemma 3.26. *Let $\phi\colon G \to H$ be a morphism of expansive profinite groups. If G is σ-connected, then $\phi(G)$ is σ-connected.*

Proof. If V is a closed σ-stable subset of H, then $\phi^{-1}(V)$ is a closed σ-stable subset of G. Thus ϕ is σ-continuous, i.e., continuous with respect to the σ-topologies on G and H. So the claim follows from the general fact that a continuous map sends connected subsets to connected subsets. □

Lemma 3.27. *Let G be an expansive profinite group. Then* $\mathrm{ld}(G^{\sigma o}) = \mathrm{ld}(G)$.

Proof. Since $G/G^{\sigma o}$ is finite (Lemma 3.20), we know that $\mathrm{ld}(G/G^{\sigma o}) = 1$ from Lemma 3.14. Thus the claim follows from Lemma 3.15. □

The following two lemmas are needed to prove the uniqueness of the group G_1 in the theorem stated in the introduction. The next lemma is a converse to Lemma 3.20 (ii).

Lemma 3.28. *Let N be a normal expansive subgroup of an expansive profinite group G such that G/N is finite and $\sigma\colon G/N \to G/N$ is bijective. Then $G^{\sigma o} \subseteq N$. Moreover, if N is σ-connected, then $N = G^{\sigma o}$.*

Proof. Consider the canonical map $\pi\colon G \to G/N$ and let $o_1, \dots, o_r$ denote the orbits of σ on G/N. Because G/N is finite, these σ-orbits are closed and because σ is bijective on G/N the orbits are disjoint. If follows that G is the disjoint union of the closed σ-stable subsets $\pi^{-1}(o_i)$. Since $N = \pi^{-1}(o_1)$, where $o_1 = \{1\}$ is the σ-orbit of the identity of G/N, we see that $G^{\sigma o} \subseteq N$. If N is σ-connected, then $\pi^{-1}(o_1)$ is a σ-connected component. So $N = G^{\sigma o}$. □

Lemma 3.29. *Let G be an expansive profinite group with a normal expansive subgroup N such that N and G/N are σ-connected. Then G is σ-connected.*

Proof. As N is σ-connected and contains 1, we have $N \subseteq G^{\sigma o}$. Thus $G^{\sigma o}/N$ is a normal expansive subgroup of G/N with $(G/N)/(G^{\sigma o}/N) \simeq G/G^{\sigma o}$. So $(G/N)/(G^{\sigma o}/N)$ is finite and $\sigma\colon (G/N)/(G^{\sigma o}/N) \to (G/N)/(G^{\sigma o}/N)$ is bijective (Lemma 3.20). Because $G^{\sigma o}/N$ is σ-connected (Lemma 3.26) it follows from Lemma 3.28 that $G^{\sigma o}/N = (G/N)^{\sigma o} = G/N$. Therefore $G^{\sigma o} = G$. □

3.5. **One-sided group shifts on finite simple groups.** The results in this subsection are needed for the uniqueness statement in the main decomposition theorem.

Lemma 3.30. *Let $\mathcal{G}$ be a finite simple group and $G = \mathcal{G}^{\mathbb{N}}$ the full one-sided group shift on $\mathcal{G}$. If N is a proper normal expansive subgroup of G, then N is finite and G/N is isomorphic to $\mathcal{G}^{\mathbb{N}}$.*

Proof. We have to distinguish two cases: First we assume that $\mathcal{G}$ is not abelian. This implies that any normal subgroup $\mathcal{N}$ of $\mathcal{G}^n$ is of the form $\mathcal{N} = \mathcal{N}_1 \times \ldots \times \mathcal{N}_n$ with $\mathcal{N}_i \in \{1, \mathcal{G}\}$ for $i = 1, \dots, n$. To see this, note that if $(h_1, \dots, h_n) \in \mathcal{N}$ with $h_i \neq 1$ for some $1 \leq i \leq n$, then there exists g in $\mathcal{G}$ with $gh_i \neq h_i g$ as otherwise the center of $\mathcal{G}$ would be non-trivial. Then

$$\begin{aligned}&(1, \dots, 1, g, 1, \dots, 1)(h_1, \dots, h_n)(1, \dots, 1, g, 1, \dots, 1)^{-1}(h_1, \dots, h_n)^{-1} = \\ &= (1, \dots, 1, gh_i g^{-1} h_i^{-1}, 1, \dots, 1)\end{aligned}$$

is a non-trivial element of $\mathcal{N} \cap (1 \times \ldots \times 1 \times \mathcal{G} \times 1 \times \ldots \times 1)$. By the simplicity of $\mathcal{G}$ we find $1 \times \ldots \times 1 \times \mathcal{G} \times 1 \times \ldots \times 1 \subseteq \mathcal{N}$.

As N is a proper subgroup of G, there exists an $i \in \mathbb{N}$ such that $N[i]$ is a proper subgroup of $\mathcal{G}^{i+1}$. Let i be minimal with this property. Because N is normal in G, $N[i]$ is normal in $\mathcal{G}^{i+1}$. By the minimality of i we have $\mathcal{G}^i \times \{1\} \subseteq N[i]$. It follows that $N[i] = \mathcal{G}^i \times \{1\}$. But then necessarily $N = \mathcal{G}^i \times 1 \times 1 \times \ldots \leq \mathcal{G}^{\mathbb{N}}$. The surjective morphism

$$\mathcal{G}^{\mathbb{N}} \to \mathcal{G}^{\mathbb{N}}, \ (g_0, g_1, \ldots) \mapsto (g_i, g_{i+1}, \ldots)$$

induces an isomorphism $G/N \simeq \mathcal{G}^{\mathbb{N}}$.

We now treat the case that $\mathcal{G}$ is abelian. Then $\mathcal{G}$ is cyclic of prime order and does not have any proper non-trivial subgroups. For $i \geq 1$ let $\mathcal{N}_i$ denote the subgroup of $\mathcal{G}$ such that the kernel of $\pi_i\colon N[i] \to N[i-1]$ is of the form $\{1\}^i \times \mathcal{N}_i \leq \mathcal{G}^{i+1}$. We also set $\mathcal{N}_0 = N[0]$. Then the $\mathcal{N}_i$ are a decreasing chain of subgroups of $\mathcal{G}$ (cf. proof of Proposition 2.1). We cannot have $\mathcal{N}_i = \mathcal{G}$ for all $i \in \mathbb{N}$ because this would imply $N = G$.

Thus there exist an $n \in \mathbb{N}$ such that $\mathcal{N}_0, \dots, \mathcal{N}_{n-1}$ are all equal to $\mathcal{G}$ and $\mathcal{N}_n, \mathcal{N}_{n+1}, \dots$ are all equal to the trivial group. So $\mathrm{ld}(N) = 1$ and N is n-step by Lemma 3.12. In particular,

N is finite by Lemma 3.14. As $\mathcal{G}^{n+1}/N[n]$ has the same (prime) cardinality as $\mathcal{G}$ we see that $\mathcal{G}^{n+1}/N[n] \simeq \mathcal{G}$.

The map $G \to (\mathcal{G}^{n+1}/N[n])^{\mathbb{N}},\ (g_0, g_1, \ldots) \mapsto (\overline{(g_i, g_{i+1}, \ldots, g_{i+n})})_{i\in\mathbb{N}}$ is a surjective morphism of expansive profinite groups with kernel N and therefore induces an isomorphism $G/N \simeq (\mathcal{G}^{n+1}/N[n])^{\mathbb{N}} \simeq \mathcal{G}^{\mathbb{N}}$. □

Example 3.31. In the proof of Lemma 3.30 we have seen that if $\mathcal{G}$ is a finite non-abelian simple group, then every proper normal expansive subgroup N of $\mathcal{G}^{\mathbb{N}}$ is of the form $N = \mathcal{G}^i \times 1 \times 1 \ldots \leq \mathcal{G}^{\mathbb{N}}$ for some $i \in \mathbb{N}$. If $\mathcal{G}$ is not abelian, this is not true anymore, for example, for $\mathcal{G}$ abelian, the "diagonal" subgroup $N = \{(g, g, \ldots) |\ g \in \mathcal{G}\}$ is a proper normal expansive subgroup.

One can recover $\mathcal{G}$ from $\mathcal{G}^{\mathbb{N}}$:

Lemma 3.32. *Let $\mathcal{G}$ and $\mathcal{H}$ be finite groups. If the full one-sided group shifts $\mathcal{G}^{\mathbb{N}}$ and $\mathcal{H}^{\mathbb{N}}$ are isomorphic, then $\mathcal{G}$ and $\mathcal{H}$ are isomorphic.*

Proof. It suffices to note that $\mathcal{G}$ can be recovered from $G = \mathcal{G}^{\mathbb{N}}$ as the kernel of $\sigma\colon G \to G$. □

3.6. **σ-Infinitesimal expansive profinite groups.** In this short subsection we deal with the groups that occur in the last position in the subnormal series in the main decomposition theorem (Theorem 4.6).

Definition 3.33. *An expansive profinite group G is* σ-infinitesimal *if for every $g \in G$ there exists an $n \in \mathbb{N}$ such that $\sigma^n(g) = 1$.*

Example 3.34. In the proof of Lemma 3.30 we have seen that every proper normal expansive subgroup of a full one-sided shift on a finte non-abelian simple group is σ-infinitesimal.

Lemma 3.35. *Let G be an expansive profinite group. Then G is σ-infinitesimal if and only if G is finite and some power of $\sigma\colon G \to G$ is the trivial endomorphism $g \mapsto 1$.*

Proof. By Lemma 3.16, we may assume that $G = G_\Gamma$ for some directed group graph Γ. Suppose Γ contains a cycle that is not equal to the cycle whose only edge is $(1, 1)$. Looping inside this cycle yields a periodic point $g \in G$. This contradicts the assumption that $\sigma^n(g) = 1$ for some $n \in \mathbb{N}$. Thus the only circuit in Γ is stationary at 1. This implies that G is finite and so $\sigma^n(g) = 1$ for all $g \in G$ for $n \gg 1$.

The reverse implication is clear. □

Note that a σ-infinitesimal expansive profinite group is σ-connected because every σ-stable subset contains 1. For finite groups there is a converse:

Lemma 3.36. *A finite σ-connected expansive profinite group is σ-infinitesimal.*

Proof. Let G be a finite σ-connected expansive group. Then G is the disjoint union of the σ-closed sets $\{g \in G |\ \exists\ n \in \mathbb{N}\colon \sigma^n(g) = 1\}$ and $\{g \in G |\ \sigma^n(g) \neq 1\ \forall\ n \in \mathbb{N}\}$. The former set is non-empty because it contains 1 and must therefore equal G. □

4. The decomposition theorem

In this section we prove our main result: the decomposition theorem (Theorem 4.6). The proof proceeds by induction on the limit degree. We first tackle the case where the induction hypothesis cannot be applied. More precisely, we show that for an infinite expansive σ-connected profinite group G such that $\mathrm{ld}(N) \in \{1, \mathrm{ld}(G)\}$ for any normal expansive subgroup N of G, there exists an $\ell \in \mathbb{N}$ such that $G/\ker(\sigma^\ell)$ is isomorphic to a full one-sided group shift on a finite simple group.

Let G be an expansive profinite group. It will be useful to consider the set $\mathrm{Emb}(G)$ of all morphisms $\phi\colon G \to \mathcal{G}^{\mathbb{N}}$ from G to a full one-sided group shift such that

- $\ker(\phi)$ agrees with the kernel of $\sigma^\ell\colon G \to G$ for some $\ell \in \mathbb{N}$, in particular, $\ker(\phi)$ is σ-infinitesimal (for $\ell = 0$, by definition, $\sigma^\ell = \mathrm{id}$ and so $\ker(\sigma^\ell) = 1$),
- $\phi(G)[0] = \mathcal{G}$ and
- $\mathrm{ld}(G) = |\ker(\phi(G)[1] \xrightarrow{\pi_1} \phi(G)[0])|$.

Recall that π_1 and the notation $G[i]$ was defined in Section 2. Note that by Lemma 3.16 $\mathrm{Emb}(G)$ is non-empty. Moreover, for $\phi \in \mathrm{Emb}(G)$ we have $\mathrm{ld}(\phi(G)) = \mathrm{ld}(G)$ and $\phi(G)$ is 1-step (Lemmas 3.15, 3.14, 3.35 and 3.12).

Lemma 4.1. *Let G be an expansive profinite group and let $\phi\colon G \to \mathcal{G}^{\mathbb{N}}$ be an element of $\mathrm{Emb}(G)$ such that $|\mathcal{G}|$ is minimal. Then, for every $i \in \mathbb{N}$, the map $\phi(G) \to \mathcal{G},\ (g_0, g_1, \ldots) \mapsto g_i$ is surjective.*

Proof. Assume, for a contradiction, that there exists an $i \in \mathbb{N}$ such that the image $\mathcal{H} \leq \mathcal{G}$ of $\phi(G) \to \mathcal{G},\ (g_0, g_1, \ldots) \mapsto g_i$ is properly contained in $\mathcal{G}$. The map

$$\phi'\colon \phi(G) \to \mathcal{H}^{\mathbb{N}},\ (g_0, g_1, \ldots) \mapsto (g_i, g_{i+1}, \ldots)$$

is a morphism of expansive profinite groups and so is the composition $\phi'' = \phi'\phi\colon G \to \mathcal{H}^{\mathbb{N}}$. We will show that $\phi'' \in \mathrm{Emb}(G)$.

Assume $\ker(\phi) = \ker(\sigma^\ell)$. We claim that $\ker(\phi'') = \ker(\sigma^{\ell+i})$. If $g \in \ker(\phi'')$, then $\phi(g) \in \ker(\phi')$ and so $\sigma^i(\phi(g)) = 1$. Thus $\phi(\sigma^i(g)) = \sigma^i(\phi(g)) = 1$ and so $\sigma^i(g) \in \ker(\phi) = \ker(\sigma^\ell)$. Therefore $g \in \ker(\sigma^{\ell+i})$.

Conversely, if $g \in \ker(\sigma^{\ell+i})$, then $\sigma^i(g) \in \ker(\sigma^\ell) = \ker(\phi)$, and so $\sigma^i(\phi(g)) = \phi(\sigma^i(g)) = 1$. Thus $\phi(g) \in \ker(\phi')$ and $g \in \ker(\phi'')$.

By construction $\phi''(G)[0] = \mathcal{H}$. We have a commutative diagram

$$\begin{array}{ccc} \phi''(G)[1] & \longrightarrow & \phi''(G)[0] \\ \downarrow{\scriptstyle \rho_1} & & \downarrow{\scriptstyle \rho_0} \\ \phi(G)[1] & \longrightarrow & \phi(G)[0] \end{array}$$

where $\rho_1(h_0, h_1) = (h_0, h_1)$ and $\rho_0(h_0) = h_0$. As ρ_1 maps the kernel of $\phi''(G)[1] \to \phi''(G)[0]$ injectively into the kernel of $\phi(G)[1] \to \phi(G)[0]$, we see that

$$|\ker(\phi''(G)[1] \to \phi''(G)[0])| \leq |\ker(\phi(G)[1] \to \phi(G)[0])| = \mathrm{ld}(G),$$

where the latter equality follows from $\phi \in \mathrm{Emb}(G)$. By Lemma 3.12 the sequence $|\ker(\phi''(G)[j] \to \phi''(G)[j-1])|_{j\geq 1}$ is non-increasing and stabilizes with value $\mathrm{ld}(\phi''(G))$. But, using Lemmas 3.15 and 3.14, we find

$$\mathrm{ld}(\phi''(G)) = \mathrm{ld}(G/\ker(\phi'')) = \frac{\mathrm{ld}(G)}{\mathrm{ld}(\ker(\phi''))} = \mathrm{ld}(G).$$

In summary, it follows that $\phi'' \in \mathrm{Emb}(G)$. Because $|\mathcal{H}| < |\mathcal{G}|$, this contradicts the choice of ϕ. □

Proposition 4.2. *Let G be an infinite expansive profinite group and let $\phi\colon G \to \mathcal{G}^{\mathbb{N}}$ be an element of $\mathrm{Emb}(G)$ such that $|\mathcal{G}|$ is minimal. Then there exists a normal non-trivial subgroup $\mathcal{N}$ of $\mathcal{G}$ such that $\mathcal{N}^{\mathbb{N}} \subseteq \phi(G)$.*

Proof. We consider $\phi(G)[1] \leq \mathcal{G} \times \mathcal{G}$ and $\pi_1\colon \phi(G)[1] \to \phi(G)[0] = \mathcal{G},\ (g_0, g_1) \mapsto g_0$. We also have a group homomorphism $\sigma_1\colon \phi(G)[1] \to \mathcal{G},\ (g_0, g_1) \mapsto g_1$. Let $\mathcal{G}_1 \leq \mathcal{G}$ be such that $\ker(\pi_1) = \{1\} \times \mathcal{G}_1$. Similarly, let $\mathcal{G}' \leq \mathcal{G}$ be such that $\ker(\sigma_1) = \mathcal{G}' \times 1$. Then $\mathcal{G}' \times \mathcal{G}_1$ is a normal subgroup of $\phi(G)[1]$. Moreover, since σ_1 is surjective (Lemma 4.1), $\mathcal{G}_1$ is normal in $\mathcal{G}$ and because π_1 maps onto $\mathcal{G}$, $\mathcal{G}'$ is normal in $\mathcal{G}$. Thus $\mathcal{N} = \mathcal{G}_1 \cap \mathcal{G}'$ is normal in $\mathcal{G}$.

Suppose $\mathcal{N} = 1$. Define $\mathcal{H} = \phi(G)[1]/(\mathcal{G}' \times \mathcal{G}_1)$ and consider the morphism

$$\phi'\colon G \to \mathcal{H}^{\mathbb{N}},\ g \mapsto (\overline{\phi(g)_i, \phi(g)_{i+1}})_{i\in\mathbb{N}}$$

of expansive profinite groups. Note that ϕ' is the composition of $\phi\colon G \to \phi(G)$, the 2-block presentation $\phi(G) \simeq (\phi(G)[1])^{\mathbb{N}}$ and the 1-block map $(\phi(G)[1])^{\mathbb{N}} \to \mathcal{H}^{\mathbb{N}}$.

We will show that $\phi' \in \mathrm{Emb}(G)$. Let $\ell \in \mathbb{N}$ be such that $\ker(\phi) = \ker(\sigma^\ell)$. We claim that $\ker(\phi') = \ker(\sigma^{\ell+1})$. If $g \in \ker(\phi')$, then $\phi(g)$ lies in the kernel of the map

$$\phi(G) \to \mathcal{H}^{\mathbb{N}},\ (g_0, g_1, \ldots) \mapsto \left(\overline{(g_i, g_{i+1})}\right)_{i\in\mathbb{N}},$$

which equals $\mathcal{G}' \times 1 \times 1 \ldots \leq \mathcal{G}^{\mathbb{N}}$ because $\mathcal{N} = 1$. Thus $\phi(\sigma(g)) = \sigma(\phi(g)) = 1$. So $\sigma(g) \in \ker(\phi) = \ker(\sigma^\ell)$ and therefore $g \in \ker(\sigma^{\ell+1})$.

Conversely, if $g \in \ker(\sigma^{\ell+1})$, then $\sigma(g) \in \ker(\sigma^\ell) = \ker(\phi)$ and so $\sigma(\phi(g)) = \phi(\sigma(g)) = 1$. Thus $\phi(g) = (g', 1, 1, \ldots)$ with $g' \in \mathcal{G}'$ and therefore $g \in \ker(\phi')$.

In particular, $\ker(\phi')$ is σ-infinitesimal and therefore finite (Lemma 3.35). So, using Lemmas 3.15 and 3.14 we have

$$\mathrm{ld}(\phi'(G)) = \mathrm{ld}(G/\ker(\phi')) = \frac{\mathrm{ld}(G)}{\mathrm{ld}(\ker(\phi'))} = \mathrm{ld}(G).$$

The surjective group homomorphism $\phi(G)[1] \to \mathcal{G}/\mathcal{G}',\ (g_0, g_1) \mapsto \overline{g_0}$ has kernel $\mathcal{G}' \times \mathcal{G}_1$ and therefore induces an isomorphism $\eta\colon \mathcal{H} \to \mathcal{G}/\mathcal{G}'$. The group homomorphism

$$\xi\colon \phi(G)[1] \to \mathcal{H} \times \mathcal{H},\ (g_0, g_1) \mapsto \left(\overline{(g_0, g_1)}, \eta^{-1}(\overline{g_1})\right)$$

has image $\phi'(G)[1]$, because an element of $\phi'(G)[1]$ is of the form $\left(\overline{(g_0, g_1)}, \overline{(g_1, g_2)}\right) = \left(\overline{(g_0, g_1)}, \eta^{-1}(\overline{g_1})\right)$ with $(g_0, g_1, g_2) \in \phi(G)[2]$, i.e., $(g_0, g_1) \in \phi(G)[1]$ and $(g_1, g_2) \in \phi(G)[1]$ as $\phi(G)$ is 1-step. The kernel of ξ is $\mathcal{G}' \times (\mathcal{G}' \cap \mathcal{G}_1) = \mathcal{G}' \times 1$. It follows that $|\phi'(G)[1]| = \frac{|\phi(G)[1]|}{|\mathcal{G}'|}$ and so

$$|\ker(\phi'(G)[1] \to \phi'(G)[0])| = \frac{|\phi'(G)[1]|}{|\phi'(G)[0]|} = \frac{\frac{|\phi(G)[1]|}{|\mathcal{G}'|}}{\frac{|\phi(G)[1]|}{|\mathcal{G}'|\cdot|\mathcal{G}_1|}} = |\mathcal{G}_1| = \mathrm{ld}(G),$$

where the last equality above holds because $\phi \in \mathrm{Emb}(G)$. Since $\phi'(G)[0] = \mathcal{H}$ by construction, we see that $\phi' \in \mathrm{Emb}(G)$.

By the minimality of $|\mathcal{G}|$ we have $|\mathcal{H}| \geq |\mathcal{G}|$. But $\mathcal{H} \simeq \mathcal{G}/\mathcal{G}'$ and so we must have $\mathcal{G}' = 1$. By Lemma 4.1 the map $\phi(G)[1] \to \mathcal{G},\ (g_0, g_1) \mapsto g_1$ is surjective. As $\mathcal{G}' = 1$ it is an isomorphism. So $|\phi(G)[1]| = |\mathcal{G}|$. But also $|\phi(G)[0]| = |\mathcal{G}|$ and therefore

$$\mathrm{ld}(G) = |\mathcal{G}_1| = \frac{|\phi(G)[1]|}{|\phi(G)[0]|} = 1.$$

By Lemma 3.14 this contradicts the assumption that G is infinite. Thus $\mathcal{N} \neq 1$. Since $\mathcal{N} \times \mathcal{N} \subseteq \phi(G)[1]$ and $\phi(G)$ is 1-step, we see that $\mathcal{N}^{\mathbb{N}} \subseteq \phi(G)^{\mathbb{N}}$. □

The following corollary is a key step in our proof of the decomposition theorem.

Corollary 4.3. *Let G be an infinite σ-connected expansive profinite group such that for every normal expansive subgroup N of G we have $\mathrm{ld}(N) = 1$ or $\mathrm{ld}(N) = \mathrm{ld}(G)$. Then there exists an $\ell \in \mathbb{N}$ such that $G/\ker(\sigma^\ell)$ is isomorphic to a full one-sided group shift on a finite simple group.*

Proof. We continue to use the notation of the proof of Proposition 4.2. In particular, $\phi\colon G \to \mathcal{G}^{\mathbb{N}}$ is an element of $\mathrm{Emb}(G)$ such that $|\mathcal{G}|$ is minimal. We will show that ϕ is surjective and that $\mathcal{G}$ is simple.

In the proof of Proposition 4.2 we have seen that $\mathcal{N} = \mathcal{G}' \cap \mathcal{G}_1$ is non-trivial. As $\mathcal{N}^{\mathbb{N}} \subseteq \phi(G)$ maps to 1 under

$$\phi(G) \to \mathcal{H}^{\mathbb{N}},\ (g_0, g_1, \ldots) \mapsto \left(\overline{(g_i, g_{i+1})}\right)_{i\in\mathbb{N}},$$

we deduce that $\phi^{-1}(\mathcal{N}^{\mathbb{N}}) \subseteq \ker(\phi')$. In particular, $N = \ker(\phi')$ is infinite and therefore has limit degree strictly greater than 1 (Lemma 3.14). As N is a normal expansive subgroup of G we have, by assumption, $\mathrm{ld}(N) = \mathrm{ld}(G)$.

Thus $\mathrm{ld}(G/N) = 1$ and therefore $G/N \simeq \phi'(G)$ is finite (Lemma 3.14). Because G is σ-connected, also G/N is σ-connected (Lemma 3.26). So G/N is a finite σ-connected expansive profinite group and must therefore be σ-infinitesimal by Lemma 3.36. Thus there exists an $n \in \mathbb{N}$ such that $\sigma^n(\phi'(G)) = 1$, i.e., $(\phi(g)_i, \phi(g)_{i+1}) \in \mathcal{G}' \times \mathcal{G}_1$ for $i \geq n$. So $\phi(g)_i \in \mathcal{G}'$ and $\phi(g)_{i+1} \in \mathcal{G}_1$ for all $g \in G$ and $i \geq n$. On the other hand, by Lemma 4.1, we have $\{\phi(g)_i |\ g \in G\} = \mathcal{G}$ for every $i \in \mathbb{N}$. This shows that $\mathcal{G}' = \mathcal{G}$ and $\mathcal{G}_1 = \mathcal{G}$. But then $\phi(G)[1] = \mathcal{G} \times \mathcal{G}$ and $\phi(G)$ is the full one-sided group shift on $\mathcal{G}$. So $G/\ker(\phi) \simeq \mathcal{G}^{\mathbb{N}}$.

It remains to see that $\mathcal{G}$ is a simple group. Suppose $\mathcal{G}$ has a non-trivial proper normal subgroup $\mathcal{N}$. Then $\mathcal{N}^{\mathbb{N}}$ is a normal expansive subgroup of $\mathcal{G}^{\mathbb{N}}$ and $N = \phi^{-1}(\mathcal{N}^{\mathbb{N}})$ is a normal expansive subgroup of G. Since $N/\ker(\phi) \simeq \mathcal{N}^{\mathbb{N}}$ we have

$$\mathrm{ld}(N) = \frac{\mathrm{ld}(N)}{\mathrm{ld}(\ker(\phi))} = \mathrm{ld}(\mathcal{N}^{\mathbb{N}}) = |\mathcal{N}|$$

by Lemma 3.15 and Example 3.13. As $1 < |\mathcal{N}| < |\mathcal{G}| = \mathrm{ld}(G)$ we arrive at a contradiction. □

The following Corollary is a one-sided version of the Corollary to Theorem 2 in [Kit87].

Corollary 4.4. *Let G be a σ-connected expansive profinite group such that $p = \mathrm{ld}(G)$ is a prime number. Then there exists an $\ell \in \mathbb{N}$ such that $G/\ker(\sigma^\ell)$ is isomorphic to the full one-sided group shift on the finite cyclic group of order p.*

Proof. As the assumptions of Corollary 4.3 are met, there exists an $\ell \in \mathbb{N}$ such that $G/\ker(\sigma^\ell)$ is isomorphic to the full one-sided group shift on a finite simple group $\mathcal{G}$. Because $p = \mathrm{ld}(G) = \mathrm{ld}(G/\ker(\sigma^\ell) = \mathrm{ld}(\mathcal{G}^{\mathbb{N}}) = |\mathcal{G}|$, it follows that $\mathcal{G}$ is cyclic of order p. □

The following lemma will be useful for the induction step in the proof of the main decomposition theorem. Roughly speaking, it allows us to remove the top σ-infinitesimal quotient in a subnormal series.

Lemma 4.5. *Let G be an expansive profinite group with a subnormal series*

$$G \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{n+1}$$

such that G/G_1 is σ-infinitesimal, G_i/G_{i+1} is isomorphic to a full one-sided group shift on a finite simple group for $i = 1, \ldots n$ and G_{n+1} is σ-infinitesimal. Then there exists a subnormal series

$$G \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_n$$

such that G/H_1 and H_i/H_{i+1} $(i = 1, \ldots, n-1)$ are isomorphic to full one-sided group shifts on finite simple groups and H_n is σ-infinitesimal.

Proof. Since G/G_1 is σ-infinitesimal, there exists an $r \in \mathbb{N}$ such that $\sigma^r(g) = 1$ for all $g \in G/G_1$ (Lemma 3.35). In other words, $\sigma^{-r}(G_1) = G$. We claim that the subnormal series

$$G = \sigma^{-r}(G_1) \supseteq \sigma^{-r}(G_2) \supseteq \ldots \supseteq \sigma^{-r}(G_{n+1})$$

has the required properties. As σ is surjective on a full one-sided group shift we see that $\sigma^r \colon \sigma^{-r}(G_i) \to G_i/G_{i+1}$ is surjective and so $\sigma^{-r}(G_i)/\sigma^{-r}(G_{i+1})$ is isomorphic to G_i/G_{i+1} for $i = 1, \ldots, n$.

Finally, if $s \in \mathbb{N}$ is such that $\sigma^s(g) = 1$ for all $g \in G_{n+1}$, then $\sigma^{r+s}(g) = 1$ for all $g \in \sigma^{-r}(G_{n+1})$. Thus $\sigma^{-r}(G_{n+1})$ is σ-infinitesimal. □

Finally, we are prepared to prove our main result.

Theorem 4.6. *Let G be an expansive profinite group. Then there exists a subnormal series*

$$G \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n$$

such that $G_1 = G^{\sigma o}$, G_i/G_{i+1} is isomorphic to a full one-sided group shift on a finite simple group $\mathcal{G}_i$ for $i = 1, \dots, n-1$ and G_n is σ-infinitesimal. If

$$G \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_m$$

is another subnormal series such that $H_1 = G^{\sigma o}$, H_i/H_{i+1} is isomorphic to a full one-sided group shift on a finite simple group $\mathcal{H}_i$ for $i = 1, \dots, m-1$ and H_m is σ-infinitesimal, then $m = n$ and there exists a permutation π such that $\mathcal{G}_i$ is isomorphic to $\mathcal{H}_{\pi(i)}$ for $i = 1, \dots, n-1$.

Proof. We first establish the existence of the decomposition by induction on $\mathrm{ld}(G)$. If $\mathrm{ld}(G) = 1$, then G is finite (Lemma 3.14) and the theorem holds with $n = 1$ by Example 3.23.

So we may assume that $\mathrm{ld}(G) > 1$. Replacing G with $G^{\sigma o}$, we may also assume that G is σ-connected. (Note that by Lemma 3.27 the limit degree remains unchanged.) If there does not exist a normal expansive subgroup N of G such that $1 < \mathrm{ld}(N) < \mathrm{ld}(G)$, then there exists a decomposition of the desired form with $n = 2$ by Corollary 4.3.

So we may assume that there exists a normal expansive subgroup N of G such that $1 < \mathrm{ld}(N) < \mathrm{ld}(G)$. We know from Lemma 3.25 that also $N^{\sigma o}$ is a normal expansive subgroup of G. Moreover $\mathrm{ld}(N) = \mathrm{ld}(N^{\sigma o})$ by Lemma 3.27. Replacing N by $N^{\sigma o}$ we may thus assume that N is σ-connected.

Because $\mathrm{ld}(G/N) = \mathrm{ld}(G)/\mathrm{ld}(N) < \mathrm{ld}(G)$ we can apply the induction hypothesis to G/N. As G is σ-connected, also G/N is σ-connected (Lemma 3.26). So, using Proposition 3.7, we obtain a subnormal series

$$G/N \supseteq G_1/N \supseteq \cdots \supseteq G_n/N$$

for G/N, where $G \supseteq G_1 \supseteq \cdots \supseteq G_n \supseteq N$ is a subnormal series for G such that G_n/N is σ-infinitesimal and $(G_i/N)/(G_{i+1}/N) = G_i/G_{i+1}$ is isomorphic to a full one-sided group shift on a finite simple group for $i = 0, \dots, n-1$, where $G_0 := G$.

As $\mathrm{ld}(N) < \mathrm{ld}(G)$, we can also apply the induction hypothesis to N. Since N is σ-connected, we obtain a subnormal series

$$N \supseteq N_1 \supseteq \cdots \supseteq N_m,$$

with N_m σ-infinitesimal and N_i/N_{i+1} isomorphic to a full one-sided group shift on a finite simple group for $i = 0, \dots, m-1$ ($N_0 := N$). By Lemma 4.5, the subnormal series

$$G_n \supseteq N \supseteq N_1 \supseteq \cdots \supseteq N_m$$

can be replaced by a subnormal series

$$G_n \supseteq H_1 \supseteq \cdots \supseteq H_m,$$

with G_n/H_1 and H_i/H_{i+1} ($i = 1, \dots, m-1$) isomorphic to a full one-sided group shift on a finite simple group and H_m σ-infinitesimal. Then

$$G \supseteq G_1 \supseteq \cdots \supseteq G_n \supseteq H_1 \supseteq \cdots \supseteq H_m$$

is a subnormal series for G of the required form.

We next address the uniqueness: Assume that

$$G^{\sigma o} = G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n$$

and

$$G^{\sigma o} = H_1 \supseteq H_2 \supseteq \ldots \supseteq H_m$$

are subnormal series of $G^{\sigma o}$ such that G_i/G_{i+1} is isomorphic to a full one-sided group shift on a simple group $\mathcal{G}_i$ ($i = 1, \dots, n-1$), H_i/H_{i+1} is isomorphic to a full one-sided group shift on a finite simple group $\mathcal{H}_i$ ($i = 1, \dots, m-1$) and the groups G_n and H_m are σ-infinitesimal.

By Proposition 3.10 these two subnormal series for $G^{\sigma o}$ have equivalent refinements. Let

$$G_1 \supseteq G_{1,1} \supseteq G_{1,2} \supseteq \ldots \supseteq G_{1,n_1} = G_2 \supseteq \ldots \supseteq G_n \supseteq G_{n,1} \supseteq \ldots \supseteq G_{n,n_n} = 1 \tag{6}$$

and

$$H_1 \supseteq H_{1,1} \supseteq H_{1,2} \supseteq \ldots \supseteq H_{1,m_1} = H_2 \supseteq \ldots \supseteq H_m \supseteq H_{m,1} \supseteq \ldots \supseteq H_{m,m_m} = 1 \tag{7}$$

be such refinements. We may assume that all of the above inclusions are proper. Note that $G_{i,1}/G_{i+1}$ is a proper normal expansive subgroup of G_i/G_{i+1} for $i = 1, \ldots, n-1$. By Lemma 3.30 the group $G_{i,1}/G_{i+1}$ is finite. It follows that all the factor groups $G_{i,j}/G_{i,j+1}$ $(j = 1, \ldots, n_i - 1)$ are finite, whereas $G_i/G_{i,1}$ is infinite. Thus, the number of infinite factor groups of the subnormal series (6) is exactly $n-1$. Similarly, the number of infinite factor groups of the subnormal series (7) is $m-1$. Because the subnormal series (6) and (7) are equivalent, we see that $n = m$. Moreover, by Lemma 3.30 the $n-1$ infinite factor groups of (6) are isomorphic to full one-sided group shifts on the finite simple groups $\mathcal{G}_1, \ldots, \mathcal{G}_{n-1}$. Similarly, the $n-1 = m-1$ infinite factor groups of (7) are isomorphic to full one-sided group shifts on the finite simple groups $\mathcal{H}_1, \ldots, \mathcal{H}_{m-1}$. The equivalence of (6) and (7) together with Lemma 3.32 shows that there exists a permutation π such that $\mathcal{G}_i \simeq \mathcal{H}_{\pi(i)}$ for $i = 1, \ldots, n-1$. □

Remark 4.7. *For simplicity, Theorem 4.6 is stated in the introduction without reference to the σ-identitiy component and the claim concerning the uniqueness of the group G_1 made there needs some justification: Let $G \supseteq G_1 \supseteq \ldots \supseteq G_n$ be a subnormal series for an expansive profinite group G such that G_i/G_{i+1} is isomorphic to a full one-sided group shift on a finite simple group for $i = 1, \ldots, n-1$, G/G_1 is finite with $\sigma\colon G/G_1 \to G/G_1$ an automorphism and G_n is σ-infinitesimal. Then $G_1 = G^{\sigma o}$.*

Proof. Full one-sided group shifts and σ-infinitesimal expansive profinite groups are σ-connected. So it follows inductively, using Lemma 3.29, that all the G_i are σ-connected. In particular G_1 is σ-connected. Thus the claim follows from Lemma 3.28. □

We next consider some examples that illustrate Theorem 4.6. The following example shows that our decomposition theorem can be interpreted as a generalization of the classical Jordan-Hölder theorem.

Example 4.8. Let G be the full one-sided group shift on the finite group $\mathcal{G}$ and let $\mathcal{G} = \mathcal{G}_1 \supseteq \mathcal{G}_2 \supseteq \ldots \supseteq \mathcal{G}_n = 1$ be a decomposition series for $\mathcal{G}$. Then

$$G = \mathcal{G}_1^{\mathbb{N}} \supseteq \mathcal{G}_2^{\mathbb{N}} \supseteq \ldots \supseteq \mathcal{G}_n^{\mathbb{N}} = 1$$

is a subnormal series of G with the properties of Theorem 4.6. Note that G is σ-connected by Example 3.22.

Example 4.9. Let $\mathcal{G}$ be a finite simple group and let $\mathcal{G}'$ be any finite group containing $\mathcal{G}$. Then $G = \mathcal{G}' \times \mathcal{G} \times \mathcal{G} \times \ldots$ is an expansive profinite group under $\sigma\colon G \to G$, $(g', g_1, g_2, \ldots) \mapsto (g_1, g_2, \ldots)$. Moreover, G is σ-connected (e.g., by Lemma 3.20 (iii)) and $G_2 = \mathcal{G}' \times 1 \times 1 \ldots \leq G$ is a normal σ-infinitesimal expansive subgroup of G such that G/G_2 is isomorphic to the full one-sided group shift on $\mathcal{G}$. Thus $G = G_1 \supseteq G_2$ is a decomposition as in Theorem 4.6.

Example 4.10. This example is taken from [Kit87] (Example 4). However, we use a multiplicative notation, so that subgroups can easily be described by equations (rather than by listing elements). Let us write $\mathbb{G}_m = \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ for the multiplicative group of the complex numbers and consider $\mathbb{G}_m^{\mathbb{N}}$ as a group under componentwise multiplication. For $g = (g_0, g_1, \ldots) \in \mathbb{G}_m^{\mathbb{N}}$ we set $\sigma(g) = (g_1, g_2, \ldots)$ as usual. Let

$$G = \left\{ (g, h) \in (\mathbb{G}_m^2)^{\mathbb{N}} \mid g^4 = 1,\ h^2 = 1,\ \sigma(h) = g^2 h \right\}.$$

Then G is a subgroup of $\mathcal{G}^{\mathbb{N}}$, where $\mathcal{G} = \{a \in \mathbb{C}^\times \mid a^4 = 1\} \times \{b \in \mathbb{C}^\times \mid b^2 = 1\}$ is a product of a cyclic group of order four and a cyclic group of order two. Indeed G is a 1-step group shift

on $\mathcal{G}$. Set $G_2 = \{(g,h) \in G |\ h = 1\} = \{(g,1) \in \mathbb{G}_m |\ g^2 = 1\}$. So G_2 is a full one-sided group shift on a cyclic group of order two. The map $G \to \mathbb{G}_m^{\mathbb{N}},\ (g,h) \to h$ has kernel G_2 and image $\{h \in \mathbb{G}_m^{\mathbb{N}} |\ h^2 = 1\}$. Thus G/G_2 is isomorphic to a full one-sided group shift on a cyclic group of order two. So there exists a short exact sequence

$$1 \to C_2^{\mathbb{N}} \to G \to C_2^{\mathbb{N}} \to 1, \tag{8}$$

where C_2 is the cyclic group of order two. By Lemma 3.29 and Example 3.22 the expansive profinite group G is σ-connected. So

$$G = G_1 \supseteq G_2 \supseteq G_3 = 1$$

is a subnormal series as in Theorem 4.6. We note that the exact sequence (8) is not split. Indeed, G is not isomorphic to a full one-sided group shift ([Kit87, Example 4]).

Example 4.11. We use the same notation as in the previous example. Set

$$G = \left\{(g_1,g_2,g_3) \in (\mathbb{G}_m^3)^{\mathbb{N}} |\ g_1^4 = g_2^4 = g_3^2 = 1,\ \sigma(g_1) = g_2^2,\ \sigma(g_3) = g_3\right\}.$$

Then G is a one-sided group shift on the finite group $\mathcal{G}$, where $\mathcal{G}$ is a direct product of two cyclic groups of order four and a cyclic group of order two. Let G_1, G_2 and G_3 be the subgroups of G given by

$$G_1 = \left\{(g_1,g_2,1) \in (\mathbb{G}_m^3)^{\mathbb{N}} |\ g_1^4 = g_2^4 = 1,\ \sigma(g_1) = g_2^2,\right\},$$

$$G_2 = \left\{(g_1,g_2,1) \in (\mathbb{G}_m^3)^{\mathbb{N}} |\ g_1^4 = g_2^2 = 1,\ \sigma(g_1) = 1,\right\},$$

and

$$G_3 = \left\{(g_1,1,1) \in (\mathbb{G}_m^3)^{\mathbb{N}} |\ g_1^4 = 1,\ \sigma(g_1) = 1\right\}.$$

We will show that

$$G \supseteq G_1 \supseteq G_2 \supseteq G_3$$

is a subnormal series as in Theorem 4.6.

Clearly G_3 is σ-infinitesimal. The map $G_1 \to \mathbb{G}_m^{\mathbb{N}},\ (g_1,g_2,1) \mapsto g_2$ has kernel G_3 and image $\{g \in \mathbb{G}_m^{\mathbb{N}} |\ g^4 = 1\}$, a full one-sided group shift on a cyclic group of order four. The full one-sided group shift $\{g \in \mathbb{G}_m^{\mathbb{N}} |\ g^2 = 1\}$ contained in the image corresponds to G_2. So G_1/G_2 and G_2/G_3 are both full one-sided group shifts on a cyclic group of order two.

So it only remains to show that $G_1 = G^{\sigma o}$. As in Remark 4.7 it follows that G_1 is σ-connected. According to Lemma 3.28 it suffices to show that G/G_1 is finite with $\sigma\colon G/G_1 \to G/G_1$ bijective. But G/G_1 is a group of order two with σ the identity map.

5. Topological conjugacy

Recall that two topological spaces (X,σ) and (Y,σ) equipped with continuous endomorphisms are *topologically conjugate* if there exists a homeomorphism $X \to Y$ such that

$$\begin{array}{ccc} X & \longrightarrow & Y \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ X & \longrightarrow & Y \end{array}$$

commutes. In [Kit87] B. Kitchens showed that every profinite group equipped with an expansive *automorphism* is topologically conjugate to $\mathcal{A}^{\mathbb{Z}} \times \mathcal{F}$, a full two-sided shift on a finite set $\mathcal{A}$ times a finite (discrete) set $\mathcal{F}$ equipped with an automorphism.

We establish here a similar result for expansive *endomorphisms*: If G is an expansive profinite group, then there exists an $\ell \in \mathbb{N}$ such that $\sigma^\ell(G)$ is topologically conjugate to $\mathcal{A}^{\mathbb{N}} \times \mathcal{F}$, a full one-sided shift on a finite set $\mathcal{A}$ times a finite set $\mathcal{F}$ equipped with an automorphism. We will need the following preparatory lemma.

Lemma 5.1. *Let G be an expansive profinite group and N a normal expansive subgroup of G that is isomorphic to a full one-sided group shift. Then G is topologically conjugate to $G/N \times N$.*

Proof. To be clear, the topology on $G/N \times N$ is the product topology and the endomorphism σ on $G/N \times N$ sends $(h, n) \in G/N \times N$ to $(\sigma(h), \sigma(n))$.

To begin with, choose a continuous section φ of the canonical map $\pi\colon G \to G/N$, i.e., a continuous map $\varphi\colon G/N \to G$ such that $\pi\varphi = \mathrm{id}_{G/N}$. Such a map always exists by [RZ10, Proposition 2.2.2]. (Note that we do not require that φ commutes with σ or is a group homomorphism.) The map $\eta\colon G/N \times N \to G,\ (h, n) \mapsto \varphi(h)n$ is a homeomorphism with inverse $\eta^{-1}\colon G \to G/N \times N,\ g \mapsto (\pi(g), \varphi(\pi(g))^{-1}g)$. For $(h, n) \in G/N \times N$ we have

$$\eta^{-1}(\sigma(\eta(h, n))) = \eta^{-1}(\sigma(\varphi(h))\sigma(n)) = (\sigma(\pi(\varphi(h)), \varphi(\pi(\sigma(\varphi(h))\sigma(n)))^{-1}\sigma(\varphi(h))\sigma(n)) =$$
$$= (\sigma(h), \varphi(\sigma(h))^{-1}\sigma(\varphi(h))\sigma(n)).$$

Thus G is topologically conjugate to $(G/N \times N, \sigma')$ with $\sigma'\colon G/N \times N \to G/N \times N$ given by $\sigma'(h, n) = (\sigma(h), \psi(h)\sigma(n))$, where $\psi\colon G/N \to N,\ h \mapsto \varphi(\sigma(h))^{-1}\sigma(\varphi(h))$.

So it suffices to show that $(G/N \times N, \sigma')$ and $(G/N \times N, \sigma)$ are topologically conjugate. We may assume that $N = \mathcal{N}^{\mathbb{N}}$ for some finite group $\mathcal{N}$. So for $h \in G/N$ the element $\psi(h) = (\psi(h)_i)_{i\in\mathbb{N}}$ is a sequence in $\mathcal{N}$. Define a continuous map $\alpha\colon G/N \to N = \mathcal{N}^{\mathbb{N}}$ by $\alpha(h)_0 = 1$ and $\alpha(h)_i = \psi(h)_{i-1}^{-1}\psi(\sigma(h))_{i-2}^{-1}\dots\psi(\sigma^{i-1}(h))_0^{-1}$ for $i \geq 1$. Then $\psi(h)_i\alpha(h)_{i+1} = \alpha(\sigma(h))_i$ for all $i \in \mathbb{N}$, i.e., $\psi(h)\sigma(\alpha(h)) = \alpha(\sigma(h))$ for all $h \in G/N$.

The map $\xi\colon G/N \times N \to G/N \times N,\ (h, n) \mapsto (h, \alpha(h)n)$ is a homeomorphism and

$$\xi(\sigma(h, n)) = (\sigma(h), \alpha(\sigma(h))\sigma(n)) = (\sigma(h), \psi(h)\sigma(\alpha(h))\sigma(n)) = \sigma'(h, \alpha(h)n) = \sigma'(\xi(h, n))$$

for all $(h, n) \in G/N \times N$. Thus ξ is a conjugacy between $(G/N \times N, \sigma)$ and $(G/N \times N, \sigma')$. □

Let G be an expansive profinite group. Note that for $\ell \in \mathbb{N}$, the kernel $\ker(\sigma^\ell)$ of $\sigma^\ell\colon G \to G$ is a σ-infinitesimal expansive subgroup of G. In particular, $\ker(\sigma^\ell)$ is finite. Moreover $\sigma^\ell(G)$ is an expansive subgroup of G and σ^ℓ induces an isomorphism $G/\ker(\sigma^\ell) \to \sigma^\ell(G)$ of expansive profinite groups.

Theorem 5.2. *Let G be an expansive profinite group. Then there exists an $\ell \in \mathbb{N}$ such that $\sigma^\ell(G)$ is topologically conjugate to $\mathcal{A}^{\mathbb{N}} \times \mathcal{F}$, where $\mathcal{A}$ is a finite set and $\mathcal{F}$ is a finite set equipped with a bijective map $\sigma\colon \mathcal{F} \to \mathcal{F}$ having a fixed point.*

Proof. We will prove the theorem by induction on $\mathrm{ld}(G)$. If $\mathrm{ld}(G) = 1$, then G is finite (Lemma 3.14) and for large enough ℓ, the map $\sigma\colon \sigma^\ell(G) \to \sigma^\ell(G)$ is bijective. Thus the theorem holds with $\mathcal{A}$ a one-element set and $\mathcal{F} = \sigma^\ell(G)$. (The identity element $1 \in \mathcal{F}$ is a fixed point.)

Assume that $\mathrm{ld}(G) > 1$. By Proposition 4.2 there exists an $\ell \in \mathbb{N}$ and a normal expansive subgroup N of $\sigma^\ell(G)$ such that N is isomorphic to a full one-sided group shift on a non-trivial finite group. From Lemma 5.1 we obtain that $\sigma^\ell(G)$ is topologically conjugate to $\sigma^\ell(G)/N \times N$. We have $\mathrm{ld}(\sigma^\ell(G)/N) = \frac{\mathrm{ld}(\sigma^\ell(G))}{\mathrm{ld}(N)} < \mathrm{ld}(G)$ and so we can apply the induction hypothesis to $G' = \sigma^\ell(G)/N$: There exists an $\ell' \in \mathbb{N}$, a finite set $\mathcal{A}'$ and a finite set $\mathcal{F}'$ equipped with an automorphism having a fixed point such that $\sigma^{\ell'}(G')$ is topologically conjugate to $\mathcal{A}'^{\mathbb{N}} \times \mathcal{F}'$.

Since $\sigma^\ell(G)$ is topologically conjugate to $G' \times N$, we see that $\sigma^{\ell+\ell'}(G)$ is topologically conjugate to $\sigma^{\ell'}(G' \times N) = \sigma^{\ell'}(G') \times \sigma^{\ell'}(N) \simeq \mathcal{A}'^{\mathbb{N}} \times \mathcal{F}' \times N$. So, if $N \simeq \mathcal{N}^{\mathbb{N}}$, then $\sigma^{\ell+\ell'}(G)$ is topologically conjugate to $(\mathcal{A}' \times \mathcal{N})^{\mathbb{N}} \times \mathcal{F}'$. □

Note that a full one-sided group shift is σ-connected and has a surjective σ. The following corollary provides a converse for expansive profinite groups:

Corollary 5.3. *Let G be a σ-connected expansive profinite group with $\sigma\colon G \to G$ surjective. Then G is topologically conjugate to a full one-sided shift.*

Proof. Since $\sigma\colon G \to G$ is surjective, it follows from Theorem 5.2 that G is topologically conjugate to $\mathcal{A}^{\mathbb{N}} \times \mathcal{F}$. Let $f \in \mathcal{F}$ be a fixed point. Then $\mathcal{A} \times \mathcal{F}$ is the disjoint union of the σ-closed sets $\mathcal{A} \times \{f\}$ and $\mathcal{A} \times (\mathcal{F} \smallsetminus \{f\})$. As G is σ-connected, we must have $\mathcal{F} = \{f\}$. Thus G is topologically conjugate to $\mathcal{A}^{\mathbb{N}}$. □

Because full one-sided shifts are σ-irreducible, Corollary 5.3 implies that a σ-connected expansive profinite group G with $\sigma\colon G \to G$ surjective is σ-irreducible.

6. Expansive automorphisms

In this section we establish an analog of Theorem 4.6 for expansive automorphisms in place of expansive endomorphisms. There are no immediate implications between results about profinite groups equipped with an expansive endomorphism and results about profinite groups equipped with an expansive automorphism. Indeed, if G is a profinite group and $\sigma\colon G \to G$ is a map that is simultaneously an expansive endomorphism and an expansive automorphism, then G is finite by Corollary 3.17. However, it seems possible to obtain a proof of an analog of Theorem 4.6 for expansive automorphisms by carefully going through all the steps of the proof of Theorem 4.6 and performing some minor modifications here and there. Indeed, the situation is simpler in the automorphism setting because there are no σ-infinitesimal groups in this context.

There is, however, a slightly more elegant path that we will follow here. There is a universal construction $G \rightsquigarrow G^*$ that associates to any profinite group G equipped with an expansive endomorphism, a profinite group G^* equipped with an expansive automorphism. Moreover, any profinite group equipped with an expansive automorphism is of the form G^* for some G. In this fashion, results about profinite groups with expansive endomorphisms can be transformed to results about profinite groups with expansive automorphisms. This way we are able to avoid having to enter into the details of the proof of the existence part of Theorem 4.6 again.

We begin by recalling the two-sided setup in symbolic dynamics. See [Kit98] or [LM95]. Let $\mathcal{A}$ be a finite set. We consider $\mathcal{A}^{\mathbb{Z}}$ as a topological space via the product topology of the discrete topology on $\mathcal{A}$. The topological space $\mathcal{A}^{\mathbb{Z}}$ together with the homeomorphism $\sigma\colon \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$, given by $\sigma(a_{n\in\mathbb{Z}}) = (a_{n+1})_{n\in\mathbb{Z}}$ is the *full two-sided shift* on the alphabet $\mathcal{A}$. A *two-sided shift* on $\mathcal{A}$ is a closed subset X of $\mathcal{A}^{\mathbb{Z}}$ such that $\sigma(X) = X$. A *word* or *block* of length i is a sequence of i elements from $\mathcal{A}$. A two-sided shift X on $\mathcal{A}$ is a (two-sided) *subshift of finite type* if there exists a finite set $\mathcal{F}$ of blocks such that X consists of all elements of $\mathcal{A}^{\mathbb{Z}}$ that do not contain any blocks from $\mathcal{F}$. If Γ is a directed graph with set of vertices equal to $\mathcal{A}$, then the set $X_\Gamma^* \subseteq \mathcal{A}^{\mathbb{Z}}$ consisting of all biinfinite sequences in $\mathcal{A}$ that trace out a biinfinite directed path in Γ is a subshift of finite type.

In case the alphabet $\mathcal{A} = \mathcal{G}$ is a finite group, $\mathcal{G}^{\mathbb{Z}}$ inherits a group structure. In fact, $\mathcal{G}^{\mathbb{Z}}$ is a profinite group and $\sigma\colon \mathcal{G}^{\mathbb{Z}} \to \mathcal{G}^{\mathbb{Z}}$ is an automorphism (of profinite groups). A *two-sided group shift* G on $\mathcal{G}$ is a two-sided shift on $\mathcal{G}$ that is a subgroup of $\mathcal{G}^{\mathbb{Z}}$. In particular, G is a profinite group and $\sigma\colon G \to G$ is an autmorphism. It is shown in [Kit87] that every two-sided group shift is a subshift of finite type. If Γ is a directed group graph on a finite group $\mathcal{G}$, then $G_\Gamma^* = X_\Gamma^*$ is a two-sided group shift.

In this section we consider expansive endomorphisms and expansive automorphisms of profinite groups. To have a clear notational distinction between the two, we add a "$*$" to the notation whenever we are dealing with expansive automorphisms. We continue to use the notation of the previous sections. In particular, an expansive profinite group is a profinite group together with an expansive endomorphism (Definition 3.1).

Definition 6.1. *An automorphism $\sigma\colon G \to G$ of a profinite group G is an* expansive automorphism *if there exists a neighborhood U of 1 such that $\cap_{n\in\mathbb{Z}}\sigma^n(U) = 1$. A* $*$expansive profinite group *is a profinite group G together with an expansive automorphism $\sigma\colon G \to G$.*

As for expansive profinite groups, once can assume that U is an open normal subgroup of G. The study of $*$expansive profinite groups was initiated by B. Kitchens in [Kit87].

A *topological σ-group* is a topological group G equipped with an endomorphism (i.e., a continuous group homomorphism) $\sigma\colon G \to G$. A morphism $G \to H$ of topological σ-groups is a continuous group homomorphism such that

$$\begin{array}{ccc} G & \longrightarrow & H \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ G & \longrightarrow & H \end{array}$$

commutes. A morphism of $*$expansive profinite groups is a morphism of topological σ-groups.

We will need the $*$-analogs of the elementary results from Section 3.2. The proofs are very similar to Section 3.2. We therefore omit the details.

Lemma 6.2. *Let G be a $*$expansive profinite group.*

(i) *If H is a closed subgroup of G such that $\sigma(H) = H$, then H (with the induced topology and automorphism) is a $*$expansive profinite group. In this case, we call H a $*$expansive subgroup of G.*

(ii) *If N is a normal $*$expansive subgroup of G, then G/N (with the quotient topology and induced automorphism) is a $*$expansive profinite group and the canonical map $G \to G/N$ is a morphism of $*$expansive profinite groups.*

We note that point (ii) of Lemma 6.2 is proved in far greater generality in [GR17].

Proposition 6.3 (Isomorphism theorems for $*$expansive profinite groups)**.**

(i) *Let $\phi\colon G \to H$ be a morphism of $*$expansive profinite groups. Then $\phi(G)$ is a $*$expansive subgroup of H, $\ker(\phi)$ is a normal $*$expansive subgroup of G and the canonical map $G/\ker(\phi) \to \phi(G)$ is an isomorphism of $*$expansive profinite groups.*

(ii) *Let N be a normal $*$expansive subgroup of a $*$expansive group G and $\pi\colon G \to G/N$ the canonical map. Then the map*

$$\{*\text{expansive subgroups of } G \text{ containing } N\} \longrightarrow \{*\text{expansive subgroups of } G/N\},$$

$H \mapsto \pi(H) = H/N$ is a bijection with inverse $H' \mapsto \pi^{-1}(H')$. Moreover H is normal in G if and only if H/N is normal in G/N and in that case $G/H \simeq (G/N)/(H/N)$.

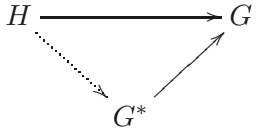
(iii) *Let H and N be $*$expansive subgroups of a $*$expansive profinite group G such that H normalizes N. Then HN is an $*$expansive subgroup of G, $H \cap N$ is a normal $*$expansive subgroup of H and $HN/N \simeq H/H \cap N$.*

Subnormal series, their refinements and equivalence of subnormal series for $*$expansive profinite groups are defined as for expansive profinite groups.

Proposition 6.4. *Any two subnormal series of a $*$expansive profinite group have equivalent refinements.*

The following proposition allows us to associate a $*$expansive profinite group G^* to any expansive profinite group G.

Proposition 6.5. *Let G be an expansive profinite group. There exists a $*$expansive profinite group G^* together with a morphism $G^* \to G$ of topological σ-groups satisfying the following universal property: If H is a $*$expansive profinite group and $H \to G$ is a morphism of topological σ-groups, then there exists a unique morphism $H \to G^*$ such that*



commutes.

Proof. For $i \in \mathbb{N}$ let G_i be a copy of G and consider the projective system $(G_i,\ \phi_{i+1})_{i\in\mathbb{N}}$, where the connection maps $\phi_{i+1}\colon G_{i+1} \to G_i$ are all equal to $\sigma\colon G \to G$. Let G^* be the projective limit of this projective system. Explicitly, we have

$$G^* = \left\{(g_0, g_1, g_2, \ldots) \in G^{\mathbb{N}} \middle|\ \sigma(g_{i+1}) = g_i\ \forall\ i \in \mathbb{N}\right\}.$$

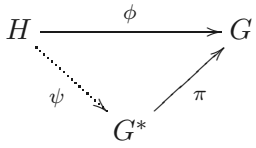
Define $\sigma\colon G^* \to G^*$ by $\sigma(g_0, g_1 \ldots) = (\sigma(g_0), \sigma(g_1), \ldots)$. Then $\sigma\colon G^* \to G^*$ is continuous because the maps $G^* \to G$, $(g_0, g_1, \ldots) \mapsto \sigma(g_i)$ are continuous for every $i \in \mathbb{N}$. If $g^* = (g_0, g_1, \ldots)$ lies in the kernel of $\sigma\colon G^* \to G^*$, then $\sigma(g_i) = 1$ for all $i \in \mathbb{N}$. But $\sigma(g_i) = g_{i-1}$ for $i \geq 1$. So $g^* = 1$ and σ is injective. On the other hand, if $g^* = (g_0, g_1, \ldots) \in G^*$, then $\sigma((g_1, g_2, \ldots)) = g^*$, so $\sigma\colon G^* \to G^*$ is surjective. A bijective morphism of profinite groups is an automorphism because any surjective morphism of profinite groups is open ([FJ08, Remark 1.2.1 (f)]). Thus $\sigma\colon G^* \to G^*$ is an automorphism.

The projection $\pi\colon G^* \to G$, $(g_0, g_1, \ldots) \mapsto g_0$ is a morphism of topological σ-groups. Let U be an open subgroup of G such that $\cap_{n\in\mathbb{N}}\sigma^{-n}(U) = 1$. Set $U^* = \pi^{-1}(U)$. We claim that $\cap_{n\in\mathbb{Z}}\sigma^n(U^*) = 1$. Assume that $g^* = (g_0, g_1, \ldots) \in \cap_{n\in\mathbb{Z}}\sigma^n(U^*)$. Let $n, i \in \mathbb{N}$. As $g^* \in \sigma^{i-n}(U^*)$, we see that

$$\sigma^{n-i}(g^*) = \sigma^n(g_i, g_{i+1}, \ldots) = (\sigma^n(g_i), \sigma^n(g_{i+1}), \ldots)$$

lies in U^*, i.e., $\sigma^n(g_i) \in U$. So $g_i \in \sigma^{-n}(U)$ for all $n \in \mathbb{N}$. Thus $g_i = 1$ for all $i \in \mathbb{N}$ and $g^* = 1$ as desired. Therefore G^* is a $*$expansive profinite group.

Let H be a $*$expansive profinite group and $\phi\colon H \to G$ a morphism of profinite σ-groups. Define $\psi\colon H \to G^*$ by $\psi(h) = (\phi(h), \phi(\sigma^{-1}(h)), \phi(\sigma^{-2}(h)), \ldots)$. Then ψ is a morphism of topological σ-group such that



commutes. Indeed, ψ is the only such morphism, because any other morphism $\psi'\colon H \to G^*$ with this property satisfies $\pi(\sigma^{-i}(\psi'(h))) = \pi(\psi'(\sigma^{-i}(h))) = \phi(\sigma^{-i}(h))$ for all $i \in \mathbb{N}$. □

Example 6.6. If $G = \mathcal{G}^{\mathbb{N}}$ is the full one-sided group shift on a finite group $\mathcal{G}$, then $G^* = \mathcal{G}^{\mathbb{Z}}$ is the full two-sided group shift on $\mathcal{G}$ and $G^* \to G$, $(g_n)_{n\in\mathbb{Z}} \mapsto (g_n)_{n\in\mathbb{N}}$ is the projection.

The following example generalizes Example 6.6.

Example 6.7. Let Γ be a directed group graph on the finite group $\mathcal{G}$. Then $(G_\Gamma)^* = G_\Gamma^*$. (Recall that G_Γ is defined after Definition 2.5 and G_Γ^* is defined before Definition 6.1.)

Proof. We have a natural map $\pi\colon G_\Gamma^* \to G_\Gamma$ that associates to the vertices of a biinfinite directed path the vertices of the infinite directed subpath starting at the vertex in position zero. Let H be a $*$expansive profinite group and $\phi\colon H \to G_\Gamma$ a morphism of topological σ-groups. For every $h \in H$, the first vertex of the path corresponding to $\phi(\sigma^{-1}(h))$ extends the path corresponding to $\phi(h)$ one step further to the left, similarly for σ^{-n} in place of σ^{-1}. So we see that there exists a unique $g = \psi(h) \in G_\Gamma^*$ such that $\phi(\sigma^{-n}(h)) = \pi(\sigma^{-n}(g))$ for all $n \in \mathbb{N}$. □

Corollary 6.8. *Every $*$expansive profinite group H is of the form $H = G^*$ for some expansive profinite group G.*

Proof. By [Kit87, Theorem 1, (i)] every $*$expansive profinite group H is isomorphic to G_Γ^* for some directed group graph Γ. By Example 6.7 we can thus take $G = G_\Gamma$. □

Example 6.9. Let G be a σ-infinitesimal expansive profinite group. Then $G^* = 1$. Indeed, any morphism $\phi\colon H \to G$ with H a $*$expansive profinite group satisfies $\phi(H) = 1$.

Proof. By Lemma 3.35 there exists an $n \in \mathbb{N}$ such that $\sigma^n(g) = 1$ for all $g \in G$. If $h \in H$ then we can write $h = \sigma^n(h')$ for some $h' \in H$ and then $\phi(h) = \sigma^n(\phi(h')) = 1$. □

Example 6.10. If G is a finite (discrete) group with an endomorphism $\sigma\colon G \to G$, then $G^* = \cap_{n\in\mathbb{N}}\sigma^n(G)$. In particular, if $\sigma\colon G \to G$ is an automorphism, then $G^* = G$.

Lemma 6.11. *If H is an expansive subgroup of an expansive profinite group G, then H^* is a $*$expansive subgroup of G^*. Moreover, if H is normal in G, then H^* is normal in G^* and $G^*/H^* \simeq (G/H)^*$.*

Proof. Clearly $H^* = \{(h_0, h_1, \ldots) \in H^{\mathbb{N}} |\ \sigma(h_{i+1}) = h_i\ \forall\ i \in \mathbb{N}\}$ is a $*$expansive subgroup of $G^* = \{(g_0, g_1, \ldots) \in G^{\mathbb{N}} |\ \sigma(g_{i+1}) = g_i\ \forall\ i \in \mathbb{N}\}$. If H is normal in G, then H^* is normal in G^*. The map $G^*/H^* \to (G/H)^*$, $\overline{(g_0, g_1, \ldots)} \mapsto (\overline{g_0}, \overline{g_1}, \ldots)$ is an isomorphism. □

We will also need a $*$version of Lemma 3.30.

Lemma 6.12. *Let $\mathcal{G}$ be a finite simple group and $G = \mathcal{G}^{\mathbb{Z}}$ the full two-sided group shift on $\mathcal{G}$. Let N be a proper $*$expansive subgroup of G.*

(i) *If $\mathcal{G}$ is non-commutative, then N is trivial.*
(ii) *If $\mathcal{G}$ is commutative, then N is finite and G/N is isomorphic to G.*

So, in either case, N is finite and G/N is isomorphic to G.

Proof. For $i \in \mathbb{N}$ let $N[i]$ denote the image of N under the projection $\mathcal{G}^{\mathbb{Z}} \to \mathcal{G}^{i+1}$, $(g_n)_{n\in\mathbb{N}} \mapsto (g_0, \ldots, g_i)$. In other words, $N[i]$ is the subgroup of $\mathcal{G}^{i+1}$ consisting of all blocks of length $i+1$ that occur in elements of N. As N is normal in G, we see that $N[i]$ is normal in $\mathcal{G}^{i+1}$. Moreover, since N is a proper subgroup of G, there must exist an $i \in \mathbb{N}$ such that $N[i]$ is a proper subgroup of $\mathcal{G}^{i+1}$.

We first treat the case that $\mathcal{G}$ is non-commutative. Then, as explained in the proof of Lemma 3.30, the group $N[i]$ is an $i+1$-fold product, where each factor is either 1 or $\mathcal{G}$. In particular, one of the factors, say, the j-th factor, has to be 1. This means that every block of length $i+1$ that occurs in an element of N has a 1 in its j-th position. But every entry of an element of N is the j-th entry of some block of length $i+1$, so $N = 1$.

We next treat the commutative case. So $\mathcal{G}$ is cyclic of prime order. For every $i \geq 1$ the kernel of the projection $N[i] \to N[i-1]$, $(g_0, \ldots, g_i) \mapsto (g_0, \ldots, g_{i-1})$ is of the form $\{1\}^i \times \mathcal{N}_i$ for some subgroup $\mathcal{N}_i$ of $\mathcal{G}$, i.e., $\mathcal{N}_i = 1$ ore $\mathcal{N}_i = \mathcal{G}$. Set $\mathcal{N}_0 = N[0]$. There exists an $n \in \mathbb{N}$ such that $\mathcal{N}_0, \ldots, \mathcal{N}_{n-1}$ are all equal to $\mathcal{G}$ and $\mathcal{N}_n, \mathcal{N}_{n+1}, \ldots$ are all trivial. So $N[i] = |\mathcal{G}|^n$ for all $i \geq n-1$. It follows that $|N| = |\mathcal{G}|^n$, in particular, N is finite. The group $\mathcal{G}^{n+1}/N[n]$ is isomorphic to $\mathcal{G}$ because it has the same order. The map $G \to (\mathcal{G}^{n+1}/N[n])^{\mathbb{Z}}$, $(g_m)_{m\in\mathbb{Z}} \mapsto (\overline{(g_m, g_{m+1}, \ldots, g_{m+n})})_{m\in\mathbb{Z}}$ has kernel N and thus induces an isomorphism $G/N \simeq \mathcal{G}^{\mathbb{Z}}$. □

We are now prepared to establish the $*$version of Theorem 4.6.

Theorem 6.13. *Let G be a $*$expansive profinite group. Then there exists a subnormal series*

$$G \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = 1$$

of $*$expansive subgroups G_i of G such that G/G_1 is a finite group and G_i/G_{i+1} is isomorphic to a full two-sided group shift on a finite simple group $\mathcal{G}_i$ for $i = 1, \ldots, n-1$. Moreover, the length n of such a series and the isomorphism classes of the finite simple groups $\mathcal{G}_i$ are uniquely determined by G.

Proof. We know from Corollary 6.8 that G is of the form $G = H^*$ for some expansive profinite group H. Let

$$H \supseteq H_1 \supseteq \ldots \supseteq H_n$$

be a subnormal series for H as in Theorem 4.6. For $i = 1, \dots, n$ set $G_i = H_i^*$. By Lemma 6.11 we have a subnormal series

$$G \supseteq G_1 \supseteq \dots \supseteq G_n \tag{9}$$

of $*$expansive subgroup for $G = H^*$. As H/H_1 is finite and $\sigma\colon H/H_1 \to H/H_1$ is bijective (Lemma 3.20 (ii)) we see, using Lemma 6.11 and Example 6.10, that $G/G_1 = H^*/H_1^* = (H/H_1)^* = H/H_1$ is finite. It follows from Example 6.6 that $G_i/G_{i+1} = H_i^*/H_{i+1}^* = (H_i/H_{i+1})^*$ is isomorphic to a full two-sided group shift on a finite simple group $\mathcal{G}_i$ for $i = 1, \dots, n-1$. Moreover, by Example 6.9 we have $G_n = H_n^* = 1$. So the subnormal series (9) has all the required properties.

The proof of the uniqueness claim is similar to the proof in Theorem 4.6. Assume we have another subnormal series

$$G \supseteq H_1 \supseteq \dots \supseteq H_m = 1$$

as in the theorem and let $\mathcal{H}_1 \dots, \mathcal{H}_{m-1}$ denote the corresponding finite simple groups. According to Proposition 6.4, we can find equivalent refinements. Using Lemma 6.12 we see that the number of infinite factor groups in a refinement equals $n-1$ respectively $m-1$. Because the refinements are equivalent, we must have $m = n$. Using Lemma 6.12 again, we see that there exists a permutation π such that $\mathcal{G}_i^{\mathbb{Z}}$ is isomorphic to $\mathcal{H}_{\pi(i)}^{\mathbb{Z}}$. But then $\mathcal{G}_i \simeq \mathcal{H}_i$ ([Kit87, Proposition 7]). □

7. Babbitt's decomposition

Babbitt's decomposition theorem is an important classical theorem in difference algebra that elucidates the structure of algebraic difference field extensions. See [Coh65, Chapter 7, Theorem 7], [Lev08, Theorem 5.4.13] or [Bab62, Theorem 2.3] for the original reference.

In this section we explain how our main result (Theorem 4.6) implies Babbitt's decomposition theorem and indeed yields additional information concerning the uniqueness of the decomposition.

To state Babbitt's decomposition theorem we need to recall some basic notation from difference algebra. See [Coh65] or [Lev08]. A *difference field*, or *σ-field* for short, is a field K equipped with an endomorphism $\sigma\colon K \to K$. An extension L/K of difference fields is an extension of fields such that $\sigma\colon L \to L$ extends $\sigma\colon K \to K$. An *intermediate σ-field* of a σ-field extension L/K is a subfield M of L containing K such that $\sigma(M) \subseteq M$. If L/K is an extension of σ-fields and A a subset of L, then $K\langle A\rangle \subseteq L$ denotes the smallest intermediate σ-field of L/K that contains A. Note that $K\langle A\rangle = K(A, \sigma(A), \sigma^2(A) \dots)$, the field extension of K generated by $A, \sigma(A), \dots$. If $L = K\langle A\rangle$ for a finite set A, then L/K is called *finitely σ-generated*.

A σ-field extension L/K is Galois if the underlying field extension is Galois, i.e., normal and separable. (So the field extension is algebraic but not necessarily finite.) The following lemma explains the connection between extensions of difference fields and expansive profinite groups. See [Lev08, Section 8.1] for related results in a slightly different context. (In [Lev08, Section 8.1] it is always assumed that $\sigma\colon K \to K$ is an automorphism.)

Lemma 7.1. *Let L/K be a Galois extension of σ-fields and let $G = G(L/K)$ be the Galois group (of the underlying field extension).*

(i) *For every $g \in G$ there exists a unique $g^\sigma \in G$ such that $\sigma g^\sigma = g\sigma$ as maps from L to L.*
(ii) *The map $\sigma\colon G \to G$, $g \mapsto g^\sigma$ is a continuous group homomorphism.*
(iii) *The extension L/K is finitely σ-generated if and only if G is an expansive profinite group.*

Proof. In [TW18, Lemma 1.23] it is shown that for any two extensions $\sigma_1, \sigma_2\colon L \to L$ of $\sigma\colon K \to K$, there exists a unique element $\tau \in G$ such that $\sigma_2 = \sigma_1\tau$. Applying this with $\sigma_1 = \sigma\colon L \to L$ and $\sigma_2 = g\sigma\colon L \to L$ yields (i).

A basis for the topology of G is given by the open subgroups

$$U_A = \{g \in G |\ g(a) = a\ \forall\ a \in A\},$$

where A is a finite subset of L. For $a \in L$ and $g \in G$ we have $\sigma(g)(a) = a$ if and only if $\sigma(\sigma(g)(a)) = \sigma(a)$ because $\sigma\colon L \to L$ is injective. But $\sigma(\sigma(g)(a)) = g(\sigma(a))$ by definition of $\sigma\colon G \to G$. It follows that $\sigma^{-1}(U_A) = U_{\sigma(A)}$. Therefore $\sigma\colon G \to G$ is continuous. A straight forward calculations shows that $\sigma\colon G \to G$ is a group homomorphism.

To establish (iii), assume first that A is a finite subset of L such that $L = K\langle A\rangle$. We claim that $\cap_{n\in\mathbb{N}}\sigma^{-n}(U_A) = 1$. Indeed, if $g \in \cap_{n\in\mathbb{N}}\sigma^{-n}(U_A)$, then $g \in \sigma^{-n}(U_A) = U_{\sigma^n(A)}$ for all $n \in \mathbb{N}$. So g fixes all elements in $A, \sigma(A), \sigma^2(A), \ldots$. Since these generate L as a field extension of K, we see that g fixes all elements of L. Thus $g = 1$ and G is an expansive profinite group.

Conversely, assume that U is an open subgroup of G such that $\cap_{n\in\mathbb{N}}\sigma^{-n}(U) = 1$. Then L^U is a finite field extension of K and therefore of the form $L^U = K(A)$ for a finite subset A of L. In other words, $U = U_A$. As $L/K(A, \sigma(A), \ldots)$ has Galois group $\cap_{n\in\mathbb{N}}\sigma^{-n}(U) = 1$, we must have $L = K\langle A\rangle$. □

To state Babbitt's decomposition theorem we need some more notation from difference algebra. An extension L/K of σ-fields is *σ-separable* if $\sigma\colon L \otimes_K K' \to L \otimes_K K',\ a \otimes b \mapsto \sigma(a) \otimes \sigma(b)$ is injective for any σ-field extension K'/K. For other equivalent characterizations of this notion see [TW18, Section 1.1].

Let L/K be a finitely σ-generated Galois extension of σ-fields and let $\pi_0^\sigma(L/K)$ denote the union of all intermediate σ-fields M of L/K such that M is a finite field extension of K and M/K is σ-separable. Then $\pi_0^\sigma(L/K)/K$ is a finite field extension ([TW18, Remarkark 1.27]) and Galois ([TW18, Corollary 1.35]). It follows that $\pi_0^\sigma(L/K)$ is the largest intermediate σ-field of L/K with the property that $\pi_0^\sigma(L/K)/K$ is finite Galois and σ-separable.

A Galois extension L/K of σ-fields is *benign* if there exists an intermediate field $K \subseteq M \subseteq L$ such that

- M/K is a finite Galois extension with $L = K\langle M\rangle$,
- the degree of $K(\sigma^n(M))$ over K equals the degree of M over K for all $n \in \mathbb{N}$ and
- the fields $(K(\sigma^n(M)))_{n\in\mathbb{N}}$ are linearly disjoint over K.

An extension L/K of σ-fields is *σ-radicial* if for every $a \in L$ there exists an $n \in \mathbb{N}$ such that $\sigma^n(a) \in K$.

Now we are prepared to state Babbitt's decomposition theorem. The version we state here is from [TW18, Theorem 2.9] and in contrast to the references given at the beginning of this section does not require $\sigma\colon K \to K$ to be an automorphism.

Theorem 7.2 (Babbitt's decomposition theorem)**.** *Let L/K be a finitely σ-generated Galois extension of σ-fields. Then there exists a chain*

$$K \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_n \subseteq L$$

of intermediate σ-fields such that $L_1 = \pi_0^\sigma(L/K)$, L_{i+1}/L_i is benign for $i = 1, \ldots, n-1$ and L/L_n is σ-radicial.

To deduce Theorem 7.2 from Theorem 4.6 we need to know how properties of expansive profinite groups correspond to properties of σ-field extensions. This is explained in the following lemma.

Lemma 7.3. *Let L/K be a finitely σ-generated Galois extension of σ-fields and let G be the Galois group of L/K, considered as an expansive profinite group as in Lemma 7.1.*

(i) *L/K is σ-separable if and only if $\sigma\colon G \to G$ is surjective.*
(ii) *L/K is finite and σ-separable if and only if G is finite and $\sigma\colon G \to G$ is bijective.*
(iii) *L/K is benign if and only if G is isomorphic to a full one-sided group shift.*

(iv) *L/K is σ-radicial if and only if G is σ-infinitesimal.*

Proof. We begin with (i). By [TW18, Proposition 1.2] the σ-field extension L/K is σ-separable if and only if whenever $f_1, \dots, f_n \in L$ are K-linearly independent then also $\sigma(f_1), \dots, \sigma(f_n)$ are K-linearly independent.

Assume that L/K is σ-separable. To show that $\sigma\colon G \to G$ is surjective, it suffices to show that $G \xrightarrow{\sigma} G \to G/U$ is surjective for every normal open subgroup U of G. With notation as in the proof of Lemma 7.1, we have $U = U_A$ for some finite subset A of L. So G/U can be identified with the Galois group of $K(A)/K$. As $\sigma^{-1}(U_A) = U_{\sigma(A)}$, we see that $G/\sigma^{-1}(U)$ can be identified with the Galois group of $K(\sigma(A))/K$. Because L/K is σ-separable, we see that $K(A)$ and $K(\sigma(A))$ have the same degree over K. Since the map $G/\sigma^{-1}(U) \to G/U$ induced by $\sigma\colon G \to G$ is injective it must then be surjective. Therefore $\sigma\colon G \to G$ is surjective.

Conversely, assume that $\sigma\colon G \to G$ is surjective. By the primitive element theorem it suffices to show that for any element $a \in L$ such that $K(a)/K$ is Galois, the fields $K(a)$ and $K(\sigma(a))$ have the same degree over K. Let n be the degree of $K(a)/K$. Then a has n conjugates $g_1(a), \dots, g_n(a) \in L$. We have to show that $\sigma(g_1(a)), \dots, \sigma(g_n(a)) \in L$ are also conjugate over K. Because $\sigma\colon G \to G$ is surjective we may write $g_i = \sigma(h_i)$ for some $h_i \in G$. Then $\sigma(g_i(a)) = \sigma(\sigma(h_i)(a)) = h_i(\sigma(a))$ and therefore these elements are conjugate over K.

Point (ii) follows from (i), because for G finite, $\sigma\colon G \to G$ is surjective if and only if it is bijective.

We next prove (iii). Assume that L/K is benign and let $K \subseteq M \subseteq L$ be a finite Galois extension of K such that $L = K\langle M\rangle$, the degree of $K(\sigma^n(M))$ over K equals the degree of M over K for all $n \in \mathbb{N}$ and the fields $(K(\sigma^n(M)))_{n\in\mathbb{N}}$ are linearly disjoint over K. Let $A \subseteq M$ be finite such that $M = K(A)$. Set $U = U_A$. Then G/U can be identified with the Galois group of M/K. More generally, as $\sigma^{-n}(U_A) = U_{\sigma^n(A)}$, we see that $G/\sigma^{-n}(U)$ can be identified with the Galois group of $K(\sigma^n(A)) = K(\sigma^n(M))$ over K. As $L = K\langle M\rangle$ and the fields $(K(\sigma^n(M)))_{n\in\mathbb{N}}$ are linearly disjoint over K, the canonical map $G \to \prod_{n\in\mathbb{N}} G/\sigma^{-n}(U)$ is an isomorphism of profinite groups. As M and $K(\sigma^n(M))$ have the same degree over K for all $n \in \mathbb{N}$, the map $\sigma_{n+1}\colon G/\sigma^{-(n+1)}(U) \to G/\sigma^{-n}(U)$ induced by $\sigma\colon G \to G$ is an isomorphism. If we define

$$\sigma\colon \prod_{n\in\mathbb{N}} G/\sigma^{-n}(U) \to \prod_{n\in\mathbb{N}} G/\sigma^{-n}(U),\ (g_n)_{n\in\mathbb{N}} \mapsto (\sigma_{n+1}(g_{n+1}))_{n\in\mathbb{N}},$$

then $G \to \prod_{n\in\mathbb{N}} G/\sigma^{-n}(U)$ becomes an isomorphism of expansive profinite groups. But $\prod_{n\in\mathbb{N}} G/\sigma^{-n}(U)$ is isomorphic to the full one-sided group shift on G/U.

Conversely, assume that G is isomorphic to the full one-sided group shift on a finite group $\mathcal{G}$. Let U be the open normal subgroup of G corresponding to $1 \times \mathcal{G} \times \mathcal{G} \times \ldots \leq \mathcal{G}^{\mathbb{N}}$ and define M as L^U, so M/K has Galois group $G/U = \mathcal{G}$. Then M has all the required properties.

Finally, we prove (iv). Assume that L/K is σ-radicial. Let A be finite subset of L such that $L = K\langle A\rangle$. As L/K is σ-radicial there exists an $n \in \mathbb{N}$ such that $\sigma^n(A) \in K$. But then in fact $\sigma^n(L) \subseteq K$. For $a \in L$ and $g \in G$ we have $\sigma(\sigma(g)(a)) = g(\sigma(a))$ and so inductively $\sigma^n(\sigma^n(g)(a)) = g(\sigma^n(a) = \sigma^n(a)$ because $\sigma^n(a) \in K$. The injectivity of $\sigma\colon L \to L$ implies $\sigma^n(g)(a) = a$ for all $a \in L$, i.e., $\sigma^n(g) = 1$.

Conversely, assume that G is σ-infinitesimal. By Lemma 3.35 there exists an integer $n \in \mathbb{N}$ such that $\sigma^n(g) = 1$ for all $g \in G$. Then $g(\sigma^n(a)) = \sigma^n(\sigma^n(g)(a)) = \sigma^n(a)$ for all $g \in G$ and $a \in L$. Thus $\sigma^n(a) \in K$. □

The following lemma is a "one-sided" version of [Lev08, Theorem 8.1.1].

Lemma 7.4. *Let L/K be a finitely σ-generated Galois extension of σ-fields and consider the Galois group $G = G(L/K)$ of L/K as an expansive profinite group as in Lemma 7.1.*

(i) *The maps $M \mapsto G(L/M)$ and $H \mapsto L^H$ define a bijection between the intermediate σ-fields of L/K and the expansive subgroups of G.*

(ii) *If M and H correspond to each other in* (i)*, then M/K is Galois if and only if H is normal in G and in that case, $G(M/K)$ and G/H are isomorphic as expansive profinite groups.*

(iii) *The expansive subgroup $G^{\sigma o}$ of G corresponds to the intermediate σ-field $\pi_0^\sigma(L/K)$.*

Proof. By the Galois correspondence, the map $M \mapsto G(L/M)$ is a bijection between the set of all intermediate fields of L/K and the set of closed subgroups of G with inverse $H \mapsto L^H$. So, if M corresponds to H, it suffices to show that $\sigma(M) \subseteq M$ if and only if $\sigma(H) \subseteq H$. First assume that $\sigma(M) \subseteq M$. Then, for $a \in M$ and $h \in H$ we have $\sigma(\sigma(h)(a)) = h(\sigma(a)) = \sigma(a)$ because $\sigma(a) \in M$. From the injectivity of $\sigma\colon L \to L$ it follows that $\sigma(h)(a) = a$ for all $a \in M$, i.e., $\sigma(h) \in H$. Conversely, assume that $\sigma(H) \subseteq H$ and $a \in M$. Then $\sigma(h)(a) = a$ and therefore $\sigma(a) = \sigma(\sigma(h)(a)) = h(\sigma(a))$ for all $h \in H$. Thus $\sigma(a) \in M$.

Part (ii) is clear from Galois theory. The only aspect that needs to be checked is that the restriction map $G \to G(M/K)$ commutes with σ, but this follows directly from the definition of the action of σ.

We know from Lemma 3.28 that $G^{\sigma o}$ is the smallest normal expansive subgroup of G such that $G/G^{\sigma o}$ is finite and $\sigma\colon G/G^{\sigma o} \to G/G^{\sigma o}$ is bijective. Thus, by Lemmas 7.3 and 7.4, $L^{G^{\sigma o}}$ is the largest Galois extension of K such that $L^{G^{\sigma o}}/K$ is finite and σ-separable. But this is exactly $\pi_0^\sigma(L/K)$. □

With these preparations at hand, it is now a straight forward matter to deduce Babbitt's decomposition theorem from Theorem 4.6.

Theorem 7.5. *Let L/K be a finitely σ-generated Galois extension of σ-fields. Then there exists a chain*

$$K \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_n \subseteq L$$

of intermediate σ-fields such that $L_1 = \pi_0^\sigma(L/K)$, L_{i+1}/L_i is benign with Galois group isomorphic to a full one-sided group shift on a finite simple group $\mathcal{G}_i$ for $i = 1, \ldots, n-1$ and L/L_n is σ-radicial. Moreover, the length n of such a chain and the isomorphism classes of the finite simple groups $\mathcal{G}_i$ are uniquely determined by L/K.

Proof. Let $G = G(L/K)$ denote the Galois group of L/K, considered as an expansive profinite group as in Lemma 7.1. Let

$$G \supseteq G_1 \supseteq \ldots \supseteq G_n$$

be a subnormal series as in Theorem 4.6. For $i = 1, \ldots, n$ set $L_i = L^{G_i}$. Then

$$K \subseteq L_1 \subseteq \ldots \subseteq L_n \subseteq L$$

is an ascending chain of intermediate σ-field that has the required properties by Lemmas 7.4 and 7.3.

If we have another chain

$$K \subseteq L_1' \subseteq \ldots \subseteq L_{n'}' \subseteq L$$

as in the theorem, then setting $G_i' = G(L/L_i')$ for $i = 1, \ldots, n'$ yields a subnormal series

$$G \supseteq G_1' \supseteq \ldots \supseteq G_{n'}'$$

as in Theorem 4.6. The uniqueness part of Theorem 4.6 thus implies the claimed uniqueness statement. □

References

[Bab62] Albert E. Babbitt, Jr. Finitely generated pathological extensions of difference fields. *Trans. Amer. Math. Soc.*, 102:63–81, 1962.

[BS08] Mike Boyle and Michael Schraudner. $\mathbb{Z}^d$ group shifts and Bernoulli factors. *Ergodic Theory Dynam. Systems*, 28(2):367–387, 2008.

[Coh65] Richard M. Cohn. *Difference algebra*. Interscience Publishers John Wiley & Sons, New York-London-Sydeny, 1965.
[Fag96] Fabio Fagnani. Some results on the classification of expansive automorphisms of compact abelian groups. *Ergodic Theory Dynam. Systems*, 16(1):45–50, 1996.
[FJ08] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics*. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.
[GR17] Helge Glöckner and C. R. E. Raja. Expansive automorphisms of totally disconnected, locally compact groups. *J. Group Theory*, 20(3):589–619, 2017.
[Kit87] Bruce P. Kitchens. Expansive dynamics on zero-dimensional groups. *Ergodic Theory Dynam. Systems*, 7(2):249–261, 1987.
[Kit98] Bruce P. Kitchens. *Symbolic dynamics*. Universitext. Springer-Verlag, Berlin, 1998. One-sided, two-sided and countable state Markov shifts.
[KS89] Bruce Kitchens and Klaus Schmidt. Automorphisms of compact groups. *Ergodic Theory Dynam. Systems*, 9(4):691–735, 1989.
[Lev08] Alexander Levin. *Difference algebra*, volume 8 of *Algebra and Applications*. Springer, New York, 2008.
[LM95] Douglas Lind and Brian Marcus. *An introduction to symbolic dynamics and coding*. Cambridge University Press, Cambridge, 1995.
[Rot95] Joseph J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995.
[RZ10] Luis Ribes and Pavel Zalesskii. *Profinite groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2010.
[Sch95] Klaus Schmidt. *Dynamical systems of algebraic origin*, volume 128 of *Progress in Mathematics*. Birkhäuser Verlag, Basel, 1995.
[Sha20] Riddh Shah. Expansive automorphisms on locally compact groups. *New York J. Math.*, 26:285–302, 2020.
[Sob07] Marcelo Sobottka. Topological quasi-group shifts. *Discrete Contin. Dyn. Syst.*, 17(1):77–93, 2007.
[TW18] Ivan Tomašić and Michael Wibmer. Strongly étale difference algebras and Babbitt's decomposition. *J. Algebra*, 504:10–38, 2018.

Michael Wibmer, Institute of Analysis and Number Therory, Graz University of Technology, Kopernikusgasse 24, 8010 Graz, Austria, https://sites.google.com/view/wibmer

E-mail address: wibmer@math.tugraz.at