Université Grenoble Alpes

ANNALES DE L'INSTITUT FOURIER

Michael Wibmer

Étale difference algebraic groups

Article à paraître, mis en ligne le 17 mai 2024, 69 p.

Les *Annales de l'Institut Fourier* sont membres du Centre Mersenne pour l'édition scientifique ouverte

www.centre-mersenne.org e-ISSN : 1777-5310

Ann. Inst. Fourier, Grenoble
Article à paraître
Mis en ligne le 17 mai 2024.

ÉTALE DIFFERENCE ALGEBRAIC GROUPS

by Michael WIBMER (*)

ABSTRACT. — Étale difference algebraic groups are a difference analog of étale algebraic groups. Our main result is a Jordan–Hölder type decomposition theorem for these groups. Roughly speaking, it shows that any étale difference algebraic group can be build up from simple étale algebraic groups and two finite étale difference algebraic groups. The simple étale algebraic groups occurring in this decomposition satisfy a certain uniqueness property.

RÉSUMÉ. — Les groupes algébriques aux différences étales sont des analogues aux différence des groupes algébriques étales. Le résultat principal de cet article est un théorème de décomposition de type Jordan–Hölder pour ces groupes. Nous montrons que tout groupe algébrique aux différences étale peut être construit à partir de groupes algébriques étales simples et de deux groupes algébriques aux différences étales finis. Les groupes algébriques étales simples apparaissant dans cette décomposition satisfont une certaine propriété d'unicité.

1. Introduction

Affine difference algebraic groups are a generalization of affine algebraic groups. Instead of just algebraic equations, one allows difference algebraic equations as the defining equations. Alternatively, affine difference algebraic groups can be described as affine group schemes with an additional structure (the difference structure). In algebraic terms, to specify an affine difference algebraic group G over a difference field k (i.e., k is a field equipped with an endomorphism $\sigma\colon k \to k$) is equivalent to specifying a Hopf algebra $k\{G\}$ over k together with a ring endomorphism $\sigma\colon k\{G\} \to k\{G\}$ extending $\sigma\colon k \to k$ such that the Hopf algebra structure maps commute

Keywords: Difference algebraic group, étale algebraic group, expansive endomorphism, profinite group.
2020 *Mathematics Subject Classification:* 14L15, 12H10, 37B05.
(*) 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.

with σ. It is also required that G is “of finite σ-type”, i.e., there exists a finite subset B of $k\{G\}$ such that $B, \sigma(B), \sigma^2(B), \ldots$ generates $k\{G\}$ as a k-algebra.

Étale difference algebraic groups are a difference analog of étale algebraic groups. Algebraically, they can be described as the affine difference algebraic groups G such that every element of $k\{G\}$ satisfies a separable polynomial over k. For example, the difference algebraic equations $x^n = 1$, $\sigma(x)x = 1$ define an étale difference algebraic subgroup of the multiplicative group $\mathbb{G}_m$, as long as n is not divisible by the characteristic of k. By interpreting algebraic equations as difference algebraic equations, any étale algebraic group $\mathcal{G}$ over k defines an étale difference algebraic group $[\sigma]_k\mathcal{G}$ over k. The Hopf algebra corresponding to $[\sigma]_k\mathcal{G}$ is the Hopf algebra of the affine group scheme $\mathcal{G} \times {}^{\sigma}\mathcal{G} \times {}^{\sigma^2}\mathcal{G} \times \cdots$, where ${}^{\sigma^i}\mathcal{G}$ is the base change of $\mathcal{G}$ along $\sigma^i\colon k \to k$.

Étale difference algebraic groups feature prominently in the general structure theory of affine difference algebraic groups, as any affine difference algebraic group G fits into a short exact sequence

$$1 \to G^o \to G \to \pi_0(G) \to 1,$$

with G^o a connected affine difference algebraic group (the identity component of G) and $\pi_0(G) \simeq G/G^o$ an étale difference algebraic group (the group of connected components of G).

The components referred to here are the components of the underlying group scheme of G, i.e., the affine group scheme represented by $k\{G\}$. Typically, there are infinitely many such components, i.e., $k\{\pi_0(G)\}$ is an infinite dimensional k-vector space. In this article we also study a true difference analog of the identity component of an algebraic group. The *σ-identity component* $G^{\sigma o}$ of an affine difference algebraic group G is such that $G/G^{\sigma o}$ is finite, i.e., $k\{G/G^{\sigma o}\}$ is a finite dimensional k-vector space. A *σ-infinitesimal* étale difference algebraic group is an étale difference algebraic group G such that $G(R) = 1$ whenever $\sigma\colon R \to R$ is injective. A σ-infinitesimal étale difference algebraic group is automatically finite.

Our main result is a Jordan–Hölder type decomposition theorem for étale difference algebraic groups.

Theorem (Theorem 6.38). — *Let G be an étale difference algebraic group. Then there exists a subnormal series*

$$G \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n \supseteq 1$$

of difference algebraic subgroups of G such that $G_1 = G^{\sigma o}$, G_n is σ-infinitesimal and $G_i/G_{i+1} \simeq [\sigma]_k\mathcal{G}_i$ for some σ-stably simple étale algebraic group $\mathcal{G}_i$ for $i = 1, \dots, n-1$.

If

$$G \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_m \supseteq 1$$

is another subnormal series such that $H_1 = G^{\sigma o}$, H_m is σ-infinitesimal and $H_i/H_{i+1} \simeq [\sigma]_k\mathcal{H}_i$ for some σ-stably simple étale algebraic group $\mathcal{H}_i$ for $i = 1, \dots, m-1$, then $m = n$ and there exists a permutation τ such that $\mathcal{G}_i$ and $\mathcal{H}_{\tau(i)}$ are σ-stably equivalent.

Here an étale algebraic group $\mathcal{G}$ is called *simple* if its only closed normal subgroups are 1 and $\mathcal{G}$ and *σ-stably simple* if ${}^{\sigma^i}\mathcal{G}$ is simple for every $i \in \mathbb{N}$. Finally, two étale algebraic groups $\mathcal{G}$ and $\mathcal{H}$ are *σ-stably equivalent* if there exist $i, j \in \mathbb{N}$ such that ${}^{\sigma^i}\mathcal{G}$ and ${}^{\sigma^j}\mathcal{H}$ are isomorphic.

The category of étale algebraic groups over k is equivalent to the category of finite groups equipped with a continuous action of the absolute Galois group of k. There is a similar combinatorial-arithmetic description of étale difference algebraic groups (Theorem 5.6): Fix an extension $\sigma\colon k_s \to k_s$ of $\sigma\colon k \to k$ to the separable algebraic closure k_s of k. Then there exists a unique endomorphism $\sigma\colon \mathscr{G} \to \mathscr{G}$ of the absolute Galois group $\mathscr{G} = \mathscr{G}(k_s/k)$ of k such that for every $\tau \in \mathscr{G}$ the diagram

$$\begin{tikzcd} k_s \arrow[r, "\sigma(\tau)"] \arrow[d, "\sigma"'] & k_s \arrow[d, "\sigma"] \\ k_s \arrow[r, "\tau"] & k_s \end{tikzcd}$$

commutes. Recall that an endomorphism $\sigma\colon \mathtt{G} \to \mathtt{G}$ of a profinite group $\mathtt{G}$ is called *expansive* if there exists a normal open subgroup $\mathtt{N}$ of $\mathtt{G}$ such that $\bigcap_{i\in\mathbb{N}} \sigma^{-i}(\mathtt{N}) = 1$. The category of étale difference algebraic groups over k is equivalent to the category of profinite groups $\mathtt{G}$ equipped with an expansive endomorphism $\sigma\colon \mathtt{G} \to \mathtt{G}$ and a continuous action of $\mathscr{G}$ that is compatible with σ in the sense that $\sigma(\tau(g)) = \sigma(\tau)(\sigma(g))$ for $\tau \in \mathscr{G}$ and $g \in \mathtt{G}$.

In particular, if k is separably algebraically closed, the category of étale difference algebraic groups over k is equivalent to the category of profinite groups equipped with an expansive endomorphism. The study of expansive endo- or automorphisms of profinite groups or more generally totally disconnected locally compact groups is an interesting topic in its own right. See e.g., [12, 14, 35, 36]. When translated to profinite groups (via Theorem 5.6) our decomposition theorem recovers results proved by G. Willis

([35, Section 6]) for expansive automorphisms of profinite groups. (The case of expansive endomorphisms of profinite groups is somewhat more complicated than the case of expansive automorphisms but similar ideas and techniques apply.) A restatement and proof of Theorem 6.38 in the language of profinite groups can be found in [33].

Our decomposition theorem has some formal similarities with Babbitt's decomposition theorem ([18, Theorem 5.4.13]), an important structure theorem for finitely generated extensions of difference fields whose underlying field extension is Galois. This similarity is no coincidence, in fact, as detailed in [33, Section 6], one can deduce Babbitt's decomposition theorem from the profinite group version of Theorem 6.38 via the Galois correspondence.

The theory of difference algebraic groups is still in its infancy, at least compared to the sister theory of differential algebraic groups, where a large body of foundational material was developed well before the turn of the century. (See the text books [5, 17] and the references given there.) Therefore, a goal of this article is also to provide some foundational results and ideas to pave the way for a further comprehensive study of affine difference algebraic groups. In this regard, our main contributions are

- our study of the difference identity component of an affine difference algebraic group and the associated group of difference connected components,
- our study of σ-infinitesimal difference algebraic groups (a difference analog of infinitesimal algebraic groups),
- our study of the σ-Frobenius morphism (a difference analog of the Frobenius morphism of an algebraic group).

Note that, while infinitesimal algebraic groups and the Frobenius morphism only make sense over a field of positive characteristic, σ-infinitesimal difference algebraic groups and the σ-Frobenius morphism make sense over an arbitrary difference field. Roughly speaking, the idea is that the abstract endomorphism σ assumes the role played, in the study of algebraic groups, by the Frobenius endomorphism $a \mapsto a^p$ in characteristic p.

A main motivation for developing the theory of affine difference algebraic groups, is that these groups can be used, via appropriate Galois theories ([9, 21]), to study the difference algebraic relations among the solutions of linear differential and difference equations. In this context, Theorem 6.38 sheds light on the possible difference algebraic relations among algebraic solutions of linear differential or difference equations.

We conclude the introduction with an overview of the article. In Section 2 we go through the details of the definition of affine difference algebraic groups and we review the known results on affine difference algebraic groups relevant for our purpose. We then embark on a general study of the difference identity component of a difference algebraic group and the associated group of difference connected components in Section 3. After a brief discussion of basic properties of étale difference algebraic groups in Section 4, we establish the combinatorial-arithmetic description of the category of étale difference algebraic groups in Section 5. Finally, in Section 6 we prove our decomposition theorem.

2. Preliminaries and notation

In this preliminary section we recall the basic definitions and constructions from difference algebra. We also review the required results from [32] and [34] concerning affine difference algebraic groups.

All rings are assumed to be commutative and unital. The natural numbers $\mathbb{N}$ contain 0.

2.1. Difference algebra

Difference algebra is the study of difference equations from an algebraic perspective. Standard references are [8] and [18].

A *difference ring*, or *σ-ring* for short, is a ring R together with an endomorphism $\sigma\colon R \to R$. A *difference field*, or *σ-field* for short, is a difference ring whose underlying ring is a field. A *σ-subring* of a σ-ring R is a subring S of R such that $\sigma(S) \subseteq S$. In case S and R are fields, we call R a *σ-field extension* of S.

A *morphism of σ-rings* $\psi\colon R \to S$ is a morphism of rings such that

$$\begin{tikzcd} R \arrow[r, "\psi"] \arrow[d, "\sigma"'] & S \arrow[d, "\sigma"] \\ R \arrow[r, "\psi"] & S \end{tikzcd}$$

commutes. In this situation, we also say that S is an *R-σ-algebra* or that S is a *difference algebra over R*. An *R-σ-subalgebra* of an R-σ-algebra S is an R-subalgebra of S that is a σ-subring. A *morphism of R-σ-algebras* is a morphism of σ-rings that also is a morphism of R-algebras. If S_1 and

S_2 are R-σ-algebras, the tensor product $S_1 \otimes_R S_2$ is an R-σ-algebra via $\sigma(s_1 \otimes s_2) = \sigma(s_1) \otimes \sigma(s_2)$. This is, in fact, the coproduct in the category of R-σ-algebras.

An R-σ-algebra S is *finitely σ-generated* (over R) if there exists a finite subset B of S such that $B, \sigma(B), \sigma^2(B), \ldots$ generates S as an R-algebra.

A *difference ideal*, or *σ-ideal* for short, of a σ-ring R is an ideal I of R such that $\sigma(I) \subseteq I$. In this case, R/I naturally carries the structure of a σ-ring such that the canonical map $R \to R/I$ is a morphism of σ-rings. For $F \subseteq R$, the smallest σ-ideal of R that contains F is called the *σ-ideal σ-generated by F*. It is denoted by $[F]$. Explicitly, we have $[F] = (F, \sigma(F), \sigma^2(F), \ldots)$.

As a matter of convenience, we usually suppress the endomorphism σ in the notation, e.g., we speak of the σ-ring R, rather than the σ-ring (R, σ). In case we have need to indicate that we consider the underlying ring without the endomorphism, we will write $R^\sharp$.

Let k be σ-field. The functor $R \rightsquigarrow R^\sharp$ from the category of k-σ-algebras to the category of k-algebras has a right adjoint $T \rightsquigarrow [\sigma]_k T$ ([34, Lemma 1.7]). Explicitly, for a k-algebra T, the k-σ-algebra $[\sigma]_k T$ can be described as follows. For $i \in \mathbb{N}$ let ${}^{\sigma^i}T = T \otimes_k k$ denote the k-algebra obtained from T by base change via $\sigma^i \colon k \to k$. In particular, multiplication in ${}^{\sigma^i}T = T \otimes_k k$ is determined by $(t_1 \otimes \lambda_1) \cdot (t_1 \otimes \lambda_2) = t_1 t_2 \otimes \lambda_1 \lambda_2$. Moreover, $\lambda_1 t \otimes \lambda_2 = t \otimes \sigma^i(\lambda_1)\lambda_2 \in {}^{\sigma^i}T$ for $\lambda_1, \lambda_2 \in k$ and $t \in T$ and the k-algebra structure of ${}^{\sigma^i}T$ is given by $k \to {}^{\sigma^i}T,\ \lambda \mapsto 1 \otimes \lambda$.

Set

$$T[i] = T \otimes_k {}^{\sigma}T \otimes_k \cdots \otimes_k {}^{\sigma^i}T$$

and let $[\sigma]_k T$ be the union the $T[i]$'s. The endomorphism $\sigma \colon [\sigma]_k T \to [\sigma]_k T$ is given by

$$\sigma((t_0 \otimes \lambda_0) \otimes \cdots \otimes (t_i \otimes \lambda_i)) = (1 \otimes 1) \otimes (t_0 \otimes \sigma(\lambda_0)) \otimes \cdots \otimes (t_i \otimes \sigma(\lambda_i)) \in T[i+1]$$

for $(t_0 \otimes \lambda_0) \otimes \cdots \otimes (t_i \otimes \lambda_i) \in {}^{\sigma^0}T \otimes_k \cdots \otimes_k {}^{\sigma^i}T = T[i]$. Note that if $B \subseteq T$ generates T as a k-algebra, then $B \subseteq [\sigma]_k T$ σ-generates $[\sigma]_k T$ as a k-σ-algebra.

2.2. Affine difference algebraic geometry

Let k be a σ-field. The *σ-polynomial ring*

$$k\{y_1, \ldots, y_n\} = k[y_1, \ldots, y_n, \sigma(y_1), \ldots, \sigma(y_n), \sigma^2(y_1), \ldots, \sigma^2(y_n), \ldots]$$

over k in the σ-variables $y_1, \ldots, y_n$ is the polynomial ring over k in the variables $\sigma^i(y_j)$ $(i \in \mathbb{N}, 1 \leqslant j \leqslant n)$ equipped with the action of σ that extends $\sigma\colon k\to k$ and acts on the variables as suggested by their names. If $f\in k\{y_1,\ldots,y_n\}$ is a σ-polynomial and $a=(a_1,\ldots,a_n)\in R^n$, where R is a k-σ-algebra, then $f(a)\in R$ is defined by replacing $\sigma^i(y_j)$ with $\sigma^i(a_j)$. For $F\subseteq k\{y_1,\ldots,y_n\}$, the set of R-valued solutions of F is

$$\mathbb{V}_R(F)=\{a\in R^n \mid f(a)=0\ \forall\ f\in F\}.$$

Note that $R\rightsquigarrow \mathbb{V}_R(F)$ is naturally a functor from the category of k-σ-algebras to the category of sets.

Definition 2.1. — *An* affine difference variety*, or* affine σ-variety *for short, over k is a functor from the category of k-σ-algebras to the category of sets that is isomorphic to a functor of the form $R\rightsquigarrow \mathbb{V}_R(F)$ for some $n\geqslant 1$ and $F\subseteq k\{y_1,\ldots,y_n\}$.*

All difference varieties in this article are affine and for the sake of brevity we shall henceforth drop the attribute affine. A *morphism of σ-varieties* (over k) is a morphism of functors, i.e., a natural transformation.

The functor $R\rightsquigarrow \mathbb{V}_R(F)$ is represented by the finitely σ-generated k-σ-algebra $k\{y_1,\ldots,y_n\}/[F]$. Indeed,

$$\operatorname{Hom}(k\{y_1,\ldots,y_n\}/[F],R)\to \mathbb{V}_R(F),\ \psi\mapsto(\psi(\overline{y_1}),\ldots,\psi(\overline{y_n}))$$

is a bijection that is functorial in R. As any finitely σ-generated k-σ-algebra can be written in the form $k\{y_1,\ldots,y_n\}/[F]$, it follows that a functor from the category of k-σ-algebras to the category of sets is a σ-variety if and only if it is representable by a finitely σ-generated k-σ-algebra. Thus, from the Yoneda lemma we obtain:

Remark 2.2. — The category of σ-varieties over k is anti-equivalent to the category of finitely σ-generated k-σ-algebras.

For a σ-variety X we denote its representing k-σ-algebra with $k\{X\}$ and call it the *coordinate ring* of X. We will usually identify X with the functor $R\rightsquigarrow \operatorname{Hom}(k\{X\},R)$. For a morphism $\phi\colon X\to Y$ of σ-varieties, the corresponding morphism $\phi^*\colon k\{Y\}\to k\{X\}$ of k-σ-algebras is called the *morphism dual to ϕ*.

A *σ-closed σ-subvariety* X of a σ-variety Y is a subfunctor X of Y that is defined by a σ-ideal $\mathbb{I}(X)$ of $k\{Y\}$. In more detail, the requirement is that for any k-σ-algebra R, the bijection $Y(R)\simeq \operatorname{Hom}(k\{Y\},R)$ maps $X(R)$ onto $\{\psi\in \operatorname{Hom}(k\{Y\},R)\mid \psi(\mathbb{I}(X))=0\}$. We call $\mathbb{I}(X)$ the *defining ideal of X* (in $k\{Y\}$). We may write $X\subseteq Y$ to indicate that X is a σ-closed σ-subvariety of Y.

Note that a σ-closed σ-subvariety is a σ-variety it its own right; it is represented by $k\{X\}=k\{Y\}/\mathbb{I}(X)$. The canonical map $k\{Y\}\to k\{Y\}/\mathbb{I}(X)$

is the dual of the inclusion morphism $X \to Y$. The σ-closed σ-subvarieties of Y are in bijection with the σ-ideals of $k\{Y\}$ ([34, Lemma 1.4]).

A morphism $\phi\colon X \to Y$ of σ-varieties is a *σ-closed embedding* if it induces an isomorphism between X and a σ-closed σ-subvariety of Y. This is equivalent to $\phi^*\colon k\{Y\} \to k\{X\}$ being surjective ([34, Lemma 1.6]).

Let $\phi\colon X \to Y$ be a morphism of σ-varieties and let Z be a σ-closed σ-subvariety of Y. We define a subfunctor $\phi^{-1}(Z)$ of X by $\phi^{-1}(Z)(R) = \phi_R^{-1}(Z(R))$, where $\phi_R\colon X(R) \to Y(R)$ for any k-σ-algebra R. As

$$\begin{aligned}\phi^{-1}(Z)(R) &= \{\psi \in \operatorname{Hom}(k\{X\}, R) \mid \mathbb{I}(Z) \subseteq \ker(\psi\phi^*)\}\\ &= \{\psi \in \operatorname{Hom}(k\{X\}, R) \mid \phi^*(\mathbb{I}(Z)) \subseteq \ker(\psi)\},\end{aligned}$$

we see that $\phi^{-1}(Z)$ is the σ-closed σ-subvariety of X defined by $\mathbb{I}(\phi^{-1}(Z)) = [\phi^*(\mathbb{I}(Z))] \subseteq k\{X\}$.

Notational conventions. — Throughout the article we will work with σ-varieties (over the σ-field k) and with varieties/schemes (over the field k). To have a clear notational distinction between the two, we will, following the conventions from [32] and [34], use standard font, e.g., X, Y, G, H for σ-varieties and calligraphic font, e.g., $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{G}$, $\mathcal{H}$ for varieties/schemes.

A similar convention is used for coordinate rings. As usual, we use $k[\mathcal{X}]$ to denote the coordinate ring, i.e., the ring of global sections, of an affine scheme $\mathcal{X}$ over k. For σ-varieties we use, as above, curly brackets, e.g., $k\{X\}$ is the coordinate ring of a σ-variety X over k.

For an affine scheme $\mathcal{X}$ of finite type over k, the functor $[\sigma]_k\mathcal{X}$ defined by $([\sigma]_k\mathcal{X})(R) = \mathcal{X}(R)$ for any k-σ-algebra R is a σ-variety over k. Indeed, if $k[\mathcal{X}]$ is the coordinate ring of $\mathcal{X}$, then $\operatorname{Hom}(k[\mathcal{X}], R^\sharp) \simeq \operatorname{Hom}([\sigma]_k k[\mathcal{X}], R)$ for any k-σ-algebra R. So $k\{[\sigma]_k\mathcal{X}\} = [\sigma]_k k[\mathcal{X}]$. For simplicity, we will write $k\{\mathcal{X}\}$ for $k\{[\sigma]_k\mathcal{X}\} = [\sigma]_k k[\mathcal{X}]$. By a *$\sigma$-closed σ-subvariety of $\mathcal{X}$* we mean a σ-closed σ-subvariety of $[\sigma]_k\mathcal{X}$.

Let Y be a σ-closed σ-subvariety of $\mathcal{X}$. For $i \in \mathbb{N}$ let ${}^{\sigma^i}\mathcal{X}$ be the base change of $\mathcal{X}$ via $\sigma^i\colon k \to k$ and set

$$\mathcal{X}[i] = \mathcal{X} \times {}^{\sigma}\mathcal{X} \times \cdots \times {}^{\sigma^i}\mathcal{X}.$$

The *i-th order Zariski closure $Y[i]$ of Y in $\mathcal{X}$* is the scheme theoretic image of the morphism $Y^\sharp \to \mathcal{X}[i]$ of affine schemes corresponding to the morphism $k[\mathcal{X}[i]] \hookrightarrow k\{\mathcal{X}\} \to k\{Y\}$ of k-algebras. In other words, if $\mathbb{I}(Y) \subseteq k\{\mathcal{X}\} = [\sigma]_k k[\mathcal{X}] = \bigcup_{i\in\mathbb{N}} k[\mathcal{X}[i]]$ is the defining ideal of Y in $[\sigma]_k\mathcal{X}$, then $Y[i]$ is the closed subscheme of $\mathcal{X}[i]$ defined by the ideal $\mathbb{I}(Y) \cap k[\mathcal{X}[i]]$ of $k[\mathcal{X}[i]]$. We say that Y is *Zariski dense* in $\mathcal{X}$ if $Y[0] = \mathcal{X}$ and we refer to $Y[0]$ as the Zariski closure of Y in $\mathcal{X}$.

Note that the projections $\pi_i\colon \mathcal{X}[i] \to \mathcal{X}[i-1],\ (x_0,\ldots,x_i) \mapsto (x_0,\ldots,x_{i-1})$ restrict to projections $\pi_i\colon Y[i] \to Y[i-1]$.

2.3. Difference algebraic groups

The category of σ-varieties over k has products. Indeed, if X and Y are σ-varieties over k, the functor $X \times Y$ defined by $(X\times Y)(R) = X(R)\times Y(R)$ for any k-σ-algebra R, is a product of X and Y. It is represented by $k\{X\}\otimes_k k\{Y\}$. There also is a terminal object, namely the σ-variety represented by the k-σ-algebra k. Therefore we can make the following definition.

Definition 2.3. — *A* σ-algebraic group *(over k) is a group object in the category of σ-varieties (over k).*

In other words, a σ-algebraic group over k is a functor from the category of k-σ-algebras to the category of groups such that the correspond functor to the category of sets is representable by a finitely σ-generated k-σ-algebra.

A morphism of σ-algebraic groups $\phi\colon G \to H$ is a morphism of σ-varieties such that $\phi_R\colon G(R) \to H(R)$ is a morphism of groups for any k-σ-algebra. See [34, Section 2] for a list of examples of σ-algebraic groups.

A *σ-closed subgroup* of a σ-algebraic group G is a σ-closed σ-subvariety H of G such that $H(R)$ is a subgroup of $G(R)$ for any k-σ-algebra R. We may write $H \leqslant G$ to indicate that H is a σ-closed subgroup of G. A *σ-closed embedding of σ-algebraic groups* is a morphism of σ-algebraic groups that is a σ-closed embedding of σ-varieties.

Recall (see e.g., [31, Section 1.4]) that affine group schemes correspond to Hopf algebras. A *k-σ-Hopf algebra* is a k-σ-algebra R equipped with the the structure of a Hopf algebra such that the Hopf algebra structure maps (the comultiplication $\Delta\colon R \to R\otimes_k R$, the counit $\varepsilon\colon R \to k$ and the antipode $S\colon R \to R$) are morphisms of k-σ-algebras. From Remark 2.2 we obtain:

Remark 2.4. — The category of σ-algebraic groups over k is anti-equivalent to the category of finitely σ-generated k-σ-Hopf algebras.

For a σ-algebraic group G, we write $\mathfrak{m}_G$ for the kernel of the counit $\varepsilon\colon k\{G\} \to k$. Note that $\mathfrak{m}_G$ defines the trivial subgroup 1 of G.

Lemma 2.5 ([34, Lemma 2.15]). — *Let R be a k-σ-Hopf algebra and S a k-Hopf algebra. If $S \to R$ is a morphism of k-Hopf algebras, the induced morphism $[\sigma]_k S \to R$ is a morphism of k-σ-Hopf algebras.*

Example 2.6. — To any finite group $\mathtt{G}$ equipped with an endomorphism $\sigma\colon \mathtt{G}\to\mathtt{G}$ one can associate a σ-algebraic group G. Since we will refer to this example later, we explain the details. For any k-σ-algebra R, let $G(R)$ denote the set of all locally constant functions $f\colon \operatorname{Spec}(R)\to\mathtt{G}$ such that

$$\begin{array}{ccc} \operatorname{Spec}(R) & \xrightarrow{f} & \mathtt{G} \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ \operatorname{Spec}(R) & \xrightarrow{f} & \mathtt{G} \end{array}$$

commutes, where $\sigma\colon \operatorname{Spec}(R)\to\operatorname{Spec}(R)$ is the continuous map induced by $\sigma\colon R\to R$. Then $G(R)$ is a group under pointwise multiplication.

Let $k^{\mathtt{G}}$ be the finite dimensional k-algebra of all maps from $\mathtt{G}$ to k. As explained in [31, Section 2.3] the k-algebra $k^{\mathtt{G}}$ naturally has the structure of a k-Hopf algebra. Defining $\sigma\colon k^{\mathtt{G}}\to k^{\mathtt{G}}$ by $\sigma(h)(g)=\sigma(h(\sigma(g)))$ for $h\colon \mathtt{G}\to k$ and $g\in\mathtt{G}$ defines the structure of k-σ-Hopf algebra on $k^{\mathtt{G}}$. One can show ([34, Example 2.14]) that G is represented by the k-σ-Hopf algebra $k\{G\}=k^{\mathtt{G}}$.

For further examples of σ-algebraic groups see [34, Section 2]. Before further discussing σ-algebraic groups, let us agree on the following conventions.

Notation for algebraic groups. — We use the term "algebraic group (over k)" as synonymous for "affine group scheme of finite type (over k)". The coordinate ring, i.e., the ring of global sections, of an algebraic group $\mathcal{G}$ is denoted by $k[\mathcal{G}]$. Following [20, Definition 5.5] a morphism $\phi\colon \mathcal{G}\to\mathcal{H}$ of algebraic groups is a *quotient map* if the dual map $\phi^*\colon k[\mathcal{H}]\to k[\mathcal{G}]$ is injective (equivalently, faithfully flat). By a *closed subgroup* of an algebraic group we mean a closed subgroup scheme.

From now on and throughout this article k denotes an arbitrary σ-field. All σ-varieties, σ-algebraic groups and algebraic groups are assumed to be over k (unless the contrary is explicitly indicated).

If $\phi\colon X\to Y$ is a morphism of σ-varieties, there exists a unique σ-closed σ-subvariety $\phi(X)$ of Y such that ϕ factors through the inclusion $\phi(X)\subseteq Y$ and if Z is any σ-closed σ-subvariety of Y such that ϕ factors through Z, then $\phi(X)\subseteq Z$ ([34, Lemma 1.5]). Indeed, $\phi(X)$ is the σ-closed σ-subvariety of Y defined by $\mathbb{I}(\phi(X))=\ker(\phi^*)$. If $\phi\colon G\to H$ is a morphism of σ-algebraic groups, then $\phi(G)$ is a σ-closed subgroup of H.

If $\mathcal{G}$ is an algebraic group over k, then $[\sigma]_k\mathcal{G}$ is a σ-algebraic group. By a *σ-closed subgroup of $\mathcal{G}$*, we mean a σ-closed subgroup of $[\sigma]_k\mathcal{G}$. For

$i \in \mathbb{N}$ the affine scheme $\mathcal{G}[i] = \mathcal{G} \times \cdots \times {}^{\sigma^i}\mathcal{G}$ is an algebraic group and if G is a σ-closed subgroup of $\mathcal{G}$, then $G[i]$ is a closed subgroup of $\mathcal{G}[i]$. The projections $\pi_i \colon G[i] \to G[i-1]$ are morphisms of algebraic groups. In fact, they are quotient maps.

A basic fact about σ-algebraic groups is that every σ-algebraic group is isomorphic to a σ-closed subgroup of an algebraic group.

Proposition 2.7 ([34, Proposition 2.16]). — *Let G be a σ-algebraic group. Then there exists an algebraic group $\mathcal{G}$ and a σ-closed embedding $G \to [\sigma]_k\mathcal{G}$.*

These σ-closed embeddings of σ-algebraic groups into algebraic groups can be used to define three numerical invariants of a σ-algebraic group G: the *σ-dimension* $\sigma\text{-}\dim(G)$, the *order* $\operatorname{ord}(G)$ and the *limit degree* $\operatorname{ld}(G)$.

Theorem 2.8 ([34, Theorem 3.7]). — *Let G be a σ-closed subgroup of an algebraic group $\mathcal{G}$. For $i \in \mathbb{N}$ let $d_i = \dim(G[i])$ denote the dimension of the i-th order Zariski closure of G in $\mathcal{G}$. Then there exist $d, e \in \mathbb{N}$ such that $d_i = d(i+1)+e$ for all sufficiently large i. The integer d only depends on G (and not on the choice of the σ-closed embedding of G into $\mathcal{G}$). Moreover, if $d = 0$, the integer e only depends on G.*

The integer d of Theorem 2.8 is called the σ-dimension of G. If $\sigma\text{-}\dim(G) = 0$, the integer e of Theorem 2.8 is called the order of G.

For an algebraic group $\mathcal{G}$ we denote with $|\mathcal{G}|$ the dimension of $k[\mathcal{G}]$ as a k-vector space. (This is infinite if $\mathcal{G}$ has positive dimension.)

Proposition 2.9. — *Let G be a σ-closed subgroup of an algebraic group $\mathcal{G}$ and for $i \in \mathbb{N}$ let $G[i]$ denote the i-th order Zariski closure of G in $\mathcal{G}$. Let $\mathcal{G}_i$ denote the kernel of the projection $\pi_i \colon G[i] \to G[i-1]$. Then the sequence $(|\mathcal{G}_i|)_{i\in\mathbb{N}}$ is non-increasing and therefore eventually constant. The eventual value $\lim_{i\to\infty} |\mathcal{G}_i|$ only depends on G (and not on the choice of the σ-closed embedding of G into $\mathcal{G}$).*

Proof. — This follows by combining Propositions 4.1 and 5.1 in [34]. □

The value $\operatorname{ld}(G) = \lim_{i\to\infty} |\mathcal{G}_i|$ from Proposition 2.9 is called the *limit degree* of G. Note that $\operatorname{ld}(G)$ is finite if and only if $\sigma\text{-}\dim(G) = 0$. In [7], the authors introduce an invariant for difference field extension called the *distant degree* and discuss its relation with the limit degree. See, in particular, [7, Sections 1.14 and 1.15] where the case of difference groups is discussed. It also seems interesting to note that the main result of [7] as well as our decomposition theorem (Theorem 6.38) are closely related to results of G. Willis on automorphisms of totally disconnected locally compact groups.

The following Lemma explains the meaning of $\mathrm{ld}(G)=1$.

Lemma 2.10 ([34, Lemma 5.7]). — *Let G be a σ-algebraic group. Then $\mathrm{ld}(G)=1$ if and only if $k\{G\}$ is finitely generated as a k-algebra.*

We next discuss quotients. A σ-closed subgroup N of a σ-algebraic group G is *normal* if $N(R)$ is a normal subgroup of $G(R)$ for any k-σ-algebra R. We may write $N \trianglelefteq G$ to indicate that N is a normal σ-closed subgroup of G.

The *kernel* $\ker(\phi)$ of a morphism $\phi\colon G \to H$ of σ-algebraic groups is defined by $\ker(\phi)(R)=\ker(\phi_R)$ for any k-σ-algebra R. Since $\ker(\phi)=\phi^{-1}(1)$, where 1 is the trivial subgroup of H (defined by the kernel $\mathfrak{m}_H$ of the counit $k\{H\}\to k$), we see that $\ker(\phi)$ is the normal σ-closed subgroup of G defined by $\mathbb{I}(\ker(\phi))=(\phi^*(\mathfrak{m}_H))\subseteq k\{G\}$.

A *quotient of G mod N* is a σ-algebraic group G/N together with a morphism $\pi\colon G\to G/N$ of σ-algebraic groups such that $N\subseteq \ker(\pi)$ and for any other morphism $\phi\colon G\to H$ of σ-algebraic groups such that $N\subseteq\ker(\phi)$ there exists a unique morphism $\phi'\colon G/N\to H$ such that

$$\begin{tikzcd} G \arrow[rr, "\pi"] \arrow[dr, "\phi"'] & & G/N \arrow[dl, dotted, "\phi'"] \\ & H & \end{tikzcd}$$

commutes.

Theorem 2.11 ([32, Theorem 3.3]). — *Let G be σ-algebraic group and N a normal σ-closed subgroup of G. Then a quotient of G mod N exists. Moreover, a morphism $\pi\colon G\to G/N$ of σ-algebraic groups is a quotient of G mod N if and only if $N=\ker(\pi)$ and $\pi^*\colon k\{G/N\}\to k\{G\}$ is injective.*

A morphism $\phi\colon G\to H$ of σ-algebraic groups is a *quotient map* if it is a quotient of G mod N for some normal σ-closed subgroup of G. Equivalently, $\phi(G)=H$, i.e., $\phi^*\colon k\{H\}\to k\{G\}$ is injective. See [32, Proposition 4.10] for further characterizations of quotient maps.

A sequence $1\to N\xrightarrow{\alpha} G\xrightarrow{\beta} H\to 1$ of morphisms of σ-algebraic groups is *exact* if α is a σ-closed embedding, β is a quotient map and $\alpha(N)=\ker(\beta)$.

A *k-σ-Hopf subalgebra* of a k-σ-Hopf algebra is a Hopf subalgebra that is also a k-σ-subalgebra.

Theorem 2.12 ([34, Theorem 4.5]). — *A k-σ-Hopf subalgebra of a finitely σ-generated k-σ-Hopf algebra is finitely σ-generated.*

Corollary 2.13. — *Let G be a σ-algebraic group. There is a bijection between the normal σ-closed subgroups of G and the k-σ-Hopf subalgebras of $k\{G\}$.*

Proof. — If N is a normal σ-closed subgroup of G and $\pi\colon G \to G/N$ the corresponding quotient, then $\pi^*(k\{G/N\})$ is k-σ-Hopf subalgebra of $k\{G\}$. Conversely, if R is a k-σ-Hopf subalgebra of $k\{G\}$, then R is finitely σ-generated by Theorem 2.12. So $R = k\{H\}$ for some σ-algebraic group H. The kernel N of the morphism $G \to H$ of σ-algebraic groups corresponding to the inclusion $R \subseteq k\{G\}$ is a normal σ-closed subgroup of G. By Theorem 2.11 these two constructions are inverse to each other. □

The three numerical invariants are well-behaved under quotients.

Proposition 2.14. — *Let N be a normal σ-closed subgroup of a σ-algebraic group G. Then*

$$\sigma\text{-}\dim(G) = \sigma\text{-}\dim(N) + \sigma\text{-}\dim(G/N),$$
$$\operatorname{ord}(G) = \operatorname{ord}(N) + \operatorname{ord}(G/N)$$

and

$$\operatorname{ld}(G) = \operatorname{ld}(G/N) \cdot \operatorname{ld}(N).$$

Proof. — This is Corollaries 3.13 and 3.15 in [34]. □

The formulas in Proposition 2.14 are written in a form so that they still make sense in case infinite values are involved. For example, if $\operatorname{ld}(G)$ is finite, then also $\operatorname{ld}(N)$ and $\operatorname{ld}(G/N)$ are finite and $\operatorname{ld}(G/N) = \frac{\operatorname{ld}(G)}{\operatorname{ld}(N)}$.

If X is a σ-variety over k and R a k-σ-algebra, we denote with X_R the functor from the category of R-σ-algebras to the category of sets such that $X_R(R') = X(R')$ for any R-σ-algebra R'. Note that X_R is represented by $k\{X\} \otimes_k R$. In particular, if $R = k'$ is a σ-field extension of k, then $X_{k'}$ is a σ-variety over k', called the *base change of X* along $k \to k'$.

Quotients have all the expected good properties, for example:

Lemma 2.15 ([32, Lemma 3.9]). — *Let N be a normal σ-closed subgroup of a σ-algebraic group G and let k' be a σ-field extension of k. Then $(G/N)_{k'} = G_{k'}/N_{k'}$.*

Lemma 2.16 ([32, Corollary 3.4]). — *If $\phi\colon G \to H$ is a morphism of σ-algebraic groups, the induced morphism $G/\ker(\phi) \to H$ is a σ-closed embedding.*

Example 2.17 ([32, *Example 3.7*]*).* — If $\mathcal{N}$ is a normal closed subgroup of an algebraic group $\mathcal{G}$. Then $[\sigma]_k\mathcal{G}/[\sigma]_k\mathcal{N} = [\sigma]_k(\mathcal{G}/\mathcal{N})$.

The isomorphism theorems hold for σ-algebraic groups. In particular, we have the first isomorphism theorem:

Theorem 2.18 ([32, Theorem 5.2]). — *Let $\phi\colon G \to H$ be a morphism of σ-algebraic groups. Then the induced morphism $G/\ker(\phi) \to \phi(G)$ is an isomorphism of σ-algebraic groups.*

As a corollary to the above theorem we obtain:

Corollary 2.19. — *A morphism of σ-algebraic groups that is a quotient map and a σ-closed embedding is an isomorphism.*

The following is the third isomorphism theorem for σ-algebraic groups.

Theorem 2.20 ([32, Theorem 5.9]). — *Let N be a normal σ-closed subgroup of a σ-algebraic group G with quotient map $\pi\colon G \to G/N$. Then the map $H \mapsto \pi(H) = H/N$ defines a bijection between the σ-closed subgroups H of G containing N and the σ-closed subgroups of G/N. The inverse is $H' \mapsto \pi^{-1}(H')$. A σ-closed subgroup H of G containing N is normal in G if and only if H/N is normal in G/N. In this case the canonical morphism $G/H \to (G/N)/(H/N)$ is an isomorphism.*

Let G be a σ-algebraic group. A *subnormal series* of G is a sequence

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1 \tag{2.1}$$

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

$$G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = 1 \tag{2.2}$$

is a refinement of (2.1) if $\{G_0, \ldots, G_n\} \subseteq \{H_1, \ldots, H_m\}$. The subnormal series (2.1) and (2.2) are equivalent if $m = n$ and there exists a permutation π such that the factor groups G_i/G_{i+1} and $H_{\pi(i)}/H_{\pi(i)+1}$ are isomorphic for $i = 0, \ldots, n-1$.

Our main main decomposition theorem (Theorem 6.38) is reminiscent of the Jordan–Hölder theorem. The standard proof of the uniqueness part of the Jordan–Hölder theorem proceeds through the Schreier refinement theorem. The following is the Schreier refinement theorem for σ-alegbraic groups.

Theorem 2.21 ([32, Theorem 7.5]). — *Any two subnormal series of a σ-algebraic group have equivalent refinements.*

3. The difference identity component

There are three types of "identity components" for a σ-algebraic group G. The *identity component* G^o, the *σ-identity component* $G^{\sigma o}$ and the *strong identity component* G^{so}. The identity component and the strong identity component are discussed in [32, Section 6]. These are not relevant for the purpose of this article. However, it might be interesting to note that, more or less by definition, a σ-algebraic group G is σ-étale if and only if $G^o = 1$.

In this section we discuss the σ-identity component. It plays a crucial role in our decomposition theorem (Theorem 6.38). The σ-identity component was already used in [1] to derive a necessary condition on a σ-algebraic group to be a σ-Galois group over the difference-differential field $\mathbb{C}(x)$ with derivation $\delta = \frac{\mathrm{d}}{\mathrm{d}\,x}$ and endomorphism σ given by $\sigma(f(x)) = f(x+1)$. Some difference algebraic results necessary to define the difference identity component also already appeared in [29].

We will give a difference topological interpretation of the difference identity component. Therefore, we begin with some general difference topological definitions and observations.

3.1. The difference topology

Let X be a topological space equipped with a continuous endomorphism $\sigma\colon X \to X$. In this situation we may call X a *σ-topological space*. A morphism of σ-topological spaces is a continuous map that commutes with the action of σ. A subset V of X is called *σ-invariant* if $\sigma(V) \subseteq V$. We call V *σ-closed* if it is closed and σ-invariant. The *σ-topology* on X is the topology on X whose closed sets are the σ-closed sets. The *σ-connected components* of X are the connected components with respect to the σ-topology. We call X *σ-connected* if X is connected with respect to the σ-topology.

We are mainly interested in the following example: For a σ-ring R, $\operatorname{Spec}(R)$ is a naturally a σ-topological space. The topology is the usual Zariski topology and

$$\sigma\colon \operatorname{Spec}(R) \to \operatorname{Spec}(R),\ \mathfrak{p} \mapsto \sigma^{-1}(\mathfrak{p})$$

is the continuous endomorphism induced by $\sigma\colon R \to R$.

For a subset B of R, let us denote with $\mathcal{V}(B) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid B \subseteq \mathfrak{p}\}$ the closed subset of $\operatorname{Spec}(R)$ defined by B. The map $\mathfrak{a} \mapsto \mathcal{V}(\mathfrak{a})$ is a bijection between the set of radical σ-ideals of R and the set of σ-closed subsets of $\mathrm{Spec}(R)$.

Our first goal is to express the property that $\mathrm{Spec}(R)$ is σ-connected via difference algebraic conditions on R. Recall that an element e of a ring is called *idempotent* if $e^2 = e$. The *trivial* idempotents are 1 and 0. The spectrum of a ring R is connected if and only if R has no non-trivial idempotent elements ([26, Lemma 10.21.4] or [31, Section 5.5]). We will prove a difference analog of this result.

An element f of a σ-ring R is called *constant* if $\sigma(f) = f$. The subring of all constant elements is denoted by R^σ.

Proposition 3.1. — *Let R be a σ-ring. If $e \in R$ is a non-trivial constant idempotent element, then*

$$\mathrm{Spec}(R) = \mathcal{V}(e) \uplus \mathcal{V}(1-e)$$

is a decomposition of $\mathrm{Spec}(R)$ *into disjoint non-empty σ-closed subsets. Conversely, if* $\mathrm{Spec}(R) = X \uplus Y$ *is a decomposition of* $\mathrm{Spec}(R)$ *into disjoint non-empty σ-closed subsets, then there exists a non-trivial constant idempotent element $e \in R$ such that $X = \mathcal{V}(e)$ and $Y = \mathcal{V}(1-e)$.*

Proof. — Set $e' = 1-e$. Then also e' is constant and idempotent. Because e is constant, the ideal generated by e is a σ-ideal and therefore $\mathcal{V}(e)$ is σ-closed. Similarly, $\mathcal{V}(e')$ is σ-closed. Since $ee' = 0$, every $\mathfrak{p} \in \mathrm{Spec}(R)$ is contained in $\mathcal{V}(e)$ or $\mathcal{V}(e')$. Since $e + e' = 1$, no $\mathfrak{p}$ can be contained in $\mathcal{V}(e)$ and $\mathcal{V}(e)$. Thus $\mathrm{Spec}(R)$ is the disjoint union of the σ-closed sets $\mathcal{V}(e)$ and $\mathcal{V}(e')$.

Suppose $\mathcal{V}(e) = \emptyset$. Then 1 must lie in the ideal generated by e. So $1 = re$ for some $r \in R$. Therefore $e = re^2 = re$. Combining the last two equations yields $e = 1$; a contradiction. Suppose $\mathcal{V}(e) = \mathrm{Spec}(R)$. Then e must lie in the nilradical of R. Because e is idempotent this implies $e = 0$; again a contradiction.

Now assume that $\mathrm{Spec}(R) = X \uplus Y$ is a decomposition of $\mathrm{Spec}(R)$ into disjoint non-empty σ-closed subsets. It is known that any decomposition of $\mathrm{Spec}(R)$ into two disjoint non-empty closed subsets arises from a pair e, e' of non-trivial idempotent elements with $ee' = 0$ and $e + e' = 1$ ([26, Lemma 10.21.3] or [31, Section 5.5]). So $X = \mathcal{V}(e)$ and $Y = \mathcal{V}(e')$. It remains to show that e is constant.

Let $\mathfrak{p} \in X = \mathcal{V}(e)$. Since X is σ-invariant, $\sigma^{-1}(\mathfrak{p}) \in X$, i.e., $e \in \sigma^{-1}(\mathfrak{p})$. Thus $\sigma(e) \in \mathfrak{p}$ and $\mathcal{V}(e) \subseteq \mathcal{V}(\sigma(e))$. Similarly, one shows $\mathcal{V}(e') \subseteq \mathcal{V}(\sigma(e'))$. Because $\sigma(e)\sigma(e') = 0$ and $\sigma(e) + \sigma(e') = 1$, we have $\mathrm{Spec}(R) = \mathcal{V}(\sigma(e)) \uplus \mathcal{V}(\sigma(e'))$. This implies $\mathcal{V}(e) = \mathcal{V}(\sigma(e))$ and $\mathcal{V}(e') = \mathcal{V}(\sigma(e'))$. Consequently

$\sqrt{(e)} = \sqrt{(\sigma(e))}$. Because e is idempotent, it follows that $e = a\sigma(e)$ for some $a \in R$. Since $(1-\sigma(e))\sigma(e) = 0$, this implies $(1-\sigma(e))e = 0$. Interchanging the roles of e and $\sigma(e)$ in the last argument, we find $(1-e)\sigma(e) = 0$. Taking the difference of the last two equations yields $\sigma(e) = e$ as desired. □

From Proposition 3.1 we immediately obtain:

Corollary 3.2. — *Let R be a σ-ring. Then* $\operatorname{Spec}(R)$ *is σ-connected if and only if R contains no non-trivial constant idempotent element.*

Recall that idempotent elements $e_1, \dots, e_n$ of a ring R are called *orthogonal* if $e_ie_j = 0$ for $i \neq j$.

Proposition 3.3. — *Let R be a σ-ring and let $e_1, \dots, e_n \in R$ be constant orthogonal idempotent elements with $e_1 + \cdots + e_n = 1$ such that no e_i can be written as a sum of two non-trivial constant orthogonal idempotent elements. Then the σ-connected components of* $\operatorname{Spec}(R)$ *are $\mathcal{V}(1-e_1), \dots, \mathcal{V}(1-e_n)$. Moreover, e_iR is naturally a σ-ring and* $\operatorname{Spec}(e_iR)$ *is isomorphic to $\mathcal{V}(1-e_i)$ as a σ-topological space.*

Proof. — Note that e_iR is a σ-ideal of R but not a σ-subring of R (because the identity elements differ). However, e_iR is also a σ-ring with identity element e_i. As e_iR and $R/(1-e_i)$ are isomorphic as σ-rings, we see that $\operatorname{Spec}(e_iR)$ and $\mathcal{V}(1-e_i)$ are isomorphic as σ-topological spaces.

Assume $e \in e_iR$ is a constant idempotent element. Then $e_i = e_ie + e_i(1-e)$ expresses e_i as a sum of orthogonal constant idempotent elements. By assumption $e_ie = e_i$ or $e_ie = 0$. But $e_ie = e$, so $e = e_i$ or $e = 0$. It follows from Corollary 3.2 that $\mathcal{V}(1-e_i) \simeq \operatorname{Spec}(e_iR)$ is σ-connected.

Because the e_i's are orthogonal, the $\mathcal{V}(1-e_i)$'s are disjoint and because $e_1 + \cdots + e_n = 1$, their union equals $\operatorname{Spec}(R)$. In summary we see that the $\mathcal{V}(1-e_i)$'s are the σ-connected components of $\operatorname{Spec}(R)$. □

To show that $\operatorname{Spec}([\sigma]_kT)$ is σ-connected for any k-algebra T, we will need the following result.

Lemma 3.4. — *Let T be a k-algebra. Then $([\sigma]_kT)^\sigma = k^\sigma$.*

Proof. — Let $(v_i)_{i\in I}$ be a k-basis of $T \subseteq [\sigma]_kT$ that contains 1. For $n \geqslant 0$ and $i = (i_0, \dots, i_n) \in I^{n+1}$ define $v_{\mathbf{i}} = v_{i_0}\sigma(v_{i_1})\cdots\sigma^n(v_{i_n})$. By construction of $T[n]$ (Section 2.1), $V_n := (v_i)_{i\in I^{n+1}}$ is a k-basis of $T[n]$. Because $(v_i)_{i\in I}$ contains 1, we have $V_n \subseteq V_{n+1}$ and $\sigma(V_n) \subseteq V_{n+1}$.

Let a be a constant element of $[\sigma]_kT$ and suppose a does not lie in k. Let $n \geqslant 0$ be minimal such that $a \in T[n]$. Then we can write $a = \sum_{v\in V_n} \lambda_v v$

with $\lambda_v \in k$, where, for some $v \in V_n \smallsetminus V_{n-1}$, the coefficient λ_v is non-zero. As a is constant

$$a = \sum_{v \in V_n} \sigma(\lambda_v)\sigma(v) \tag{3.1}$$

If $v \in V_n \smallsetminus V_{n-1}$, then $\sigma(v) \in V_{n+1} \smallsetminus V_n$. Therefore equation (3.1) shows that $a \notin T[n]$, a contradiction. □

The following corollary shows that σ-connectedness is a concept that truly belongs to the σ-world. The connectedness of $\mathrm{Spec}(T)$ and the σ-connectedness of $\mathrm{Spec}([\sigma]_k T)$ are unrelated.

Corollary 3.5. — *Let T be a k-algebra. Then* $\mathrm{Spec}([\sigma]_k T)$ *is σ-connected.*

Proof. — By Corollary 3.2 it suffices to show that $[\sigma]_k T$ has no non-trivial constant idempotent element. But by Proposition 3.4 every constant idempotent of $[\sigma]_k T$ belongs to k and must therefore be trivial. □

3.2. Strongly étale difference algebras and the strong core

To motivate the definitions in this subsection, let us recall a possible path to the definition of the connected component $\mathcal{G}^o$ of an algebraic group $\mathcal{G}$. See e.g., [31, Chapter 6]. Instead of defining $\mathcal{G}^o$ directly, one first constructs the coordinate ring of $\mathcal{G}/\mathcal{G}^o$. Let $\pi_0(k[\mathcal{G}])$ be the union of all étale k-subalgebras of $k[\mathcal{G}]$. One shows that $\pi_0(k[\mathcal{G}])$ is an étale k-algebra and a Hopf subalgebra of $k[\mathcal{G}]$. One can then define $\mathcal{G}^o$ as the kernel of the morphism $\mathcal{G} \to \pi_0(\mathcal{G})$ of algebraic groups corresponding to the inclusion $\pi_0(k[\mathcal{G}]) \subseteq k[\mathcal{G}]$ of Hopf algebras.

We will follow here a similar path. The first step is to clarify, what is the appropriate difference analog of an étale k-algebra in our context. This question is addressed in the following definitions.

Definition 3.6. — *A k-σ-algebra R is* σ-separable *(over k) if the map $\sigma\colon R \otimes_k k' \to R \otimes_k k'$ is injective for every σ-field extension k' of k.*

See [29, Proposition 1.2] for other equivalent characterizations of σ-separable k-σ-algebras. E.g., a k-σ-algebra R is σ-separable if and only if the map $\overline{\sigma}\colon {}^{\sigma}\!R \to R,\ f \otimes \lambda \mapsto \sigma(f)\lambda$ is injective. Here ${}^{\sigma}\!R = R \otimes_k k$ is the base change of R via $\sigma\colon k \to k$.

Recall ([3, Chapter V, §6]) that a k-algebra T is *étale* if $T \otimes_k \overline{k}$ is isomorphic (as a $\overline{k}$-algebra) to a finite direct product of copies of the algebraic closure $\overline{k}$ of k. (In particular, T is finite dimensional as a k-vector space.) Following [29, Definition 1.7] we make the following definition.

Definition 3.7. — *A k-σ-algebra is* strongly σ-étale *if it is σ-separable over k and étale as a k-algebra. A σ-algebraic group G is* strongly σ-étale *if $k\{G\}$ is strongly σ-étale.*

Let us see some examples of strongly σ-étale σ-algebraic groups.

Example 3.8. — Let $0 \leqslant \alpha < n$ and $m \geqslant 1$ be integers and let G be the σ-closed subgroup of the multiplicative group $\mathbb{G}_m$ given by

$$G(R) = \{g \in R^\times \mid g^n = 1,\ \sigma^m(g) = g^\alpha\}$$

for any k-σ-algebra R. Then $k\{G\} = k[x, \sigma(x), \ldots, \sigma^{m-1}(x)]$, where x denotes the image of the coordinate function on $\mathbb{G}_m$. Let us assume that the characteristic of k is zero or does not divide n. Then the polynomial $y^n - 1$ is separable over k and it follows that $k\{G\}$ is an étale k-algebra.

We claim that G is strongly σ-étale if and only if α and n are relatively prime. Indeed, if there are $a, b \in \mathbb{N}$ with $1 \leqslant a < n$ and $\alpha a = bn$, then

$$\sigma(\sigma^{m-1}(x)^a - 1) = x^{\alpha a} - 1 = x^{bn} - 1 = 0$$

and so σ is not injective on $k\{G\}$ and therefore G is not strongly σ-étale. On the other hand, if $1 = a\alpha + bn$ for $a, b \in \mathbb{Z}$, then

$$\sigma(\sigma^{m-1}(x)^a) = \sigma^m(x)^a = x^{a\alpha} = x^{a\alpha}x^{bn} = x.$$

This shows that ${}^\sigma(k\{G\}) \to k\{G\}$ is surjective. Because ${}^\sigma(k\{G\}) \to k\{G\}$ is a morphism of finite dimensional k-algebras, it must then also be injective. So $k\{G\}$ is σ-separable and therefore strongly σ-étale.

Example 3.9. — Let $\mathtt{G}$ be a finite group with an endomorphism $\sigma\colon \mathtt{G} \to \mathtt{G}$ and let G be the σ-algebraic group associated to these data as in Example 2.6. We claim that G is strongly σ-étale if and only if $\sigma\colon \mathtt{G} \to \mathtt{G}$ is an automorphism. Clearly $k\{G\} = k^{\mathtt{G}}$ is étale, so the question is about the σ-separability of $k\{G\}$.

If $\sigma\colon \mathtt{G} \to \mathtt{G}$ is not an automorphism, there exist a $g \in \mathtt{G}$ that does not lie in the image of $\sigma\colon \mathtt{G} \to \mathtt{G}$. Define $h\colon \mathtt{G} \to k$ by

$$h(g') = \begin{cases} 1 \text{ if } g' = g, \\ 0 \text{ otherwise.} \end{cases}$$

Then $\sigma(h)(g') = \sigma(h(\sigma(g'))) = \sigma(0) = 0$ for any $g' \in \mathtt{G}$. Thus $\sigma(h) = 0$ and $\sigma\colon k\{G\} \to k\{G\}$ is not injective. So G is not strongly σ-étale.

Conversely, if $\sigma\colon \mathtt{G} \to \mathtt{G}$ is an automorphism, then ${}^\sigma(k\{G\}) \to k\{G\}$ is an isomorphism. Therefore $k\{G\}$ is σ-separable and so strongly σ-étale.

We proceed on our path to define the σ-identity component.

Definition 3.10 ([29, Definition 1.17]). — *Let R be a k-σ-algebra. The union $\pi_0^\sigma(R)=\pi_0^\sigma(R|k)$ of all strongly σ-étale k-σ-subalgebras of R is called the* strong core *of R.*

The strong core $\pi_0^\sigma(R)$ of R is a σ-separable k-σ-subalgebra of R ([29, Remark 1.18]). It is however an open problem if $\pi_0^\sigma(R)$ is strongly σ-étale (equivalently, finite dimensional as a k-vector space) if R is finitely σ-generated ([29, Conjecture 1.19]). However, if R is a finitely σ-generated k-σ-Hopf algebra, then $\pi_0^\sigma(R)$ is strongly σ-étale ([29, Theorem 3.2]).

The strong core has good functorial properties:

Lemma 3.11 ([29, Lemma 1.25]). — *Let R and S be k-σ-algebras. Then*

$$\pi_0^\sigma(R\otimes_k S)=\pi_0^\sigma(R)\otimes_k\pi_0^\sigma(S).$$

Lemma 3.12 ([29, Lemma 1.24]). — *Let R be a k-σ-algebra and let k' be a σ-field extension of k. Then*

$$\pi_0^\sigma(R\otimes_k k'|k')=\pi_0^\sigma(R|k)\otimes_k k'.$$

The following proposition allows us to define the σ-identity component and the group of σ-connected components of a σ-algebraic group. It is a difference analog of [31, Theorem 6.7].

Proposition 3.13. — *Let G be a σ-algebraic group. Among the morphisms from G to strongly σ-étale σ-algebraic groups there exists a universal one.*

In more detail: There exists a strongly σ-étale σ-algebraic group $\pi_0^\sigma(G)$, together with a morphism $G\to\pi_0^\sigma(G)$ of σ-algebraic groups such that for every morphism $G\to H$ of σ-algebraic groups with H strongly σ-étale, there exists a unique morphism $\pi_0^\sigma(G)\to H$ making

$$\begin{tikzcd} G \arrow[rr] \arrow[dr] & & \pi_0^\sigma(G) \arrow[dl, dotted] \\ & H & \end{tikzcd}$$

commutative.

Proof. — This was already proved in [1, Proposition 6.5]. For the convenience of the reader and because it is instructive, we sketch the proof: Using Lemma 3.11 one shows that $\pi_0^\sigma(k\{G\})$ is a k-σ-Hopf subalgebra. By Theorem 2.12 it is finitely σ-generated. Because $\pi_0^\sigma(k\{G\})$ is a union of k-σ-algebras that are finite dimensional k-vector spaces, it follows from the finite σ-generation that in fact $\pi_0^\sigma(k\{G\})$ is a finite dimensional k-vector space. Thus $\pi_0^\sigma(k\{G\})$ is strongly σ-étale and corresponds to a strongly σ-étale σ-algebraic group $\pi_0^\sigma(G)$. The inclusion $\pi_0^\sigma(k\{G\}) \subseteq k\{G\}$ correspond to a morphism $G \to \pi_0^\sigma(G)$ of σ-algebraic groups.

Let $k\{H\}$ be a strongly σ-étale k-σ-Hopf algebra and $k\{H\} \to k\{G\}$ a morphism of k-σ-Hopf algebras. Since quotients of strongly σ-étale k-σ-algebras are strongly σ-étale ([29, Lemma 1.15]), the image of $k\{H\}$ in $k\{G\}$ is strongly σ-étale, i.e., contained in $\pi_0^\sigma(k\{G\})$. In other words, the map $k\{H\} \to k\{G\}$, factors uniquely through the inclusion $\pi_0^\sigma(k\{G\}) \subseteq k\{G\}$. Dualizing yields the required universal property. □

As a corollary to the above proof we obtain:

Corollary 3.14. — *Let G be a σ-algebraic group. Then $\pi_0^\sigma(k\{G\})$ is strongly σ-étale.*

The reader may wonder about the significance of the σ-separability assumption in Definition 3.7. Indeed, one may wonder if only working with k-σ-subalgebras that are étale as k-algebras (and not necessarily strongly σ-étale) leads to similar results. The following example shows that this is not the case.

Example 3.15. — Let G be the σ-algebraic subgroup of $\mathbb{G}_m^2$ given by

$$G(R) = \left\{ \begin{pmatrix} g_1 \\ g_2 \end{pmatrix} \in \mathbb{G}_m^2(R) \;\middle|\; g_1^2 = 1,\ \sigma(g_1) = 1,\ g_2^2 = 1 \right\}$$

for any k-σ-algebra R. Let S denote the union of all k-σ-subalgebras of $k\{G\}$ that are étale as k-algebras. Then S is a k-σ-subalgebra of $k\{G\}$. However, as we will show, S is not a k-σ-Hopf subalgebra of $k\{G\}$.

Let us assume that the characteristic of k is not equal to 2. With $H_1(R) = \{g \in \mathbb{G}_m(R) \mid g^2 = 1,\ \sigma(g) = 1\}$ and $H_2(R) = \{g \in \mathbb{G}_m(R) \mid g^2 = 1\}$ we have $G = H_1 \times H_2$. Moreover,

$$\begin{aligned} k\{H_1\} &= k\{y\}/[y^2 - 1,\ \sigma(y) - 1] = k[y]/(y^2 - 1) \\ &= k[y]/(y - 1) \oplus k[y]/(y + 1) \simeq k \oplus k. \end{aligned}$$

Thus, if e_1 and e_2 denote the images of $\frac{1+y}{2}$ and $\frac{1-y}{2}$ in $k\{H_1\}$ respectively, then e_1 and e_2 are orthogonal idempotent elements of $k\{H_1\}$ with $\sigma(e_1) = 1$, $\sigma(e_2) = 0$ and $k\{H_1\} = ke_1 \oplus ke_2$. We have

$$k\{G\} = k\{H_1\} \otimes_k k\{H_2\} = (e_1 \otimes k\{H_2\}) \oplus (e_2 \otimes k\{H_2\}).$$

For any element $a \in e_2 \otimes k\{H_2\}$ we have $\sigma(a) = 0$ and so $k\{a\} = k[a]$ is a k-σ-algebra that is étale as a k-algebra. This shows that $e_2 \otimes k\{H_2\}$ is contained in S. In particular, S has infinite dimension as a k-vector space, because $k\{H_2\} = k\{y\}/[y^2-1]$ has infinite dimension as a k-vector space.

Suppose S is a k-σ-Hopf subalgebra of $k\{G\}$. Then S is finitely σ-generated over k by Theorem 2.12 and it follows that S is a finite dimensional k-vector space; a contradiction. So S is not a k-σ-Hopf subalgebra of $k\{G\}$.

3.3. The difference identity component and the group of difference connected components

Definition 3.16. — *Let G be a σ-algebraic group. The σ-algebraic group $\pi_0^\sigma(G)$ from Proposition 3.13 is called the* group of σ-connected components *of G. The kernel $G^{\sigma o}$ of $G \to \pi_0^\sigma(G)$ is called the* σ-identity component *of G.*

So $k\{\pi_0^\sigma(G)\} = \pi_0^\sigma(k\{G\})$ and $\pi_0^\sigma(G)$ is strongly σ-étale. Moreover the morphism $G \to \pi_0^\sigma(G)$ is a quotient map and $G/G^{\sigma o} = \pi_0^\sigma(G)$.

Our next goal is to connect $\pi_0^\sigma(G)$ with the σ-topology on $\operatorname{Spec}(k\{G\})$. In particular, we will see that $\pi_0^\sigma(G) = 1$ if and only if $\operatorname{Spec}(k\{G\})$ is σ-connected. To this end we need some preparatory results.

Recall that a non-zero idempotent element e is *primitive* if it cannot be written as $e = e' + e''$ for non-zero orthogonal idempotent elements e' and e''. In an étale k-algebra the set $\{e_1, \ldots, e_n\}$ of primitive idempotent elements is finite. Moreover, the e_i's are orthogonal and $e_1 + \cdots + e_n = 1$.

Lemma 3.17 ([29, Lemma 1.11]). — *Let R be a strongly σ-étale k-σ-algebra. Then σ induces a bijection on the set of primitive idempotent elements of R.*

Lemma 3.18. — *Let R be a strongly σ-étale k-σ-algebra and let us denote with $d_1, \ldots, d_m \in R$ the primitive idempotent elements of R. Let $A_1 \uplus \cdots \uplus A_n = \{1, \ldots, m\}$ be the partition of $\{1, \ldots, m\}$ corresponding to the cycle decomposition of the permutation τ of the d_i's induced by σ (cf. Lemma 3.17). For $i = 1, \ldots, n$ let $e_i = \sum_{j \in A_i} d_j$.*

Then $e_1, \ldots, e_n$ are constant orthogonal idempotent elements with $e_1 + \cdots + e_n = 1$ such that no e_i can be written as a sum of two non-trivial constant orthogonal idempotent elements.

Proof. — The e_i's are constant because the A_i's are the orbits of τ. Since the d_j's are orthogonal and the A_i's are disjoint, also the e_i's are orthogonal. We have $e_1 + \cdots + e_n = d_1 + \cdots + d_m = 1$. Any constant idempotent element of R is a sum of some e_i's, so no e_i can be written as a sum of two non-trivial constant orthogonal idempotent elements. $\square$

Proposition 3.19. — *Let R be a k-σ-algebra such that $\pi_0^\sigma(R)$ is strongly σ-étale. Let $e_1,\ldots,e_n \in \pi_0^\sigma(R)$ be as in Lemma 3.18. Then the σ-connected components of* $\operatorname{Spec}(R)$ *are* $\mathcal{V}(1-e_1),\ldots,\mathcal{V}(1-e_n)$. *Moreover* $\mathcal{V}(1-e_i)$ *is isomorphic to* $\operatorname{Spec}(e_iR)$ *as a σ-topological space.*

Proof. — By [29, Lemma 1.12] all the constant idempotent elements of R belong to $\pi_0^\sigma(R)$. So by Lemma 3.18 the constant idempotent elements $e_1,\ldots,e_n$ satisfy the condition of Proposition 3.3. □

The *topological space of a σ-algebraic group G* is $\operatorname{Spec}(k\{G\})$ (equipped with the Zariski topology). As in Section 3.1 above, we consider $\operatorname{Spec}(k\{G\})$ as a σ-topological space.

Theorem 3.20. — *Let G be a σ-algebraic group. Then the topological space of G has only finitely many σ-connected components. Moreover, the topological space of $G^{\sigma o}$ is isomorphic (as a σ-topological space) to the σ-connected component of the topological space of G that contains the identity, i.e., the kernel $\mathfrak{m}_G$ of the counit $\varepsilon\colon k\{G\}\to k$.*

Proof. — As $\pi_0^\sigma(k\{G\})$ is strongly σ-étale (Corollary 3.14), the first statement follows immediately from Theorem 3.19. Let $d_1,\ldots,d_m\in\pi_0^\sigma(k\{G\})$ and $e_1,\ldots,e_n \in \pi_0^\sigma(k\{G\})$ be as in Lemma 3.18. Then the counit $\varepsilon\colon \pi_0^\sigma(k\{G\})\to k$ maps precisely one d_i to $1\in k$ and all other d_i's to 0. We may assume that $\varepsilon(d_1)=1$. By Lemma 3.17 we have $\sigma(d_1)\in\{d_1,\ldots,d_m\}$. As $\varepsilon(\sigma(d_1))=\sigma(\varepsilon(d_1))=\sigma(1)=1$, this shows that $\sigma(d_1)=d_1$. So $e_1=d_1$. The kernel of ε on $\pi_0^\sigma(k\{G\})$ is the ideal generated by $1-e_1$. So, by the definition of $G^{\sigma o}$, we have $\mathbb{I}(G^{\sigma o})=(1-e_1)\subset k\{G\}$. Therefore $k\{G^{\sigma o}\}=k\{G\}/(1-e_1)$ and consequently $\operatorname{Spec}(k\{G^{\sigma o}\})$ is isomorphic to $\mathcal{V}(1-e_1)\subseteq \operatorname{Spec}(k\{G\})$. We know from Proposition 3.19 that $\mathcal{V}(1-e_1)$ is a σ-connected component and clearly $\mathfrak{m}_G\in\mathcal{V}(1-e_1)$. □

There does not seem to be an easy formula for the number of σ-connected components. Indeed, the following example illustrates that the number of σ-connected components does not only depend on the underlying field of the base difference field, but it also depends on the endomorphism $\sigma\colon k\to k$.

Example 3.21. — Let $k=\mathbb{Q}$ (considered as a constant σ-field). Let G be the σ-closed subgroup of $\mathbb{G}_m$ given by

$$G(R)=\{g\in R^\times \mid g^3=1,\ \sigma(g)=g\}$$

for any k-σ-algebra R. Then $\operatorname{Spec}(k\{G\})$ consists of two elements and σ is the identity map on $\operatorname{Spec}(k\{G\})$. Thus G has two σ-connected components.

Now assume k is a σ-field of characteristic zero that contains the two non-trivial third roots of unity a_1 and a_2. Then $\operatorname{Spec}(k\{G\})$ consists of three elements. The endomorphism σ either permutes or fixes a_1 and a_2. If σ fixes a_1 and a_2, then σ is the identity map on $\operatorname{Spec}(k\{G\})$ and G has three σ-connected components. If σ permutes a_1 and a_2, then G has two σ-connected components. In particular, in this case the number of σ-connected components of G is strictly smaller than the vector space dimension of $\pi_0^\sigma(k\{G\}) = k\{G\}$.

We next characterize σ-connected σ-algebraic groups.

Lemma 3.22. — *For a σ-algebraic group G, the following statements are equivalent:*

(i) *The topological space of G is σ-connected.*
(ii) $G = G^{\sigma o}$.
(iii) $\pi_0^\sigma(G) = 1$.

Proof. — The equivalence of (ii) and (iii) is tautological. The implication (iii) $\Rightarrow$ (i) follows from the fact that the topological space of $G^{\sigma o}$ is σ-connected by Theorem 3.20

Finally, let us show that (i) implies (iii). Let $d_1, \ldots, d_m \in \pi_0^\sigma(k\{G\})$ and $e_1, \ldots, e_n \in \pi_0^\sigma(k\{G\})$ be as in Lemma 3.18. Then

$$\pi_0^\sigma(k\{G\}) = e_1\pi_0^\sigma(k\{G\}) \times \cdots \times e_n\pi_0^\sigma(k\{G\})$$

and as in the proof of Theorem 3.20 we have $e_1 = d_1$. So

$$e_1\pi_0^\sigma(k\{G\}) = d_1\pi_0^\sigma(k\{G\})$$

is a finite separable field extension of k (because $\pi_0^\sigma(k\{G\})$ is an étale k-algebra). But the counit ε identifies $e_1\pi_0^\sigma(k\{G\}) = \pi_0^\sigma(k\{G\})/(1-e_1)$ with k. So $e_1\pi_0^\sigma(k\{G\}) = e_1k \simeq k$. We know from Proposition 3.19 that G has n σ-connected components. By assumption $n = 1$. So $\pi_0^\sigma(k\{G\}) = k$. $\square$

Definition 3.23. — *A σ-algebraic group satisfying the equivalent conditions of Lemma 3.22 is called* σ-connected.

As an immediate corollary to Theorem 3.20 we obtain:

Corollary 3.24. — *Let G be a σ-algebraic group. Then $G^{\sigma o}$ is σ-connected.*

Example 3.25. — Let $\mathcal{G}$ be an algebraic group. Then $[\sigma]_k\mathcal{G}$ is a σ-connected σ-algebraic group by Corollary 3.5.

Example 3.26. — The σ-algebraic group G from Example 3.15 is σ-connected. With the notation of Example 3.15, we clearly have $\pi_0^\sigma(k\{H_1\}) = k$. Note that H_2 is the algebraic group of order two, considered as a σ-algebraic group. So it follows from Example 3.25 that $\pi_0^\sigma(k\{H_2\}) = k$. Finally, using Lemma 3.11 we find

$$\pi_0^\sigma(k\{G\}) = \pi_0^\sigma(k\{H_1\} \otimes_k k\{H_2\}) = \pi_0^\sigma(k\{H_1\}) \otimes_k \pi_0^\sigma(k\{H_2\}) = k.$$

Example 3.27. — Let $n \geqslant 2$ be an integer and let G be the σ-algebraic group given by

$$G(R) = \{g \in R^\times \mid g^n = 1,\ \sigma(g) = 1\} \leqslant \mathbb{G}_m(R)$$

for any k-σ-algebra R. We claim that G is σ-connected. Let $x \in k\{G\}$ denote the image of the coordinate function on $\mathbb{G}_m$. Then $k\{G\} = k\{x\} = k[x]$ with $\sigma(x) = 1$ and $x^n = 1$. Clearly, $\sigma(x-1) = 0$. Since $\mathfrak{m}_G = (x-1)$ is a maximal ideal of $k\{G\}$, the kernel of σ on $k\{G\}$ is $\mathfrak{m}_G$. Therefore $\sigma^{-1}(\mathfrak{p}) = \mathfrak{m}_G$ for every prime ideal $\mathfrak{p}$ of $k\{G\}$. Now $\operatorname{Spec}(k\{G\})$ is a discrete topological space. Suppose X_1 and X_2 are non-empty disjoint σ-invariant subsets of $\operatorname{Spec}(k\{G\})$. A point x_1 from X_1 is mapped onto $\mathfrak{m}_G$ under σ, similarly for a point x_2 from X_2. So $\mathfrak{m}_G$ lies in the intersection of X_1 and X_2; a contradiction. Thus G is σ-connected.

An example of a σ-algebraic group that is not σ-connected can be deduced from Example 3.8:

Example 3.28. — Let G be the σ-algebraic group from Example 3.8 with $\alpha = 1$. Then $\pi_0^\sigma(G) = G$ and so $G^{\sigma o} = 1$. In particular, G is not σ-connected.

The formation of $\pi_0^\sigma(G)$ and $G^{\sigma o}$ is compatible with base extension:

Proposition 3.29. — *Let G be a σ-algebraic group and k' a σ-field extension of k. Then*

$$\pi_0^\sigma(G_{k'}) = \pi_0^\sigma(G)_{k'} \quad \text{and} \quad (G^{\sigma o})_{k'} = (G_{k'})^{\sigma o}.$$

Proof. — This is clear from Lemma 3.12. □

A connected algebraic group is geometrically connected ([20, Proposition 1.34]). From Proposition 3.29 we obtain a similar result in our setting:

Corollary 3.30. — *Let G be a σ-connected σ-algebraic group. Then $G_{k'}$ is σ-connected for every σ-field extension k' of k.*

Recall ([32, Definition 6.15]) that a σ-closed subgroup H of a σ-algebraic group G is *characteristic* if for every k-σ-algebra R, every automorphism of G_R induces an automorphism of H_R.

Theorem 3.31. — *Let G be a σ-algebraic group. Then $G^{\sigma o}$ is a characteristic subgroup of G.*

Proof. — By Lemma [32, Lemma 6.16] it suffices to show that for every k-σ-algebra R, every automorphism ψ of the R-σ-Hopf algebra $k\{G\}\otimes_k R$ maps $\pi_0^\sigma(k\{G\})\otimes_k R$ into $\pi_0^\sigma(k\{G\})\otimes_k R$. Since ψ is an automorphism of the k-σ-algebra $k\{G\}\otimes_k R$, we have $\psi(\pi_0^\sigma(k\{G\}\otimes_k R))\subseteq \pi_0^\sigma(k\{G\}\otimes_k R)$. Using Lemma 3.11, we obtain

$$\begin{aligned}\psi(\pi_0^\sigma(k\{G\})\otimes 1)\subseteq \psi(\pi_0^\sigma(k\{G\}\otimes_k R))&\subseteq \pi_0^\sigma(k\{G\}\otimes_k R)\\ &=\pi_0^\sigma(k\{G\})\otimes_k \pi_0^\sigma(R)\subseteq \pi_0^\sigma(k\{G\})\otimes_k R.\end{aligned}$$

Thus $\psi(\pi_0^\sigma(k\{G\})\otimes_k R)\subseteq \pi_0^\sigma(k\{G\})\otimes_k R$ as required. $\square$

The three basic numerical invariants for σ-algebraic groups do not change when passing to the σ-identity component.

Proposition 3.32. — *Let G be a σ-algebraic group. Then*

$$\sigma\text{-}\dim(G^{\sigma o})k=\sigma\text{-}\dim(G),\quad \operatorname{ord}(G^{\sigma o})=\operatorname{ord}(G)\quad \textit{and}\quad \operatorname{ld}(G^{\sigma o})=\operatorname{ld}(G).$$

Proof. — By Proposition 2.14 it suffices to show that $\sigma\text{-}\dim(\pi_0^\sigma(G))=0$, $\operatorname{ord}(\pi_0^\sigma(G))=0$ and $\operatorname{ld}(\pi_0^\sigma(G))=1$. Clearly a strongly σ-étale σ-algebraic group has σ-dimension zero and order zero. Furthermore, a strongly σ-étale σ-algebraic group has limit degree one by Lemma 2.10. $\square$

The following two propositions are useful for determining the σ-identity component in concrete examples. Proposition 3.33 is a difference analog of [20, Proposition 5.58], while Proposition 3.35 is a difference analog of [20, Proposition 5.59].

Proposition 3.33. — *Let G be a σ-algebraic group. If N is a normal σ-connected σ-closed subgroup of G such that G/N is strongly σ-étale, then $N=G^{\sigma o}$.*

Proof. — As G/N is strongly σ-étale, we obtain from Proposition 3.13 a commutative diagram

$$\begin{tikzcd} G \arrow[rr] \arrow[dr] & & \pi_0^\sigma(G) \arrow[dl, dotted] \\ & G/N & \end{tikzcd}$$

Hence $G^{\sigma o}\leqslant N$. On the other hand, the image of N under the morphism $G\to\pi_0^\sigma(G)$ is trivial because N is σ-connected, and so $N\leqslant G^{\sigma o}$. $\square$

For any σ-algebraic group G, there exists a unique (up to isomorphism) exact sequence

$$1\to G^{\sigma o}\to G\to \pi_0^\sigma(G)\to 1$$

with $G^{\sigma o}$ σ-connected and $\pi_0^\sigma(G)$ strongly σ-étale. The existence follows from Proposition 3.13 and Corollary 3.24, while the uniqueness follows from Proposition 3.33 (or directly from Proposition 3.13).

The following example shows how Proposition 3.33 can be used to determine the σ-identity component of a σ-algebraic group.

Example 3.34. — Let G be the σ-algebraic group given by

$$G(R) = \{g \in R^\times \mid g^4 = 1,\ g^2\sigma(g)^2 = 1\} \leqslant \mathbb{G}_m(R)$$

for any k-σ-algebra R. Let us assume that the characteristic of k is not equal to two. We will show that G is not σ-connected. Indeed, G has two σ-connected components and $G^{\sigma o}$ is given by $G^{\sigma o}(R) = \{g \in R^\times \mid g^2 = 1\}$.

Let H be the σ-algebraic group given by

$$H(R) = \{g \in R^\times \mid g^2 = 1,\ \sigma(g) = g\} \leqslant \mathbb{G}_m(R)$$

for any k-σ-algebra R. It follows from $g^4 = 1$ and $g^2\sigma(g)^2 = 1$ that $\sigma(g^2) = g^2$ in $G(R)$. Therefore we can define a morphism of σ-algebraic groups

$$\phi\colon G \to H,\ g \mapsto g^2.$$

We claim that ϕ is a quotient map. Recall ([32, Example 4.5 and Proposition 4.10]) that quotient maps are not necessarily surjective on the R-points. Indeed, to see that ϕ is a quotient map, it suffices to show that $\phi(G) = H$. As $k\{H\} = k\{y\}/[y^2-1, \sigma(y)-y] = k[y]/(y^2-1) = k \times k$, we see that the only closed subgroups of H are H itself and the trivial group. So, it suffices to show that $\phi(G)$ is not the trivial group. But for $R = k[i] = k[y]/(y^2+1)$ with $\sigma(i) = i$ and $g = i \in G(R)$ we have $\phi_R(g) = g^2 = -1 \neq 1$ and so $\phi(G)$ is not trivial.

The kernel N of ϕ is given by $N(R) = \{g \in R^\times \mid g^2 = 1\}$. It follows from Example 3.25 that N is σ-connected. Moreover, by Example 3.8 the σ-algebraic group H is strongly σ-étale. Therefore it follows from Proposition 3.33 that $G^{\sigma o} = N$ and $\pi_0^\sigma(G) = H$. As $\pi_0^\sigma(k\{G\}) = k\{H\} = k \times k$, with the two non-trivial idempotent elements being constant, it follows from Proposition 3.19 that G has two σ-connected components.

See [1, Example 6.8] for another example computation of $\pi_0^\sigma(G)$ and $G^{\sigma o}$ that uses Proposition 3.33.

Proposition 3.35. — *Let $1 \to N \to G \to H \to 1$ be an exact sequence of σ-algebraic groups. If N and H are σ-connected, then G is σ-connected. Moreover, if G is σ-connected, then H is σ-connected.*

Proof. — By Proposition 3.13, the morphism $N \to G \to \pi_0^\sigma(G)$ factors through the morphism $N \to \pi_0^\sigma(N) = 1$. So N is contained in $G^{\sigma o}$, i.e., in the kernel of $G \to \pi_0^\sigma(G)$. We therefore have an induced quotient map $G/N \to \pi_0^\sigma(G)$. But $G/N \simeq H$ is σ-connected, so $G/N \to \pi_0^\sigma(G)$ factors through $\pi_0^\sigma(G/N) = 1$. Thus $\pi_0^\sigma(G) = 1$.

For a quotient map $G \to H$, we have an inclusion $k\{H\} \subseteq k\{G\}$. So, clearly, $\pi_0^\sigma(k\{H\}) = k$ if $\pi_0^\sigma(k\{G\}) = k$. Alternatively, this also follows from Proposition 3.13, as the quotient map $G \to H \to \pi_0^\sigma(H)$ factors through $\pi_0^\sigma(G) = 1$. $\square$

The following example illustrates how Proposition 3.35 can be used to show that a σ-algebraic group is σ-connected. See Examples 6.42 and 6.43 for more example applications of Proposition 3.35.

Example 3.36. — Let G be the σ-closed subgroup of $\mathbb{G}_m$ given by

$$G(R) = \{g \in R^\times \mid g^4 = 1,\ \sigma(g)^2 = 1\} \leqslant \mathbb{G}_m(R)$$

for any k-σ-algebra R. We will show that G is σ-connected. Let H be the σ-algebraic group given by $H(R) = \{g \in R^\times \mid g^2 = 1\}$ and let $\phi\colon G \to H$ be the morphism given by

$$\phi_R\colon G(R) \to H(R),\ g \mapsto \sigma(g).$$

As

$$\begin{aligned} k\{H\} &= k\{y\}/[y^2 - 1] \\ &= k[y, \sigma(y), \sigma^2(y), \ldots]/(y^2 - 1, \sigma(y)^2 - 1, \sigma^2(y)^2 - 1, \ldots) \end{aligned}$$

and

$$\begin{aligned} k\{G\} &= k\{y\}/[y^4 - 1, \sigma(y)^2 - 1] \\ &= k[y, \sigma(y), \sigma^2(y), \ldots]/(y^4 - 1, \sigma(y)^2 - 1, \sigma^2(y)^2 - 1, \ldots), \end{aligned}$$

we see that the dual map $\phi^*\colon k\{H\} \to k\{G\},\ \bar{y} \mapsto \overline{\sigma(y)}$ is injective and so ϕ is a quotient map. The kernel N of ϕ is given by $N(R) = \{g \in R^\times \mid g^4 = 1,\ \sigma(g) = 1\}$ for any k-σ-algebra R. We have an exact sequence $1 \to N \to G \to H \to 1$. Note that $H = [\sigma]_k\mathcal{H}$ where $\mathcal{H}$ is the algebraic group given by $\mathcal{H}(T) = \{g \in T^\times \mid g^2 = 1\}$ for any k-algebra T. So it follows from Example 3.25 that H is σ-connected. Because N is σ-connected by Example 3.27, Proposition 3.35 shows that G is σ-connected.

We conclude this section with one more example computation.

Example 3.37. — Let $\mathtt{G}$ be a finite group with an endomorphism $\sigma\colon \mathtt{G} \to \mathtt{G}$ and let G be the σ-algebraic group associated to these data as in Example 2.6. We will show that G is σ-connected if and only if some power of $\sigma\colon \mathtt{G} \to \mathtt{G}$ is the trivial endomorphism ($g \mapsto 1$) of $\mathtt{G}$.

Let us start by determining the topological space of $G^{\sigma o}$. Note that $\mathrm{Spec}(k\{G\})$ is naturally in bijection with $\mathtt{G}$. We have a commutative diagram

$$\begin{tikzcd} \mathrm{Spec}(k\{G\}) \arrow[r, "\simeq"] \arrow[d, "\sigma"'] & \mathtt{G} \arrow[d, "\sigma"] \\ \mathrm{Spec}(k\{G\}) \arrow[r, "\simeq"] & \mathtt{G} \end{tikzcd}$$

Let $\mathtt{N} = \{g \in \mathtt{G} \mid \exists\, n \geqslant 1 :\ \sigma^n(g) = 1\}$. Then $\mathtt{N}$ is a normal subgroup of $\mathtt{G}$ that is invariant under σ. Because any element of $\mathtt{N}$ will eventually map to 1 under iterations of σ, we see that $\mathtt{N}$ cannot be written as a disjoint union of σ-invariant sets. As also the complement of $\mathtt{N}$ is stable under σ, we see that $\mathtt{N}$ corresponds to the σ-connected component of $\mathrm{Spec}(k\{G\})$ that contains $\mathfrak{m}_G$ under the bijection $\mathtt{G} \simeq \mathrm{Spec}(k\{G\})$. In particular, G is σ-connected if and only if $\mathtt{G} = \mathtt{N}$, i.e., some power of σ is the trivial endomorphism of $\mathtt{G}$.

The cosets $g\mathtt{N}$ of $\mathtt{N}$ in $\mathtt{G}$ need not correspond to σ-connected components of G because they may not be stable under σ. Note that the induced map $\sigma\colon \mathtt{G}/\mathtt{N} \to \mathtt{G}/\mathtt{N}$ is an automorphism (because it is injective). The σ-connected components of G are in one-to-one correspondence with the orbits of σ on $\mathtt{G}/\mathtt{N}$.

4. Basic properties of étale difference algebraic groups

In this short section we recall the definition of étale difference algebraic groups and establish some first properties.

Recall ([26, Section 61.7]) that a k-algebra T is *ind-étale* if it is a union of étale k-subalgebras. Equivalently, T is integral over k and a separable k-algebra. Yet another characterization of ind-étale k-algebras is that every element satisfies a separable polynomial over k. Following [32, Definition 6.1] we make the following definition.

Definition 4.1. — *A k-σ-algebra is* σ-étale *if it is finitely σ-generated over k and ind-étale as a k-algebra. A σ-algebraic group G is σ-étale if $k\{G\}$ is a σ-étale k-σ-algebra.*

Of course strongly σ-étale σ-algebraic groups are σ-étale. Let us see some examples of σ-étale σ-algebraic groups.

Example 4.2. — Let $\mathtt{G}$ be a finite group and $\sigma\colon \mathtt{G} \to \mathtt{G}$ a group endomorphism. Then the σ-algebraic group G constructed from these data as in Example 2.6 is a σ-étale σ-algebraic group. This is clear because $k\{G\}$ is a finite direct product of copies of k and therefore étale.

Example 4.3. — Let $n \geqslant 2$ be an integer. If the characteristic of k does not divide n, the σ-algebraic group G given by

$$G(R) = \{g \in R^\times \mid g^n = 1\} \leqslant \mathbb{G}_m(R)$$

for any k-σ-algebra R is σ-étale. To verify that $k\{G\} = k\{y\}/[y^n - 1]$ is σ-étale it suffices to observe that $k[y]/(y^n - 1)$ is an étale k-algebra because of our assumption on the characteristic.

Example 4.4. — Let $\mathcal{G}$ be an étale algebraic group. Then $G = [\sigma]_k\mathcal{G}$ is a σ-étale σ-algebraic group with $\operatorname{ld}(G) = |\mathcal{G}|$.

As $k[\mathcal{G}]$ is an étale k-algebra, also ${}^{\sigma^i}(k[\mathcal{G}])$ and $k[\mathcal{G}[i]] = k[\mathcal{G}] \otimes_k \cdots \otimes_k {}^{\sigma^i}(k[\mathcal{G}])$ are étale k-algebras for every $i \in \mathbb{N}$. Therefore $k\{G\} = \bigcup k[\mathcal{G}[i]]$ is σ-étale. The statement that $\operatorname{ld}(G) = |\mathcal{G}|$ is a special case of [34, Example 5.5].

Note that Example 4.3 can be seen as a special case of Example 4.4, as the σ-algebraic group G from Example 4.3 is of the form $G = [\sigma]_k\mathcal{G}$, with $\mathcal{G}$ the algebraic group of n-th roots of unity, i.e., $\mathcal{G}(T) = \{g \in T^\times \mid g^n = 1\}$ for any k-algebra T.

One of the main results of this article (Theorem 6.38) shows that any σ-étale σ-algebraic group can be build up (in a rather precise way) from the σ-algebraic groups in Example 4.4 and two finite σ-étale σ-algebraic groups. (Here a σ-algebraic group G is called finite if $k\{G\}$ is a finite dimensional k-vector space.)

Definition 4.5. — *A σ-algebraic group is* benign *if it is isomorphic to a σ-algebraic group of the form $[\sigma]_k\mathcal{G}$ for an étale algebraic group $\mathcal{G}$.*

The usage of the word *benign* originates from [18, Definition 5.4.7], where it is used to describe an extension L/K of σ-fields such $L = [\sigma]_K M$ for a finite Galois extension M of K.

Clearly, a σ-étale σ-algebraic group has σ-dimension zero and order zero. However, as seen in Example 4.4, the limit degree may be strictly larger than one.

Lemma 4.6. — *Quotients and σ-closed subgroups of σ-étale σ-algebraic groups are σ-étale.*

Proof. — Let G be a σ-étale σ-algebraic group. Quotients of G correspond to k-σ-Hopf subalgebras of $k\{G\}$ (Corollary 2.13) and σ-closed subgroups of G correspond to quotients of $k\{G\}$. Thus the claim follows from the fact that subalgebras and quotients of ind-étale algebras are ind-étale (as follows from the equivalent characterizations of ind-étale algebras given at the beginning of this section). $\square$

Lemma 4.7. — *Let G be a σ-closed subgroup of an algebraic group $\mathcal{G}$. For $i \geqslant 0$ let $G[i]$ denote the i-th order Zariski closure of G in $\mathcal{G}$. Then the following statements are equivalent:*

(i) *G is σ-étale.*
(ii) *$G[0]$ is an étale algebraic group.*
(iii) *$G[i]$ is an étale algebraic group for every $i \geqslant 0$.*

Proof. — Because $k\{G\}$ is the union of the $k[G[i]]$'s (i) and (iii) are equivalent. If $k[G[0]]$ is an étale k-algebra, all the $k[G[i]]$'s are étale k-algebras, because $k[G[i]]$ is a quotient of

$$k[G[0]][i] = k[G[0]] \otimes_k {}^{\sigma}(k[G[0]]) \otimes_k \cdots \otimes_k {}^{\sigma^i}(k[G[0]])$$

and étaleness is preserved under base change, tensor products and quotients. □

A σ-closed subgroup of an étale algebraic group is σ-étale (Lemma 4.6). Conversely, if G is a σ-étale σ-algebraic group, we can embed G as a σ-closed subgroup into an étale algebraic group. For example, we may first embed G into some algebraic group $\mathcal{G}$ (Proposition 2.7) and then consider the Zariski closure of G in $\mathcal{G}$, which is an étale algebraic group by Lemma 4.7. Thus a σ-algebraic group is σ-étale if and only if it is isomorphic to a Zariski-dense σ-closed subgroup of an étale algebraic group.

Proposition 4.8. — *A σ-algebraic group G is σ-étale if and only if it is reduced (i.e., $k\{G\}$ is reduced) and has order zero.*

Proof. — Clearly a σ-étale σ-algebraic group is reduced and has order zero. Conversely, let G be a reduced σ-algebraic group of order zero. Embed G as a σ-closed subgroup in some algebraic group $\mathcal{G}$ and let $G[i]$ denote the i-th order Zariski closure of G in $\mathcal{G}$. Then each $G[i]$ is a reduced finite algebraic group and therefore étale ([31, Example 8, p. 53]). It follows from Lemma 4.7 that G is σ-étale. □

Corollary 4.9. — *Assume that the base σ-field k has characteristic zero. Then a σ-algebraic group is σ-étale if and only if it has order zero.*

Proof. — A σ-algebraic group over a σ-field of characteristic zero is reduced ([31, Theorem 11.4, p. 86]). Thus the claim follows from Proposition 4.8. □

5. Expansive endomorphisms and étale difference algebraic groups

The category of étale algebraic groups over k is equivalent to the category of finite groups equipped with a continuous action of the absolute Galois group of k ([31, Theorem 6.4]). The goal of this section is to provide a difference analog of this statement (Theorem 5.6): The category of σ-étale σ-algebraic groups is equivalent to the category of profinite groups equipped with an expansive endomorphism and a compatible action of the absolute Galois group of k.

This theorem follows rather directly from a much more general equivalence of categories proved in [30]. The equivalence in [30] works over an arbitrary σ-ring in place of our base σ-field k and its proof relies on Janelidze's categorical Galois theory. We present here a comparatively short, self-contained proof of Theorem 5.6 that avoids Janelidze's categorical Galois theory and mainly relies on the classical equivalence of ind-étale k-algebras and profinite spaces equipped with a continuous action of the absolute Galois group.

We denote with k_s the separable algebraic closure of k and with $\mathscr{G} = \mathrm{Gal}(k_s/k)$ the absolute Galois group of k. Note that it is always possible to extend $\sigma\colon k \to k$ to an endomorphism $\sigma\colon k_s \to k_s$. However, such an extension is usually not unique. We fix once and for all such an extension $\sigma\colon k_s \to k_s$. The following lemma shows that we have a natural action of σ on $\mathscr{G}$.

Lemma 5.1. — *For every $\tau \in \mathscr{G}$ there exists a unique $\sigma(\tau) \in \mathscr{G}$ such that*

$$\begin{tikzcd} k_s \arrow[r, "\sigma(\tau)"] \arrow[d, "\sigma"'] & k_s \arrow[d, "\sigma"] \\ k_s \arrow[r, "\tau"] & k_s \end{tikzcd}$$

commutes. The map $\sigma\colon \mathscr{G} \to \mathscr{G}$, $\tau \mapsto \sigma(\tau)$ is a continuous morphism of groups.

Proof. — This is points (1) and (2) of [33, Lemma 6.1]. $\square$

In the sequel we will always consider $\mathscr{G}$ as equipped with the endomorphism $\sigma\colon \mathscr{G} \to \mathscr{G}$ as in Lemma 5.1.

Recall that a continuous map $\sigma\colon X \to X$ on a metric space (X, d) is called *(forward) expansive* if there exists an $\varepsilon > 0$ such that for any $x \neq y$ in X there exists an $n \in \mathbb{N}$ with $d(\sigma^n(x), \sigma^n(y)) > \varepsilon$. In the context of a continuous group homomorphism $\sigma\colon \mathtt{G} \to \mathtt{G}$ on a topological group $\mathtt{G}$, this idea translates to: There exists a neighborhood $\mathtt{U}$ of the identity $1 \in \mathtt{G}$ such that for any $x \neq y$ in $\mathtt{G}$ there exists an $n \in \mathbb{N}$ with $\sigma^n(x) \notin \sigma^n(y)\mathtt{U}$, equivalently, $y^{-1}x \notin \sigma^{-n}(\mathtt{U})$. Since the open normal subgroups of a profinite group are a neighborhood basis at 1 ([23, Theorem 2.1.3]), we can assume that $\mathtt{U}$ is an open normal subgroup of $\mathtt{G}$, in case $\mathtt{G}$ is a profinite group. We thus arrive at the following definition.

Definition 5.2. — *An endomorphism $\sigma\colon \mathtt{G} \to \mathtt{G}$ of a profinite group $\mathtt{G}$ is* expansive *if there exists an open normal subgroup $\mathtt{N}$ of $\mathtt{G}$ such that $\bigcap_{i\in\mathbb{N}} \sigma^{-i}(\mathtt{N}) = 1$.*

Similarly, an automorphism $\sigma\colon \mathtt{G} \to \mathtt{G}$ of a profinite group $\mathtt{G}$ is *expansive* if there exists an open normal subgroup $\mathtt{N}$ of $\mathtt{G}$ such that $\bigcap_{i\in\mathbb{Z}} \sigma^{-i}(\mathtt{N}) = 1$. Profinite groups, or more general topological groups, such as totally disconnected locally compact groups, equipped with an expansive automorphism have been studied by various authors. See [4, 10, 12, 14, 16, 25, 35], [24, Chapter 3] and the references given there.

While there has been some interest in generalizing results from automorphisms to endomorphisms ([6, 11, 22, 33, 36]), the literature on expansive endomorphisms of profinite groups is rather scarce.

There are two basic examples of expansive endomorphisms of profinite groups.

Example 5.3. — Let $\mathtt{G}$ be a finite (discrete) group. Then any endomorphism $\sigma\colon \mathtt{G} \to \mathtt{G}$ is expansive since we can choose $\mathtt{N} = 1$ in Definition 5.2.

Example 5.4. — Let $\mathtt{H}$ be a finite (discrete) group and consider $\mathtt{G} = \mathtt{H}^{\mathbb{N}}$ as a profinite group under componentwise multiplication and equipped with the product topology. Then the shift map

$$\sigma\colon \mathtt{H}^{\mathbb{N}} \to \mathtt{H}^{\mathbb{N}},\ (h_0, h_1, h_2, \ldots) \mapsto (h_1, h_2, \ldots)$$

is expansive. Indeed, we can choose $\mathtt{N} = 1 \times \mathtt{H} \times \mathtt{H} \cdots \leqslant \mathtt{H}^{\mathbb{N}}$.

Definition 5.5. — *A* profinite $\mathscr{G}$-σ-group *is a profinite group $\mathtt{G}$ equipped with an endomorphism $\sigma\colon \mathtt{G} \to \mathtt{G}$ and a continuous action $\mathscr{G} \times \mathtt{G} \to \mathtt{G}$ of $\mathscr{G}$ on $\mathtt{G}$ by group automorphisms such that $\sigma(\tau(g)) = \sigma(\tau)(\sigma(g))$ for $\tau \in \mathscr{G}$ and $g \in \mathtt{G}$. An* expansive profinite $\mathscr{G}$-σ-group *is a profinite $\mathscr{G}$-σ-group such that $\sigma\colon \mathtt{G} \to \mathtt{G}$ is expansive.*

A morphism $\phi\colon \mathtt{G} \to \mathtt{H}$ of profinite $\mathscr{G}$-σ-groups is a morphism of profinite groups that commutes with σ and is $\mathscr{G}$-equivariant, i.e., $\phi(\tau(g)) = \tau(\phi(g))$ for $\tau \in \mathscr{G}$ and $g \in \mathtt{G}$. The main result of this section is the following:

Theorem 5.6. — *The category of σ-étale σ-algebraic groups over k is equivalent to the category of expansive profinite $\mathcal{G}$-σ-groups.*

The proof of Theorem 5.6 is given at the end of this section, after some preparatory results are established.

The fact that étale algebraic groups over k are equivalent to finite groups with a continuous $\mathcal{G}$-action follows from the fact that étale algebras over k are anti-equivalent to finite sets with a continuous $\mathcal{G}$-action ([31, Theorem 6.3]). For our proof of Theorem 5.6 we shall need an "infinite" version of this anti-equivalence, i.e., a version that applies to ind-étale algebras instead of just étale algebras. On the side of the $\mathcal{G}$-actions one then has to replace finite sets by profinite spaces.

Recall that a *profinite (topological) space* is a topological space that can be written as a projective limit of finite discrete topological spaces. Equivalently, a topological space is profinite, if it is Hausdorff, compact and totally disconnected ([23, Theorem 1.1.12]).

For an ind-étale k-algebra T, the set $\operatorname{Hom}(T,k_s)$ of all k-algebra morphisms of T to k_s is naturally a profinite space: As $T = \varinjlim T_i$ is the directed union of its étale k-subalgebras T_i, we see that $\operatorname{Hom}(T,k_s) = \varprojlim \operatorname{Hom}(T_i,k_s)$ is the projective limit of the finite sets $\operatorname{Hom}(T_i,k_s)$. More explicitly, a basis for the topology of $\operatorname{Hom}(T,k_s)$ is given by the open subsets

$$U(a_1,\ldots,a_n,b_1,\ldots,b_n) = \{\psi \in \operatorname{Hom}(T,k_s) \mid \psi(a_1) = b_1,\ldots,\psi(a_n) = b_n\},$$

where $a_1,\ldots,a_n \in T$ and $b_1,\ldots,b_n \in k_s$.

The action $\mathcal{G} \times \operatorname{Hom}(T,k_s) \to \operatorname{Hom}(T,k_s),\ (\tau,\psi) \mapsto \tau \circ \psi$ is continuous ([2, Lemma 3.5.4]). A *profinite $\mathcal{G}$-space* is a profinite space together with a continous $\mathcal{G}$-action. (According to [23, Lemma 5.6.4 (a)], this definition is equivalent to Definition 3.5.1 in [2], where a profinite $\mathcal{G}$-space is defined to be the projective limit of finite discrete $\mathcal{G}$-spaces.) A morphism of profinite $\mathcal{G}$-spaces is a continuous $\mathcal{G}$-equivariant map. We are now prepared to state the infinitary version of the "Galois equivalence".

Theorem 5.7 ([2, Theorem 3.5.8]). — *The functor $T \rightsquigarrow \operatorname{Hom}(T,k_s)$ defines an anti-equivalence of categories between the category of ind-étale k-algebras and the category of profinite $\mathcal{G}$-spaces. Under this anti-equivalence, surjective morphisms of ind-étale k-algebras correspond to injective morphisms of profinite $\mathcal{G}$-spaces.*

Proof. — The anti-equivalence is a special case of [2, Theorem 3.5.8], where an arbitrary Galois extension is allowed in place of k_s/k. Note that a k-algebra T is split by k_s (in the sense of Definition [2, Definition 2.3.1]) if and only if T is ind-étale.

The surjective/injective statement is [30, Lemma 3.24]. □

We now return to our difference scenario. Our first goal is to add a σ to the anti-equivalence of Theorem 5.7.

Definition 5.8. — *A* profinite $\mathscr{G}$-σ-space $\mathtt{X}$ *is a profinite space* $\mathtt{X}$ *together with a continuous endomorphism* $\sigma\colon \mathtt{X}\to\mathtt{X}$ *and a continuous action* $\mathscr{G}\times\mathtt{X}\to\mathtt{X}$ *compatible with* σ *in the sense that*

$$\sigma(\tau(x))=\sigma(\tau)(\sigma(x))$$

for $\tau\in\mathscr{G}$ *and* $x\in\mathtt{X}$.

A morphism of profinite $\mathscr{G}$-σ-spaces is a continuous $\mathscr{G}$-equivariant map that commutes with the action of σ.

A k-σ-algebra is called *ind-étale* if it is ind-étale as a k-algebra. The following two lemmas show that ind-étale k-σ-algebras give rise to profinite $\mathscr{G}$-σ-spaces.

Lemma 5.9. — *Let T be an ind-étale k-algebra and let $\alpha\colon T\to k_s$ be a morphism of rings such that $\alpha(\lambda a)=\sigma(\lambda)\alpha(a)$ for $\lambda\in k$ and $a\in T$. Then there exists a unique morphism $\beta\colon T\to k_s$ of k-algebras such that*

$$\begin{tikzcd} T \arrow[rr, "\beta"] \arrow[dr, "\alpha"'] & & k_s \arrow[dl, "\sigma"] \\ & k_s & \end{tikzcd}$$

commutes.

Proof. — The uniqueness of β holds because the field endomorphism $\sigma\colon k_s\to k_s$ is automatically injective. For the existence of β it suffices to show that $\alpha(T)\subseteq\sigma(k_s)$ (because then, for any $a\in T$, we can define $\beta(a)\in k_s$ to be the unique element of k_s such that $\alpha(a)=\sigma(\beta(a))$).

Let $a\in T$. Since T is an ind-étale k-algebra, a satisfies a monic (separable) polynomial $f\in k[x]$. Write $f=\prod_{i=1}^n(x-a_i)$ with $a_i\in k_s$. Let ${}^\sigma\! f\in k[x]$ denote the polynomial obtained from f by applying $\sigma\colon k\to k$ to the coefficients. Then ${}^\sigma\! f=\prod_{i=1}^n(x-\sigma(a_i))$.

From $f(a)=0$ and $\alpha(\lambda a)=\sigma(\lambda)\alpha(a)$ for $\lambda\in k$, we obtain ${}^\sigma\! f(\alpha(a))=0$. So $\alpha(a)\in\{\sigma(a_1),\ldots,\sigma(a_n)\}\subseteq\sigma(k_s)$. □

Recall (Section 2.1) that for a k-σ-algebra R, we denote with $R^\sharp$ the underlying k-algebra.

Lemma 5.10. — *Let R be an ind-étale k-σ-algebra. Then, for every morphism $\psi\colon R\to k_s$ of k-algebras, there exists a unique morphism $\sigma(\psi)\colon R\to k_s$ of k-algebras such that*

$$\begin{tikzcd} R \arrow[r, "\sigma(\psi)"] \arrow[d, "\sigma"'] & k_s \arrow[d, "\sigma"] \\ R \arrow[r, "\psi"] & k_s \end{tikzcd}$$

commutes. Moreover, $\sigma\colon \operatorname{Hom}(R^\sharp, k_s^\sharp) \to \operatorname{Hom}(R^\sharp, k_s^\sharp),\ \psi \mapsto \sigma(\psi)$ is continuous and

$$\sigma(\tau(\psi)) = \sigma(\tau)(\sigma(\psi)) \tag{5.1}$$

for $\tau\in\mathscr{G}$, i.e., $\operatorname{Hom}(R^\sharp, k_s^\sharp)$ is a profinite $\mathscr{G}$-σ-space.

Proof. — The existence and uniqueness of $\sigma(\psi)$ follows from Lemma 5.9 applied to

$$\alpha\colon R \xrightarrow{\sigma} R \xrightarrow{\psi} k_s.$$

For $a_1,\dots,a_n\in R$ and $b_1,\dots,b_n\in k_s$ we have,

$$\begin{aligned}\sigma^{-1}&(U(a_1,\dots,a_n,b_1,\dots,b_n)) \\ &= \{\psi\in\operatorname{Hom}(R^\sharp,k_s^\sharp) \mid \sigma(\psi)(a_i)=b_i,\ i=1,\dots,n\}.\end{aligned}$$

But

$$\sigma(\psi)(a_i)=b_i \ \Leftrightarrow\ \sigma(\sigma(\psi)(a_i))=\sigma(b_i) \ \Leftrightarrow\ \psi(\sigma(a_i))=\sigma(b_i).$$

Therefore

$$\sigma^{-1}(U(a_1,\dots,a_n,b_1,\dots,b_n)) = U(\sigma(a_1),\dots,\sigma(a_n),\sigma(b_1),\dots,\sigma(b_n))$$

is open. Formula (5.1) follows from the commutative diagram

$$\begin{tikzcd} R \arrow[r, "\sigma(\psi)"] \arrow[d, "\sigma"'] & k_s \arrow[r, "\sigma(\tau)"] \arrow[d, "\sigma"] & k_s \arrow[d, "\sigma"] \\ R \arrow[r, "\psi"] & k_s \arrow[r, "\tau"] & k_s \end{tikzcd}$$

□

If $\alpha\colon R\to S$ is a morphism of ind-étale k-σ-algebras, the commutative diagram

$$\begin{tikzcd} R \arrow[r, "\alpha"] \arrow[d, "\sigma"'] & S \arrow[r, "\sigma(\psi)"] \arrow[d, "\sigma"] & k_s \arrow[d, "\sigma"] \\ R \arrow[r, "\alpha"] & S \arrow[r, "\psi"] & k_s \end{tikzcd}$$

shows that the diagram

$$\begin{tikzcd} \mathrm{Hom}(S^\sharp, k_s^\sharp) \arrow[r] \arrow[d, "\sigma"'] & \mathrm{Hom}(R^\sharp, k_s^\sharp) \arrow[d, "\sigma"] \\ \mathrm{Hom}(S^\sharp, k_s^\sharp) \arrow[r] & \mathrm{Hom}(R^\sharp, k_s^\sharp) \end{tikzcd}$$

commutes. So the induced map $\mathrm{Hom}(S^\sharp, k_s^\sharp) \to \mathrm{Hom}(R^\sharp, k_s^\sharp)$ is a morphism of profinite $\mathscr{G}$-σ-spaces. In other words, $R \rightsquigarrow \mathrm{Hom}(R^\sharp, k_s^\sharp)$ is a contravariant functor from the category of ind-étale k-σ-algebras to the category of profinite $\mathscr{G}$-σ-spaces. To show that this functor defines an anti-equivalence we need some more preparatory results.

For a profinite $\mathscr{G}$-space $\mathtt{X}$, we can twist the action of $\mathscr{G}$ on $\mathtt{X}$ by σ to obtain a new profinite $\mathscr{G}$-space ${}^\sigma\mathtt{X}$. In detail, ${}^\sigma\mathtt{X} = \mathtt{X}$ as profinite spaces but the action of $\mathscr{G}$ on ${}^\sigma\mathtt{X}$ is given by $g(x) = \sigma(g)(x)$ for $x \in {}^\sigma\mathtt{X}$ and $g \in \mathscr{G}$. Note that for a profinite $\mathscr{G}$-σ-space $\mathtt{X}$, the map $\sigma\colon \mathtt{X} \to \mathtt{X}$ can be interpreted as a morphism $\sigma\colon \mathtt{X} \to {}^\sigma\mathtt{X}$ of profinite $\mathscr{G}$-spaces.

Recall (Section 2.1) that for a k-algebra T, we denote with ${}^\sigma T = T \otimes_k k$ the k-algebra obtained from T by base change via $\sigma\colon k \to k$.

Lemma 5.11. — *Let T be an ind-étale k-algebra. Then*

$${}^\sigma(\mathrm{Hom}(T, k_s)) \simeq \mathrm{Hom}({}^\sigma T, k_s)$$

as profinite $\mathscr{G}$-spaces.

Proof. — Let us first describe the bijection $\eta\colon \mathrm{Hom}(T, k_s) \to \mathrm{Hom}({}^\sigma T, k_s)$. If $\psi\colon T \to k_s$ is a morphism of k-algebras, then $\psi' = \eta(\psi)\colon {}^\sigma T = T \otimes_k k \to k_s,\ a \otimes \lambda \mapsto \sigma(\psi(a))\lambda$ is a morphism of k-algebras. Conversely, if $\psi'\colon {}^\sigma T \to k_s$ is a morphism of k-algebras, then $\alpha\colon T \to {}^\sigma T \xrightarrow{\psi'} k_s$ (where the first map is $a \mapsto a \otimes 1$) is a morphism of rings satisfying $\alpha(\lambda a) = \sigma(\lambda)\alpha(a)$ for $\lambda \in k$ and $a \in T$. Thus Lemma 5.9 yields a (unique) morphism $\psi = \rho(\psi')\colon T \to k_s$ of k-algebras such that

$$\begin{tikzcd} T \arrow[r, "\psi"] \arrow[d] & k_s \arrow[d, "\sigma"] \\ {}^\sigma T \arrow[r, "\psi'"] & k_s \end{tikzcd}$$

commutes. The above diagram shows that ρ is the inverse of η. For elements $a_1, \ldots, a_n \in T$ and $b_1, \ldots, b_n \in k_s$ we have

$$\begin{aligned} &\rho^{-1}(U(a_1, \ldots, a_n, b_1, \ldots, b_n)) \\ &\qquad\qquad = \{\psi' \in \mathrm{Hom}({}^\sigma T, k_s) \mid \rho(\psi')(a_i) = b_i\ i = 1, \ldots, n\}. \end{aligned}$$

But

$$\rho(\psi')(a_i) = b_i \;\Leftrightarrow\; \sigma(\rho(\psi')(a_i)) = \sigma(b_i) \;\Leftrightarrow\; \psi'(a_i \otimes 1) = \sigma(b_i).$$

So $\rho^{-1}(U(a_1,\ldots,a_n,b_1,\ldots,b_n)) = U(a_1\otimes 1,\ldots,a_n\otimes 1,\sigma(b_1),\ldots,\sigma(b_n))$ and ρ is continuous. As any continuous bijection between compact Hausdorff spaces is a homeomorphism ([27, Proposition 13.26]), we see that ρ and therefore also η is a homeomorphism.

For $a \in T$, $\lambda \in k$, $\tau \in \mathscr{G}$ and $\psi \in \mathrm{Hom}(T, k_s)$, it follows from the commutative diagram

$$\begin{tikzcd} T \arrow[r, "\psi"] \arrow[d] & k_s \arrow[r, "\sigma(\tau)"] \arrow[d, "\sigma"] & k_s \arrow[d, "\sigma"] \\ {}^{\sigma}T \arrow[r, "\eta(\psi)"] & k_s \arrow[r, "\tau"] & k_s \end{tikzcd}$$

that

$$\eta(\sigma(\tau)(\psi))(a\otimes\lambda) = \sigma(\sigma(\tau)(\psi)(a))\lambda = \tau(\eta(\psi))(a\otimes 1)\lambda = \tau(\eta(\psi))(a\otimes\lambda).$$

Thus $\eta(\sigma(\tau)(\psi)) = \tau(\eta(\psi))$ as desired. □

Lemma 5.12. — *The isomorphism from Lemma 5.11 is functorial, i.e., for a morphism $\alpha\colon S \to T$ of ind-étale k-algebras, we have a commutative diagram*

(5.2)
$$\begin{tikzcd} {}^{\sigma}(\mathrm{Hom}(T,k_s)) \arrow[r, "\simeq"] \arrow[d] & \mathrm{Hom}({}^{\sigma}T, k_s) \arrow[d] \\ {}^{\sigma}(\mathrm{Hom}(S,k_s)) \arrow[r, "\simeq"] & \mathrm{Hom}({}^{\sigma}S, k_s) \end{tikzcd}$$

in the category of profinite $\mathscr{G}$-spaces.

Proof. — Let $\psi \in {}^{\sigma}(\mathrm{Hom}(T,k_s))$. Both paths in diagram (5.2) yield the element of $\mathrm{Hom}({}^{\sigma}S, k_s)$ given by ${}^{\sigma}S \to k_s,\ s\otimes\lambda \mapsto \sigma(\psi(\alpha(s)))\lambda$. □

For a k-σ-algebra R, the map $\overline{\sigma}\colon {}^{\sigma}R \to R,\ a\otimes\lambda \mapsto \sigma(a)\lambda$ is a morphism of k-algebras. Thus, if R is ind-étale, we obtain a morphism $\mathrm{Hom}(R^\sharp, k_s^\sharp) \to \mathrm{Hom}({}^{\sigma}R^\sharp, k_s^\sharp)$ of profinite $\mathscr{G}$-spaces.

Lemma 5.13. — *Let R be an ind-étale k-σ-algebra. Then the composition*

$$\mathrm{Hom}(R^\sharp, k_s^\sharp) \to \mathrm{Hom}({}^{\sigma}R^\sharp, k_s^\sharp) \simeq {}^{\sigma}(\mathrm{Hom}(R^\sharp, k_s^\sharp))$$

equals $\sigma\colon \mathrm{Hom}(R^\sharp, k_s^\sharp) \to \mathrm{Hom}(R^\sharp, k_s^\sharp)$.

Proof. — This follows from the commutative diagram

$$\begin{tikzcd}
R \arrow[rr, "\sigma(\psi)"] \arrow[d] \arrow[dr, "\sigma"] & & k_s \arrow[d, "\sigma"] \\
{}^{\sigma}R \arrow[r, "\overline{\sigma}"] & R \arrow[r, "\psi"] & k_s
\end{tikzcd}$$

□

We are now prepared to prove a σ-version of Theorem 5.7.

Proposition 5.14. — *The functor $R \rightsquigarrow \mathrm{Hom}(R^\sharp, k_s^\sharp)$ defines an anti-equivalence of categories between the category of ind-étale k-σ-algebras and the category of profinite $\mathscr{G}$-σ-spaces.*

Proof. — We first show that the functor is fully faithful. Let R and S be ind-étale k-σ-algebras. According to Theorem 5.7 we have a bijection

$$\xi\colon \mathrm{Hom}(R^\sharp, S^\sharp) \simeq \mathrm{Hom}(\mathrm{Hom}(S^\sharp, k_s^\sharp)^\sharp, \mathrm{Hom}(R^\sharp, k_s^\sharp)^\sharp),$$

where $\mathrm{Hom}(S^\sharp, k_s^\sharp)^\sharp$ denotes the profinite $\mathscr{G}$-space obtained from the profinite $\mathscr{G}$-σ-space $\mathrm{Hom}(S^\sharp, k_s^\sharp)$ by forgetting σ. It suffices to show that ξ restricts to a bijection between the subsets $\mathrm{Hom}(R, S) \subseteq \mathrm{Hom}(R^\sharp, S^\sharp)$ and

$$\mathrm{Hom}(\mathrm{Hom}(S^\sharp, k_s^\sharp), \mathrm{Hom}(R^\sharp, k_s^\sharp)) \subseteq \mathrm{Hom}(\mathrm{Hom}(S^\sharp, k_s^\sharp)^\sharp, \mathrm{Hom}(R^\sharp, k_s^\sharp)^\sharp).$$

In fact, it suffices to show that if $\alpha\colon R \to S$ is a morphism of k-algebras, such that $\xi(\alpha)\colon \mathrm{Hom}(S^\sharp, k_s^\sharp) \to \mathrm{Hom}(R^\sharp, k_s^\sharp)$ is a morphism of profinite $\mathscr{G}$-σ-spaces, then α is a morphism of k-σ-algebras. Note that, since R and S are ind-étale k-σ-algebras, $\alpha\colon R \to S$ is a morphism of k-σ-algebras if and only if

$$\begin{tikzcd}
{}^{\sigma}R \arrow[r, "{}^{\sigma}\alpha"] \arrow[d, "\overline{\sigma}"'] & {}^{\sigma}S \arrow[d, "\overline{\sigma}"] \\
R \arrow[r, "\alpha"] & S
\end{tikzcd}$$

is a commutative diagram in the category of ind-étale k-algebras. According to Theorem 5.7 it thus suffices to show that the induced diagram

(5.3)
$$\begin{tikzcd}
\mathrm{Hom}(S^\sharp, k^\sharp) \arrow[r] \arrow[d] & \mathrm{Hom}(R^\sharp, k^\sharp) \arrow[d] \\
\mathrm{Hom}({}^{\sigma}S^\sharp, k^\sharp) \arrow[r] & \mathrm{Hom}({}^{\sigma}R^\sharp, k^\sharp)
\end{tikzcd}$$

is a commutative diagram in the category of profinite $\mathscr{G}$-spaces. Now (5.3) fits into the larger diagram

$$\tag{5.4}\begin{tikzcd}
\mathrm{Hom}(S^\sharp,k^\sharp) \arrow[r] \arrow[d] \arrow[dd, bend right=60, "\sigma"'] & \mathrm{Hom}(R^\sharp,k^\sharp) \arrow[d] \arrow[dd, bend left=60, "\sigma"] \\
\mathrm{Hom}({}^\sigma S^\sharp,k^\sharp) \arrow[r] \arrow[d, "\simeq"'] & \mathrm{Hom}({}^\sigma R^\sharp,k^\sharp) \arrow[d, "\simeq"] \\
{}^\sigma(\mathrm{Hom}(S^\sharp,k^\sharp)) \arrow[r] & {}^\sigma(\mathrm{Hom}(R^\sharp,k^\sharp))
\end{tikzcd}$$

in the category of profinite $\mathscr{G}$-spaces. Note that if $\phi\colon \mathtt{X}\to\mathtt{Y}$ is a morphism of profinite $\mathscr{G}$-σ-spaces, then

$$\begin{tikzcd}
\mathtt{X} \arrow[r, "\phi"] \arrow[d, "\sigma"'] & \mathtt{Y} \arrow[d, "\sigma"] \\
{}^\sigma\mathtt{X} \arrow[r, "\phi"] & {}^\sigma\mathtt{Y}
\end{tikzcd}$$

is a commutative diagram in the category of profinite $\mathscr{G}$-spaces. Thus the outer rectangle of (5.4) commutes. The left and right triangles commute by Lemma 5.13 and the lower rectangle commutes by Lemma 5.12. Thus also the upper rectangle commutes as desired.

It remains to show that the functor $R\rightsquigarrow \mathrm{Hom}(R^\sharp,k_s^\sharp)$ is essentially surjective, i.e., every profinite $\mathscr{G}$-σ-space is isomorphic to $\mathrm{Hom}(R^\sharp,k_s^\sharp)$ for some ind-étale k-σ-algebra R. Let $\mathtt{X}$ be a profinite $\mathscr{G}$-σ-space. From Theorem 5.7 we know that there exists an ind-étale k-algebra R and an isomorphism $\mathtt{X}\simeq\mathrm{Hom}(R,k_s^\sharp)$ of profinite $\mathscr{G}$-spaces. Again, by Theorem 5.7, the morphism

$$\mathrm{Hom}(R,k_s^\sharp)\simeq\mathtt{X}\xrightarrow{\sigma}{}^\sigma\mathtt{X}\simeq{}^\sigma(\mathrm{Hom}(R,k_s^\sharp))\simeq\mathrm{Hom}({}^\sigma R,k_s^\sharp)$$

of profinite $\mathscr{G}$-spaces is induced by a unique morphism $\overline{\sigma}\colon {}^\sigma R\to R$ of k-algebras. Then $\sigma\colon R\to R,\ a\mapsto\overline{\sigma}(a\otimes 1)$ is a ring endomorphism extending $\sigma\colon k\to k$, i.e., R is a k-σ-algebra.

By definition of $\overline{\sigma}\colon {}^{\sigma}R \to R$, the diagram

$$\begin{tikzcd}
\mathtt{X} \arrow[r, "\sigma"] \arrow[d, "\simeq"'] & {}^{\sigma}\mathtt{X} \arrow[d, "\simeq"] \\
\mathrm{Hom}(R^{\sharp}, k_s^{\sharp}) \arrow[dr] & {}^{\sigma}(\mathrm{Hom}(R^{\sharp}, k_s^{\sharp})) \arrow[d, "\simeq"] \\
 & \mathrm{Hom}({}^{\sigma}R^{\sharp}, k_s^{\sharp})
\end{tikzcd}$$

commutes. Using Lemma 5.13 it follows that

$$\begin{tikzcd}
\mathtt{X} \arrow[r, "\sigma"] \arrow[d, "\simeq"'] & {}^{\sigma}\mathtt{X} \arrow[d, "\simeq"] \\
\mathrm{Hom}(R^{\sharp}, k_s) \arrow[r, "\sigma"] & {}^{\sigma}(\mathrm{Hom}(R^{\sharp}, k_s))
\end{tikzcd}$$

commutes, i.e., $\mathtt{X} \simeq \mathrm{Hom}(R^{\sharp}, k_s^{\sharp})$ as profinite $\mathscr{G}$-σ-spaces. $\square$

Note that the profinite $\mathscr{G}$-σ-groups are exactly the group objects in the category of profinite $\mathscr{G}$-σ-spaces. From Proposition 5.14 we thus obtain:

Corollary 5.15. — *The category of ind-étale k-σ-Hopf algebras is anti-equivalent to the category of profinite $\mathscr{G}$-σ-groups.*

Example 5.16. — Let $\mathcal{H}$ be an étale algebraic group. We would like to describe the profinite $\mathscr{G}$-σ-group $\mathtt{G}$ corresponding to the ind-étale k-σ-Hopf algebra $k\{\mathcal{H}\}$ under the anti-equivalence of Corollary 5.15. Recall (Section 2.2) that $k\{\mathcal{H}\}$ is our shorthand notation for $k\{[\sigma]_k\mathcal{H}\} = [\sigma]_k k[\mathcal{H}]$.

Let $\mathtt{H} = \mathrm{Hom}(k[\mathcal{H}], k_s)$ be the finite (discrete) group equipped with the continuous $\mathscr{G}$-action corresponding to $\mathcal{H}$. Forgetting σ for now, note that $k\{\mathcal{H}\}^{\sharp}$ is the coproduct of the ${}^{\sigma^i}(k[\mathcal{H}])$'s and so $\mathtt{G}^{\sharp}$ is the product of the $\mathrm{Hom}({}^{\sigma^i}(k[\mathcal{H}]), k_s)$'s. But $\mathrm{Hom}({}^{\sigma^i}(k[\mathcal{H}]), k_s) \simeq {}^{\sigma^i}\mathtt{H}$ by Lemma 5.11. So $\mathtt{G}^{\sharp} = \mathtt{H}^{\mathbb{N}}$ with action of $\mathscr{G}$ given by

$$\tau(h_0, h_1, h_2, \ldots) = (\tau(h_0), \sigma(\tau)(h_1), \sigma^2(\tau)(h_2), \ldots).$$

Multiplication in $\mathtt{H}^{\mathbb{N}}$ is componentwise and the topology is the product topology.

The morphism $\psi\colon k\{\mathcal{H}\} \to k_s$ of k-algebras corresponding to $(\psi_i)_{i\in\mathbb{N}} \in \mathtt{H}^{\mathbb{N}}$ is determined by $\psi(a_i \otimes \lambda_i) = \sigma^i(\psi_i(a_i))\lambda_i$ for $a_i \otimes \lambda_i \in k[\mathcal{H}] \otimes_k k =$

${}^{\sigma^i}(k[\mathcal{H}])$. Thus the morphism $\sigma(\psi)\colon k\{\mathcal{H}\}\to k_s$ of k-algebras such that

$$\begin{tikzcd} k\{\mathcal{H}\} \arrow[r, "\sigma(\psi)"] \arrow[d, "\sigma"'] & k_s \arrow[d, "\sigma"] \\ k\{\mathcal{H}\} \arrow[r, "\psi"] & k_s \end{tikzcd}$$

commutes, is given by $\sigma(\psi)(a_i\otimes\lambda_i)=\sigma^i(\psi_{i+1}(a_i))\lambda_i$ for $a_i\otimes\lambda_i\in k[\mathcal{H}]\otimes_k k={}^{\sigma^i}(k[\mathcal{H}])$. This shows that

$$\sigma\colon \mathtt{H}^{\mathbb{N}}\to\mathtt{H}^{\mathbb{N}},\ (h_0,h_1,h_2,\ldots)\mapsto(h_1,h_2,\ldots)$$

is simply the shift.

For the proof of Theorem 5.6 we need one more preparatory result.

Lemma 5.17. — *Let $\mathtt{G}$ be an expansive profinite $\mathscr{G}$-σ-group. Then there exists an open normal subgroup $\mathtt{U}$ of $\mathtt{G}$ such that $\bigcap_{i\in\mathbb{N}}\sigma^{-i}(\mathtt{U})=1$ and $\tau(\mathtt{U})=\mathtt{U}$ for all $\tau\in\mathscr{G}$.*

Proof. — This proof has some similarity with the proof of [23, Lemma 5.6.4(a)]. Since $\sigma\colon\mathtt{G}\to\mathtt{G}$ is expansive, there exists an open normal subgroup $\mathtt{N}$ of $\mathtt{G}$ such that $\bigcap_{i\in\mathbb{N}}\sigma^{-i}(\mathtt{N})=1$. Set $\mathtt{U}=\bigcap_{\tau\in\mathscr{G}}\tau(\mathtt{N})$. Then $\mathtt{U}$ is a normal subgroup of $\mathtt{G}$, $\tau(\mathtt{U})=\mathtt{U}$ for all $\tau\in\mathscr{G}$ and $\bigcap_{i\in\mathbb{N}}\sigma^{-i}(\mathtt{U})=1$ because $\mathtt{U}\subseteq\mathtt{N}$.

It remains to see that $\mathtt{U}$ is open. Let $g\in\mathtt{U}$. Then $\tau(g)\in\mathtt{U}\subseteq\mathtt{N}$ for any $\tau\in\mathscr{G}$. Since $\mathtt{N}\subseteq\mathtt{G}$ is open and the action $\mathscr{G}\times\mathtt{G}\to\mathtt{G}$ is continuous, there exist open neighborhoods $\tau\in V_\tau\subseteq\mathscr{G}$ and $g\in W_\tau\subseteq\mathtt{G}$ such that $\tau'(g')\in\mathtt{N}$ for all $\tau'\in V_\tau$ and $g'\in W_\tau$. The V_τ's are an open cover of $\mathscr{G}$. Therefore, there exist $\tau_1,\ldots,\tau_n\in\mathscr{G}$ such that $\mathscr{G}=V_{\tau_1}\cup\cdots\cup V_{\tau_n}$. Set $W=W_{\tau_1}\cap\cdots\cap W_{\tau_n}$. Then W is an open neighborhood of g and $\tau'(g')\in\mathtt{N}$ for all $\tau'\in\mathscr{G}$ and $g'\in W$. Thus $g'\in\tau(\mathtt{N})$ for all $g'\in W$ and all $\tau\in\mathscr{G}$, i.e., $W\subseteq\mathtt{U}$. □

Proof of Theorem 5.6. — Given Corollary 5.15, it suffices to show that for an ind-étale k-σ-Hopf algebra R, the profinite $\mathscr{G}$-σ-group $\mathtt{G}=\operatorname{Hom}(R^\sharp,k_s^\sharp)$ is expansive if and only if R is finitely σ-generated over k.

First assume that R is finitely σ-generated, so that $R=k\{G\}$ for the σ-étale σ-algebraic group $G=\operatorname{Hom}(R,-)$. By Lemma 4.7 there exist an étale algebraic group $\mathcal{H}$ and a σ-closed embedding $G\to[\sigma]_k\mathcal{H}$. On the side of the coordinate rings, this corresponds to a surjective morphism $k\{\mathcal{H}\}\to k\{G\}$ ind-étale k-σ-Hopf algebras. (Recall that $k\{\mathcal{H}\}=k\{[\sigma]_k\mathcal{H}\}=[\sigma]_k k[\mathcal{H}]$.) Which, in turn, according to Theorem 5.7, corresponds to an injective morphism $\phi\colon\mathtt{G}\to\operatorname{Hom}(k\{\mathcal{H}\}^\sharp,k_s^\sharp)$ of profinite

$\mathscr{G}$-σ-groups. By Example 5.16, the profinite $\mathscr{G}$-σ-group $\operatorname{Hom}(k\{\mathcal{H}\}^\sharp, k_s^\sharp)$ can be identified with $\mathtt{H}^\mathbb{N}$, where $\mathtt{H} = \operatorname{Hom}(k[\mathcal{H}], k_s)$ is a finite (discrete) group and $\sigma\colon \mathtt{H}^\mathbb{N} \to \mathtt{H}^\mathbb{N}$ is the shift map. Set $\mathtt{U} = 1 \times \mathtt{H} \times \mathtt{H} \times \cdots \leqslant \mathtt{H}^\mathbb{N}$. Then $\mathtt{U}$ is an open normal subgroup of $\mathtt{H}^\mathbb{N}$ with $\bigcap_{i\in\mathbb{N}} \sigma^{-i}(\mathtt{U}) = 1$. Set $\mathtt{N} = \phi^{-1}(\mathtt{U}) \leqslant \mathtt{G}$. Then $\mathtt{N}$ is an open normal subgroup of $\mathtt{G}$ and

$$\begin{aligned}\bigcap_{i\in\mathbb{N}} \sigma^{-i}(\mathtt{N}) = \bigcap_{i\in\mathbb{N}} \sigma^{-i}(\phi^{-1}(\mathtt{U})) &= \bigcap_{i\in\mathbb{N}} \phi^{-1}(\sigma^{-i}(\mathtt{U})) \\ &= \phi^{-1}\Big(\bigcap_{i\in\mathbb{N}} \sigma^{-i}(\mathtt{U})\Big) = \phi^{-1}(1) = 1,\end{aligned}$$

since ϕ is injective. Thus $\mathtt{G} = \operatorname{Hom}(R^\sharp, k_s^\sharp)$ is expansive.

Conversely, assume that $\mathtt{G} = \operatorname{Hom}(R^\sharp, k_s^\sharp)$ is expansive. Let $\mathtt{U}$ be as in Lemma 5.17 and set $\mathtt{H} = \mathtt{G}/\mathtt{U}$. Then $\mathtt{H}$ is a finite (discrete) group equipped with a continuous action of $\mathscr{G}$. We consider $\mathtt{H}^\mathbb{N}$ as a profinite $\mathscr{G}$-σ-group as in Example 5.16. In particular, $\mathscr{G}$ is acting on $\mathtt{H}^\mathbb{N}$ via $\tau(h_0, h_1, h_2, \ldots) = (\tau(h_0), \sigma(\tau)(h_1), \sigma^2(\tau)(h_2), \ldots)$ for $\tau \in \mathscr{G}$.

The map $\phi\colon \mathtt{G} \to \mathtt{H}^\mathbb{N},\ g \mapsto (\overline{\sigma^i(g)})_{i\in\mathbb{N}}$ is a continuous group homomorphism that commutes with σ. Moreover, for $\tau \in \mathscr{G}$ and $g \in \mathtt{G}$ we have

$$\phi(\tau(g)) = (\overline{\sigma^i(\tau(g))})_{i\in\mathbb{N}} = (\overline{\sigma^i(\tau)(\sigma^i(g))})_{i\in\mathbb{N}} = \tau(\overline{\sigma^i(g)})_{i\in\mathbb{N}} = \tau(\phi(g)).$$

So ϕ is a morphism of profinite $\mathscr{G}$-σ-groups. Since $\bigcap_{i\in\mathbb{N}} \sigma^{-i}(\mathtt{U}) = 1$, the map ϕ is injective.

Let $\mathcal{H}$ be the étale algebraic group corresponding to the finite group $\mathtt{H}$ with the continuous $\mathscr{G}$-action. According to Theorem 5.6, Theorem 5.7 and Example 5.16, the injective morphism ϕ of profinite $\mathscr{G}$-σ-groups corresponds to a surjective morphism $k\{\mathcal{H}\} \to R$ of k-σ-algebras. As $k\{\mathcal{H}\}$ is finitely σ-generated, it follows that also R is finitely σ-generated. ☐

Remark 5.18. — It is a natural question to ask, which profinite $\mathscr{G}$-σ-spaces correspond to the finitely σ-generated k-σ-algebras under Proposition 5.14? As explained in [30, Theorem 5.1], these are exactly the subshifts. The subshifts of finite type, extensively studied in symbolic dynamics ([15, 19]), correspond to finitely σ-presented k-σ-algebras.

As an immediate corollary to Theorem 5.6 we obtain:

COROLLARY 5.19. — *Let k be a separably algebraically closed σ-field. Then the category of σ-étale σ-algebraic groups (over k) is equivalent to the category of profinite groups equipped with an expansive endomorphism.*

From Theorem 5.6 we also obtain a combinatorial-arithmetic description of the category of strongly σ-étale σ-algebraic groups.

Corollary 5.20. — *The category of strongly σ-étale σ-algebraic groups is equivalent to the category of finite groups equipped with an automorphism and a compatible continuous action of $\mathscr{G}$.*

Proof. — Let G be a σ-étale σ-algebraic group and $\mathtt{G} = \operatorname{Hom}(k\{G\}^\sharp, k_s^\sharp)$ the corresponding profinite $\mathscr{G}$-σ-group. Clearly, $k\{G\}$ is an étale k-algebra if and only if $\mathtt{G}$ is finite. So, assuming that $k\{G\}$ is étale, it suffices to show that $k\{G\}$ is σ-separable if and only if $\sigma\colon \mathtt{G} \to \mathtt{G}$ is bijective.

As in the proof of Proposition 5.14, the map $\sigma\colon \mathtt{G} \to \mathtt{G}$ can be interpreted as a morphism $\sigma\colon \mathtt{G} \to {}^\sigma\mathtt{G}$ of profinite $\mathscr{G}$-spaces. According to Lemma 5.13, the corresponding morphism of k-algebras is

$$\overline{\sigma}\colon {}^\sigma(k\{G\}) = k\{G\} \otimes_k k \to k\{G\},\ f \otimes \lambda \mapsto \sigma(f)\lambda.$$

So $\sigma\colon \mathtt{G} \to \mathtt{G}$ is bijective if and only if $\overline{\sigma}\colon {}^\sigma(k\{G\}) \to k\{G\}$ is bijective. Since $k\{G\}$ is a finite dimensional k-vector space, the latter is equivalent to $\overline{\sigma}\colon {}^\sigma(k\{G\}) \to k\{G\}$ being injective. This in turn is equivalent to $k\{G\}$ being σ-separable. □

We conclude this section with an example, illustrating the equivalence of Theorem 5.6.

Example 5.21. — Let $\mathtt{H} = \{1, h, h^2, h^3\}$ be the cyclic group of order four (considered as a discrete topological group). As in Example 5.16 we consider $\mathtt{H}^\mathbb{N}$ as a profinite group via the product topology. The map $\sigma\colon \mathtt{H}^\mathbb{N} \to \mathtt{H}^\mathbb{N}$ is the shift. Consider the subgroup $\mathtt{G}$ of $\mathtt{H}^\mathbb{N}$ given by $\mathtt{G} = \{(h_0, h_1, h_2, \ldots) \in \mathtt{H}^\mathbb{N} \mid h_i^2 = h_{i+1}^2\ \forall\, i \in \mathbb{N}\}$. Then $\mathtt{G}$ is a closed subgroup of $\mathtt{H}^\mathbb{N}$ and invariant under $\sigma\colon \mathtt{H}^\mathbb{N} \to \mathtt{H}^\mathbb{N}$. Since $\sigma\colon \mathtt{H}^\mathbb{N} \to \mathtt{H}^\mathbb{N}$ is expansive, also $\sigma\colon \mathtt{G} \to \mathtt{G}$ is expansive. So $\mathtt{G}$ is a profinite group equipped with an expansive endomorphism.

Let us also add the action of an absolute Galois group. Let $k = \mathbb{Q}$, considered as a constant σ-field and let $\mathscr{G}$ denote the Galois group of $k_s = \overline{\mathbb{Q}}$ over k. As extension of σ to k_s we choose the identity map. So the action of σ on $\mathscr{G}$ is trivial and consequently a compatible action of $\mathscr{G}$ on G is a continuous action that commutes with σ. Let $\mathscr{G}$ act on $\mathtt{H}$ as $\mathscr{G}$ acts on $\{1, i, -1, -i\} = \{a \in \overline{\mathbb{Q}} \mid h^4 = 1\}$ (under the isomorphism determined by $i \mapsto h$). Let $\mathscr{G}$ act on $\mathtt{G}$ by $\tau(h_0, h_1, h_2, \ldots) = (\tau(h_0), \tau(h_1), \tau(h_2), \ldots)$ for $\tau \in \mathscr{G}$. Then $\mathtt{G}$ is an expansive profinite $\mathscr{G}$-σ-group.

The corresponding σ-étale σ-algebraic group G is the σ-closed subgroup of $\mathbb{G}_m$ given by

$$G(R) = \{g \in R^\times \mid g^4 = 1,\ \sigma(g)^2 = g^2\} \leqslant \mathbb{G}_m(R)$$

for any k-σ-algebra R.

6. A decomposition theorem for étale difference algebraic groups

In this section we establish a rather precise structure theorem for σ-étale σ-algebraic groups (Theorem 6.38). In particular, this theorem shows that any σ-étale σ-algebraic group is built up from benign σ-algebraic groups and finite σ-étale σ-algebraic groups.

6.1. Infinitesimal difference algebraic groups

The last σ-closed subgroup in the subnormal series of Theorem 6.38 is σ-infinitesimal. In this subsection we establish the properties of σ-infinitesimal σ-algebraic groups relevant for the proof of Theorem 6.38.

Recall that an algebraic group $\mathcal{G}$ is *infinitesimal* if $\mathcal{G}(T) = 1$ for every reduced k-algebra T. The following definition introduces a σ-analog of infinitesimal algebraic groups. A k-σ-algebra R is called *σ-reduced* if $\sigma\colon R \to R$ is injective.

Definition 6.1. — *A σ-algebraic group G is σ-infinitesimal if $G(R) = 1$ for every σ-reduced k-σ-algebra R.*

Example 6.2. — Let $n \geqslant 2$. The σ-closed subgroup G of $\mathbb{G}_m$ given by

$$G(R) = \{g \in R^\times \mid g^n = 1,\ \sigma(g) = 1\}$$

for any k-σ-algebra R, is σ-infinitesimal.

Example 6.3. — For $r \geqslant 1$ the σ-closed subgroup G of GL_n given by

$$G(R) = \{g \in \mathrm{GL}_n(R) \mid \sigma^r(g) = I_n\}$$

for any k-σ-algebra R, is σ-infinitesimal. (Here I_n is the $n \times n$ identity matrix.)

The following lemma gives an algebraic characterization of σ-infinitesimal σ-algebraic groups.

Lemma 6.4. — *A σ-algebraic group G is σ-infinitesimal if and only if for every $f \in \mathfrak{m}_G$ there exists an $n \in \mathbb{N}$ such that $\sigma^n(f) = 0$. In fact, if G is σ-infinitesimal, then $\sigma^n(\mathfrak{m}_G) = 0$ for some $n \in \mathbb{N}$.*

Proof. — Let $\mathfrak{a} = \{f \in k\{G\} \mid \exists\, n \in \mathbb{N} : \sigma^n(f) = 0\}$ denote the reflexive closure (cf. [18, p. 107]) of the zero ideal of $k\{G\}$. Then $\mathfrak{a}$ is a σ-ideal of $k\{G\}$ and $R = k\{G\}/\mathfrak{a}$ is σ-reduced.

Assume that G is σ-infinitesimal. Then the canonical map $k\{G\} \to R$ factors through the counit $\varepsilon\colon k\{G\} \to k$. So $\mathfrak{m}_G \subseteq \mathfrak{a}$.

Conversely, assume that $\mathfrak{m}_G \subseteq \mathfrak{a}$. Then $\mathfrak{m}_G = \mathfrak{a}$, since $\mathfrak{m}_G$ is a maximal ideal of $k\{G\}$. Let R be a σ-reduced k-σ-algebra and $g\colon k\{G\} \to R$ a morphism of k-σ-algebras. To show that $G(R) = 1$, it suffices to show that $g(\mathfrak{m}_G) = 0$. But if $f \in \mathfrak{m}_G = \mathfrak{a}$, then there exists an $n \in \mathbb{N}$ with $\sigma^n(f) = 0$ and so $\sigma^n(g(f)) = g(\sigma^n(f)) = g(0) = 0$. Since $\sigma\colon R \to R$ is injective, this implies $g(f) = 0$.

The σ-ideal $\mathfrak{m}_G$ is finitely σ-generated, i.e., of the form $\mathfrak{m}_G = [f_1, \ldots, f_m]$, for $f_1, \ldots, f_m \in \mathfrak{m}_G$ (e.g., by [34, Theorem 4.1]). So we can find $n \in \mathbb{N}$ such that $\sigma^n(f_i) = 0$ for $i = 1, \ldots, m$. But then $\sigma^n(\mathfrak{m}_G) = 0$. □

Corollary 6.5. — *A σ-infinitesimal σ-algebraic group has limit degree one and is σ-connected.*

Proof. — Let G be a σ-infinitesimal σ-algebraic group. According to Lemma 2.10 it suffices to show that $k\{G\}$ is finitely generated as a k-algebra. We have $k\{G\} = k \oplus \mathfrak{m}_G$ (direct sum of k-vector spaces). Therefore, we can find a finite σ-generating set B of $k\{G\}$ that is contained in $\mathfrak{m}_G$. By Lemma 6.4 there exists an $n \in \mathbb{N}$ such that $\sigma^n(B) = 0$. So $k\{G\}$ is generated by $B, \sigma(B), \ldots, \sigma^{n-1}(B)$ as a k-algebra.

Suppose G is not σ-connected. Then $k \subsetneqq \pi_0^\sigma(k\{G\}) \subseteq k \oplus \mathfrak{m}_G = k\{G\}$ and so $\pi_0^\sigma(k\{G\})$ contains an element f of $\mathfrak{m}_G$. But then $\sigma^n(f) = 0$ for some n. This contradicts the σ-separability of $\pi_0^\sigma(k\{G\})$. □

A σ-algebraic group G is *finite* if $k\{G\}$ is a finite dimensional k-vector space.

Corollary 6.6. — *A σ-infinitesimal σ-étale σ-algebraic group is finite.*

Proof. — If G is a σ-infinitesimal σ-étale σ-algebraic group, then $k\{G\}$ is ind-étale and finitely generated as a k-algebra by Corollary 6.5. Thus $k\{G\}$ is an étale k-algebra. □

Lemma 6.7. — *A reduced finite σ-connected σ-algebraic group is σ-infinitesimal.*

Proof. — Because G is finite, $\operatorname{Spec}(k\{G\})$ is a finite discrete topological space. Set

$$Z = \{\mathfrak{p} \in \operatorname{Spec}(k\{G\}) \mid \exists\, n \in \mathbb{N}:\ \sigma^{-n}(\mathfrak{p}) = \mathfrak{m}_G\}.$$

Then Z and the complement of Z are σ-closed subsets of $\operatorname{Spec}(k\{G\})$. Because $\operatorname{Spec}(k\{G\})$ is σ-connected and $\mathfrak{m}_G \in Z$, we must have $Z = \operatorname{Spec}(k\{G\})$. It follows that there exists an $n \in \mathbb{N}$ such that $\sigma^{-n}(\mathfrak{p}) = \mathfrak{m}_G$

for every prime ideal $\mathfrak{p}$ of $k\{G\}$. Thus, for $f \in \mathfrak{m}_G$ we have $\sigma^n(f) \in \bigcap_{\mathfrak{p}\in\operatorname{Spec}(k\{G\})}\mathfrak{p} = \sqrt{0} = 0$. So G is σ-infinitesimal by Lemma 6.4. $\square$

Lemma 6.8. — *Let $\phi\colon G \to H$ be a morphism of σ-algebraic groups and let H' be a σ-infinitesimal σ-closed subgroup of H. If $\ker(\phi)$ is σ-infinitesimal, then $\phi^{-1}(H')$ is σ-infinitesimal.*

Proof. — Let R be a σ-reduced k-σ-algebra. Then

$$\phi^{-1}(H')(R) = \{g \in G(R) \mid \phi(g) \in H'(R) = 1\} = \ker(\phi)(R) = 1. \qquad \square$$

6.2. The difference Frobenius morphism

The Frobenius morphism and the closely related Frobenius kernels play an important role in the representation theory of algebraic groups in positive characteristic. (See e.g., [13, Section 9, Part I].) In this subsection we introduce a difference analog of the Frobenius morphism and establish the properties relevant for the proof of Theorem 6.38.

The idea is that in most of the constructions and results from [13, Section 9, Part I], the Frobenius endomorphism $a \mapsto a^p$ can be replaced by our "abstract" endomorphism σ.

Let R be a k-σ-algebra. For $r \in \mathbb{N}$ the map $\sigma^r\colon k \to k,\ \lambda \mapsto \sigma^r(\lambda)$ is a morphism of difference rings. We denote by ${}_{\sigma^r}R$ the k-σ-algebra obtained from R by restriction of scalars via $\sigma^r\colon k \to k$. That is, ${}_{\sigma^r}R$ equals R as a difference ring, but the k-algebra structure map is $k \to {}_{\sigma^r}R,\ \lambda \mapsto \sigma^r(\lambda)$. Note that $\sigma^r\colon R \to {}_{\sigma^r}R,\ a \mapsto \sigma^r(a)$ is a morphism of k-σ-algebras.

Let X be a σ-variety and let ${}^{\sigma^r}X$ denote the σ-variety obtained from X by base change along $\sigma^r\colon k \to k$. So

$${}^{\sigma^r}X(R) = X({}_{\sigma^r}R)$$

for any k-σ-algebra R and ${}^{\sigma^r}X$ is represented by the k-σ-algebra $k\{{}^{\sigma^r}X\} = {}^{\sigma^r}(k\{X\}) = k\{X\} \otimes_k k$, where the tensor product $k\{X\} \otimes_k k$ is formed using $\sigma^r\colon k \to k$.

We define a morphism

$$F_X^r\colon X \to {}^{\sigma^r}X$$

of σ-varieties over k by $(F_X^r)_R := X(\sigma^r)\colon X(R) \to X({}_{\sigma^r}R) = {}^{\sigma^r}X(R)$ for any k-σ-algebra R. This makes sense because $\sigma^r\colon R \to {}_{\sigma^r}R$ is a morphism of k-σ-algebras. Moreover, if $\psi\colon R \to R'$ is a morphism of k-σ-algebras, then

$$\begin{tikzcd} R \arrow[r, "\sigma^r"] \arrow[d, "\psi"'] & {}_{\sigma^r}R \arrow[d, "\psi"] \\ R' \arrow[r, "\sigma^r"] & {}_{\sigma^r}R' \end{tikzcd}$$

is a commutative diagram of k-σ-algebras. Therefore

$$\begin{tikzcd} X(R) \arrow[r, "(F_X^r)_R"] \arrow[d, "X(\psi)"'] & {}^{\sigma^r}X(R) \arrow[d, "{}^{\sigma^r}X(\psi)"] \\ X(R') \arrow[r, "(F_X^r)_{R'}"] & {}^{\sigma^r}X(R') \end{tikzcd}$$

commutes, so that F_X^r is indeed natural in R, as required. We write F_X for F_X^1 and call F_X the *σ-Frobenius morphism* of X.

If $\phi\colon X \to Y$ is a morphism of σ-varieties, then

$$\begin{tikzcd} X(R) \arrow[r, "\phi_R"] \arrow[d, "X(\sigma^r)"'] & Y(R) \arrow[d, "Y(\sigma^r)"] \\ X({}_{\sigma^r}R) \arrow[r, "\phi_{({}_{\sigma^r}R)}"] & Y({}_{\sigma^r}R) \end{tikzcd}$$

commutes for any k-σ-algebra R. Therefore, we have a commutative diagram

$$\begin{tikzcd} X \arrow[r, "\phi"] \arrow[d, "F_X^r"'] & Y \arrow[d, "F_Y^r"] \\ {}^{\sigma^r}X \arrow[r, "{}^{\sigma^r}\phi"] & {}^{\sigma^r}Y \end{tikzcd}$$

of σ-varieties.

The dual morphism $(F_X^r)^*\colon {}^{\sigma^r}(k\{X\}) \to k\{X\}$ is the image of $\mathrm{id} \in X(k\{X\}) = \mathrm{Hom}(k\{X\}, k\{X\})$ in

$$ {}^{\sigma^r}X(k\{X\}) = \mathrm{Hom}(k\{X\}, {}_{\sigma^r}(k\{X\})) = \mathrm{Hom}({}^{\sigma^r}(k\{X\}), k\{X\}) $$

under $(F_X^r)_{k\{X\}}$. Thus $(F_X^r)^*$ is given by

$$(F_X^r)^*\colon {}^{\sigma^r}(k\{X\}) \to k\{X\}, \quad f \otimes \lambda \mapsto \sigma^r(f)\lambda. \tag{6.1}$$

Note that if G is a σ-algebraic group, then $F_G^r\colon G \to {}^{\sigma^r}G$ is a morphism of σ-algebraic groups.

Example 6.9. — Let G be a σ-algebraic group. By Proposition 2.7 we may embed G as a σ-closed subgroup into some GL_n. Then also ${}^{\sigma^r}G$ is naturally embedded into GL_n: The equations defining ${}^{\sigma^r}G$ as a σ-closed subgroup of GL_n are obtained from the equations defining G as a σ-closed subgroup of GL_n by applying σ^r to the coefficients of the equations. The endomorphism ϕ of the σ-algebraic group $[\sigma]_k \mathrm{GL}_n$ given by

$$\phi_R\colon\ \mathrm{GL}_n(R) \to \mathrm{GL}_n(R),\ g \mapsto \sigma^r(g)$$

where $\sigma^r(g)$ is the matrix obtained from g by applying σ to the coefficients, restricts to a morphism $\phi\colon G \to {}^{\sigma^r}G$. The dual map of ϕ on $k\{\mathrm{GL}_n\} = k\{x_{ij}, \frac{1}{\det(x)}\}$ is given by

$$\phi^*\colon k\left\{x_{ij}, \frac{1}{\det(x)}\right\} \to k\left\{x_{ij}, \frac{1}{\det(x)}\right\},\ x_{ij} \mapsto \sigma^r(x_{ij}).$$

It follows that the dual map of $\phi\colon G \to {}^{\sigma^r}G$ agrees with the dual map of F_G^r given in (6.1). In other words, ϕ agrees with F_G^r. (The advantage of the abstract description is that it shows that ϕ does not depend on the chosen embedding of G into GL_n.)

Because of Example 6.9, we may sometimes simply write $\sigma^r(g)$ instead of $F_G^r(g)$, for $g \in G(R)$ and R a k-σ-algebra.

Our next goal is to understand when the σ-Frobenius $F_G\colon G \to {}^{\sigma^r}G$ is a quotient map. The following definition will help answer this question.

Definition 6.10. — *A σ-algebraic group G is* σ-reduced *if $k\{G\}$ is σ-reduced (i.e., $\sigma\colon k\{G\} \to k\{G\}$ is injective). A σ-algebraic group G is* absolutely σ-reduced *if $G_{k'}$ is σ-reduced for every σ-field extension k' of k.*

In other words, G is absolutely σ-reduced if and only if $k\{G\}$ is a σ-separable k-σ-algebra. The following example shows that a σ-reduced σ-algebraic group need not be absolutely σ-reduced.

Example 6.11. — Let k be a σ-field such that there exists a $\lambda \in k$ that is transcendental over $\sigma(k)$. Let G be the σ-closed subgroup of the additive group given by

$$G(R) = \{g \in R \mid \sigma^2(g) + \lambda\sigma(g) = 0\} \leqslant \mathbb{G}_a(R)$$

for any k-σ-algebra R. Then $k\{G\} = k[y, \sigma(y)]$. To show that σ is injective on $k\{G\}$, it suffices to show that $\sigma(y)$ and $\sigma^2(y) = -\lambda\sigma(y)$ are algebraically independent over $\sigma(k)$. But this is guaranteed by the assumption on λ. Thus G is σ-reduced. However, G is not absolutely σ-reduced. Over the inversive closure k^* of k ([18, Definition 2.1.6]) we can find a $\mu \in k^*$ such that $\sigma(\mu) = \lambda$ and then $\sigma(y)+\mu y$ lies in the kernel of σ on $k^*\{G_{k^*}\} = k^*[y, \sigma(y)]$.

The following lemma implies that an algebraic group, when considered as a σ-algebraic group is absolutely σ-reduced.

Lemma 6.12. — *Let T be a k-algebra. Then $[\sigma]_k T$ is σ-separable over k.*

Proof. — For a σ-field extension k' of k we have $([\sigma]_k T)\otimes_k k' = [\sigma]_{k'}(T\otimes_k k')$. Therefore, it suffices to show that $\sigma\colon [\sigma]_k T \to [\sigma]_k T$ is injective. Indeed, it suffices to show that $\sigma\colon T[i] \to T[i+1]$ is injective for every $i \geqslant 0$. But $\sigma\colon T[i] \to {}^\sigma(T[i]) \to T[i+1]$ is the composition of two injective maps. $\square$

From Lemma 6.12 we immediately obtain:

Corollary 6.13. — *Let $\mathcal{G}$ be an algebraic group. Then $[\sigma]_k\mathcal{G}$ is an absolutely σ-reduced σ-algebraic group.*

The following lemma explains when $F_G\colon G \to {}^\sigma G$ is a quotient map.

Lemma 6.14. — *Let G be a σ-algebraic group. The following statements are equivalent:*

(i) *$F_G\colon G \to {}^\sigma G$ is a quotient map.*
(ii) *$F_G^r\colon G \to {}^{\sigma^r} G$ is a quotient map for every $r \in \mathbb{N}$.*
(iii) *G is absolutely σ-reduced.*

Proof. — Recalling the equivalent characterization of σ-separability stated after Definition 3.6, we see that the k-σ-algebra $k\{G\}$ is σ-separable over k if and only if $\overline{\sigma} = (F_G)^*\colon {}^\sigma(k\{G\}) \to k\{G\}$ is injective. Thus (i) and (iii) are equivalent. To see that (i) implies (ii), note that the injectivity of $\overline{\sigma}\colon {}^\sigma(k\{G\}) \to k\{G\}$ can be rephrased as: If $f_1,\ldots,f_n \in k\{G\}$ are k-linearly independent, then $\sigma(f_1),\ldots,\sigma(f_n) \in k\{G\}$ are k-linearly independent. If this is true, and $f_1,\ldots,f_n \in k\{G\}$ are k-linearly independent, then $\sigma^r(f_1),\ldots,\sigma^r(f_n)$ are also k-linearly independent, i.e., the map $(F_G^r)^*\colon {}^{\sigma^r}(k\{G\}) \to k\{G\}$ is injective. $\square$

The following definition introduces a σ-analog of the Frobenius kernels ([13, Section 9.4, Part I])

Definition 6.15. — *Let G be a σ-algebraic group and $r \in \mathbb{N}$. The kernel $G_{(r)}$ of the morphism $F_G^r\colon G \to {}^{\sigma^r}G$ is called the* r-th σ-Frobenius kernel *of G.*

Since $F_G^{r+s} = F^s_{{}^{\sigma^r}G} \circ F_G^r$ we have

$$1 = G_{(0)} \subseteq G_{(1)} \subseteq G_{(2)} \subseteq \cdots .$$

Moreover, from formula (6.1) we see that

$$\mathbb{I}(G_{(r)}) = (\sigma^r(\mathfrak{m}_G)) \subseteq k\{G\}$$

and

$$k\{G/G_{(r)}\} = k[\sigma^r(k\{G\})] \subseteq k\{G\}.$$

Example 6.16. — The r-th σ-Frobenius kernel of $[\sigma]_k\operatorname{GL}_n$ is given by

$$([\sigma]_k\operatorname{GL}_n)_{(r)}(R)=\{g\in\operatorname{GL}_n(R)\mid \sigma^r(g)=I_n\}$$

for any k-σ-algebra R. (Here I_n denotes the $n\times n$ identity matrix.)

As a Corollary to Lemma 6.14 we obtain:

Corollary 6.17. — *Let G be an absolutely σ-reduced σ-algebraic group and let $r\in\mathbb{N}$. Then $G/G_{(r)}\simeq {}^{\sigma^r}G$.*

Proof. — This follows immediately from Lemma 6.14 (and Theorem 2.18). □

The following lemma explains the close connection between σ-infinitesimal σ-algebraic groups and the σ-Frobenius kernels.

Lemma 6.18. — *Let G be a σ-algebraic group. Then $G_{(r)}$ is a σ-infinitesimal σ-algebraic group for every $r\in\mathbb{N}$. Conversely, if H is a σ-infinitesimal σ-closed subgroup of G, then H is contained in some $G_{(r)}$. In particular, if G is σ-infinitesimal, then $G=G_{(r)}$ for some $r\in\mathbb{N}$.*

Proof. — Since $k\{G_{(r)}\}=k\{G\}/(\sigma^r(\mathfrak{m}_G))$, it is clear that the augmentation ideal $\mathfrak{m}_{G_{(r)}}$ of $G_{(r)}$ satisfies $\sigma^r(\mathfrak{m}_{G_{(r)}})=0$. So $G_{(r)}$ is σ-infinitesimal (Lemma 6.4).

If $H\leqslant G$ is σ-infinitesimal, then $\sigma^r(\mathfrak{m}_G)\subseteq\mathbb{I}(H)$ for some $r\in\mathbb{N}$ by Lemma 6.4. So $\mathbb{I}(G_{(r)})=(\sigma^r(\mathfrak{m}_G))\subseteq\mathbb{I}(H)$ and consequently $H\leqslant G_{(r)}$. □

For later use we record:

Lemma 6.19. — *Let H be a σ-closed subgroup of a σ-algebraic group G and let N be a normal σ-closed subgroup of H. If H/N is absolutely σ-reduced, then*

$$(F_G^r)^{-1}({}^{\sigma^r}H)/(F_G^r)^{-1}({}^{\sigma^r}N)\simeq {}^{\sigma^r}(H/N)$$

for every $r\in\mathbb{N}$.

Proof. — Using Lemma 2.15, we obtain a morphism

$$(F_G^r)^{-1}({}^{\sigma^r}H)\xrightarrow{F_G^r}{}^{\sigma^r}H\to{}^{\sigma^r}H/{}^{\sigma^r}N={}^{\sigma^r}(H/N)$$

with kernel $(F_G^r)^{-1}({}^{\sigma^r}N)$. By Lemma 2.16, this yields a σ-closed embedding

$$\phi\colon (F_G^r)^{-1}({}^{\sigma^r}H)/(F_G^r)^{-1}({}^{\sigma^r}N)\to{}^{\sigma^r}(H/N).$$

Since H/N is absolutely σ-reduced, $F^r_{H/N}$ is a quotient map (Lemma 6.14). As

$$\begin{tikzcd} H/N \arrow[rr] \arrow[dr, "F^r_{H/N}"'] & & (F^r_G)^{-1}({}^{\sigma^r}H)/(F^r_G)^{-1}({}^{\sigma^r}N) \arrow[dl, "\phi"] \\ & {}^{\sigma^r}(H/N) & \end{tikzcd}$$

commutes, this implies that ϕ must also be a quotient. Thus ϕ is an isomorphism by Corollary 2.19. □

Note that the functor $\mathcal{G} \rightsquigarrow [\sigma]_k\mathcal{G}$ from the category of algebraic groups to the category of σ-algebraic groups is not full. For example, for $\lambda_0, \ldots, \lambda_{n-1} \in k$, the morphism $\phi\colon [\sigma]_k\mathbb{G}_a \to [\sigma]_k\mathbb{G}_a$ given by

$$\phi(g) = \sigma^n(g) + \lambda_{n-1}\sigma^{n-1}(g) + \cdots + \lambda_0 g$$

for $g \in R$ and any k-σ-algebra R, is not induced by an endomorphism of the algebraic group $\mathbb{G}_a$. Nevertheless, we have the following result.

Proposition 6.20. — *Let $\mathcal{G}$ and $\mathcal{H}$ be algebraic groups. If $[\sigma]_k\mathcal{G}$ and $[\sigma]_k\mathcal{H}$ are isomorphic as σ-algebraic groups, then $\mathcal{G}$ and $\mathcal{H}$ are isomorphic as algebraic groups.*

Proof. — The morphism $F_{[\sigma]_k\mathcal{G}}\colon [\sigma]_k\mathcal{G} \to {}^{\sigma}([\sigma]_k\mathcal{G}) = [\sigma]_k{}^{\sigma}\mathcal{G}$ of σ-algebraic groups has the morphism

$$\mathcal{G} \times {}^{\sigma}\mathcal{G} \times {}^{\sigma^2}\mathcal{G} \times \cdots \to {}^{\sigma}\mathcal{G} \times {}^{\sigma^2}\mathcal{G} \times \cdots, \ (g_0, g_1, g_2, \ldots) \mapsto (g_1, g_2, \ldots)$$

as underlying morphism of affine group schemes. So $([\sigma]_k\mathcal{G})_{(1)}$ has $\mathcal{G}$ as the underlying affine group scheme. If $[\sigma]_k\mathcal{G} \simeq [\sigma]_k\mathcal{H}$, then $([\sigma]_k\mathcal{G})_{(1)} \simeq ([\sigma]_k\mathcal{H})_{(1)}$ and therefore also $\mathcal{G} \simeq \mathcal{H}$. □

6.3. Simple étale algebraic groups

The material in this subsection will be helpful for establishing the uniqueness part of our main decomposition theorem (Theorem 6.38).

Definition 6.21. — *Let $\mathcal{G}$ be a non-trivial étale algebraic group. Then $\mathcal{G}$ is* simple *if for every normal closed subgroup $\mathcal{N}$ of $\mathcal{G}$ either $\mathcal{N} = \mathcal{G}$ are $\mathcal{N} = 1$. Moreover, $\mathcal{G}$ is* σ-stably simple *if ${}^{\sigma^i}\mathcal{G}$ is simple for every $i \in \mathbb{N}$.*

The following example illustrates that for a simple étale algebraic group $\mathcal{G}$, the finite group $\mathcal{G}(k_s)$ need not be a simple group.

Example 6.22. — Let $V=\{(0,0),(1,0),(0,1),(1,1)\}$ be the Klein four group. Its automorphism group can be identified with the symmetric group S_3 on $(1,0),(0,1),(1,1)$. Let $\mathscr{G}$ be the Galois group of k_s/k and let $\mathscr{G}\to S_3$ be a surjective continuous morphism (i.e., we assume that S_3 is a Galois group over k). Let $\mathcal{G}$ be the étale algebraic group over k associated to this continuous action of $\mathscr{G}$ on V (as in Section 5). Then $\mathcal{G}(k_s)\simeq V$ is not a simple group. However, $\mathcal{G}$ is a simple étale algebraic group because no non-trivial proper subgroup of V is invariant under the action of $\mathscr{G}$.

The following example shows that a simple étale algebraic group need not be σ-stably simple.

Example 6.23. — Let k be a σ-field and as in Section 5 let us fix an extension of σ to the separable algebraic closure k_s of k. Let $a\in k_s$ be such that $\sigma(a)\in k$ and $k(a)\subseteq k_s$ is a Galois extension of k with Galois group isomorphic to S_3. To see that such a k and a exists, consider the difference field $K=\mathbb{C}(y,\sigma(y),\sigma^2(y),\ldots)$ obtained by taking the field of fractions of the difference polynomial ring $\mathbb{C}\{y\}=\mathbb{C}[y,\sigma(y),\sigma^2(y),\ldots]$, where $\mathbb{C}$ is considered as a σ-field via the identity map. Fix an extension of $\sigma\colon K\to K$ to the algebraic closure $\overline{K}$ of K. As any finite group is a Galois group over the rational function field $\mathbb{C}(y)$ ([28, Corollary 3.4.4]), there exists an element $a\in\overline{\mathbb{C}(\curvearrowright)}\subseteq\overline{K}$ such that $\mathbb{C}(y)(a)$ is a Galois extension of $\mathbb{C}(y)$ with Galois group isomorphic to S_3. Then $k=K(\sigma(a),\sigma^2(a),\sigma^3(a),\ldots)$ has the required properties.

Let $\mathcal{G}$ be the simple algebraic group from Example 6.22 associated with the surjection $\mathscr{G}\to S_3$, where $\mathscr{G}$ is the Galois group of k_s/k. As in Lemma 5.1 the profinite group $\mathscr{G}$ is equipped with an endomorphism $\sigma\colon\mathscr{G}\to\mathscr{G}$. The diagram

$$\begin{tikzcd} k_s \arrow[r, "\sigma(\tau)"] \arrow[d, "\sigma"'] & k_s \arrow[d, "\sigma"] \\ k_s \arrow[r, "\tau"] & k_s \end{tikzcd}$$

shows that $\sigma(\tau)(a)=a$ for all $\tau\in\mathscr{G}$, i.e., $\sigma(\mathscr{G})$ lies in the kernel of $\mathscr{G}\to S_3$. So it follows from Lemma 5.11 that $\mathscr{G}$ acts trivially on ${}^{\sigma}\mathcal{G}(k_s)$. Since the Klein four group V is not simple, ${}^{\sigma}\mathcal{G}$ is not a simple étale algebraic group.

Our main goal here is to describe the normal σ-closed subgroups of σ-stably simple étale algebraic groups and the corresponding quotients.

LEMMA 6.24. — *Let $\mathcal{G}$ be a σ-stably simple étale algebraic group that is not commutative. Let $\mathcal{N}$ be a normal closed subgroup of $\mathcal{G}\times{}^{\sigma}\mathcal{G}\times\cdots\times{}^{\sigma^n}\mathcal{G}$. Then $\mathcal{N}=\mathcal{N}_0\times\mathcal{N}_1\times\cdots\times\mathcal{N}_n$, where $\mathcal{N}_i\in\{1,{}^{\sigma^i}\mathcal{G}\}$ for $i=0,\ldots,n$.*

Proof. — For $i=0,\ldots,n$ set $\mathcal{H}_i = 1\times\cdots\times 1\times {}^{\sigma^i}\mathcal{G}\times 1\times\cdots\times 1 \leqslant \mathcal{G}\times {}^{\sigma}\mathcal{G}\times\cdots\times {}^{\sigma^n}\mathcal{G}$. It suffices to show the following: If $g=(g_0,\ldots,g_n)\in\mathcal{N}(k_s)$ with $g_i\neq 1$, then $\mathcal{H}_i\leqslant\mathcal{N}$.

Since ${}^{\sigma^i}\mathcal{G}$ is a non-commutative simple étale algebraic group, its center is trivial. Thus there exists an $h\in {}^{\sigma^i}\mathcal{G}(k_s)$ with $hg_i\neq g_ih$. Therefore

$$(1,\ldots,1,h,1,\ldots,1)(g_1,\ldots,g_n)(1,\ldots,1,h,1,\ldots,1)^{-1}(g_1,\ldots,g_n)^{-1} = \\ = (1,\ldots,1,hg_ih^{-1}g_i^{-1},1,\ldots,1)$$

is a non-trivial element of $\mathcal{N}(k_s)\cap\mathcal{H}_i(k_s)$. Since $\mathcal{H}_i$ is simple, we have $\mathcal{N}\cap\mathcal{H}_i=\mathcal{H}_i$, i.e., $\mathcal{H}_i\leqslant\mathcal{N}$ as desired. ☐

Corollary 6.25. — *Let $\mathcal{G}$ be a σ-stably simple étale algebraic group that is not commutative and let N be a proper normal σ-closed subgroup of $G=[\sigma]_k\mathcal{G}$. Then $N=G_{(r)}$ for some $r\in\mathbb{N}$.*

Proof. — For $i\in\mathbb{N}$ let $N[i]$ denote the i-th order Zariski closure of N in $\mathcal{G}$. Since N is normal in $\mathcal{G}$, it follows that $N[i]$ is normal in $\mathcal{G}[i] = \mathcal{G}\times{}^{\sigma}\mathcal{G}\times\cdots\times{}^{\sigma^i}\mathcal{G}$ (Lemma [32, Lemma 3.10]). As N is a proper subgroup of G, $N[i]$ must be a proper subgroup of $\mathcal{G}[i]$ for some i. Let $r\in\mathbb{N}$ be such that $N[i]=\mathcal{G}[i]$ for $i=0,\ldots,r-1$ but $N[r]\subsetneqq\mathcal{G}[r]$. By Lemma 6.24 we must have $N[r]=\mathcal{G}\times{}^{\sigma}\mathcal{G}\times\cdots\times{}^{\sigma^{r-1}}\mathcal{G}\times 1$. Thus $N=G_{(r)}$. ☐

The following example shows that the conclusion of Corollary 6.25 does not hold for commutative σ-stably simple étale algebraic group.

Example 6.26. — Let q be a prime number different from the characteristic of k. Then the algebraic group $\mathcal{G}=\mu_q$ defined by $\mathcal{G}(T)=\{g\in T^\times \mid g^q=1\}$ for any k-algebra T, is a σ-stably simple étale algebraic group. The proper normal σ-closed subgroup N of $\mathcal{G}$ given by $N(R)=\{g\in G(R)\mid \sigma(g)=g\}$ for any k-σ-algebra R, is not of the form $G_{(r)}$ for some $r\in\mathbb{N}$.

For clarity of the exposition, we separate the following elementary lemma from the proof of Proposition 6.29.

Lemma 6.27. — *Let $i,r\in\mathbb{N}$ and let $\mathtt{G}_0,\mathtt{G}_1,\mathtt{G}_2,\ldots,\mathtt{G}_{i+r}$ be abelian groups. For $j=0,\ldots,i$ let $\psi_j\colon \mathtt{G}_j\times\mathtt{G}_{j+1}\times\cdots\times\mathtt{G}_{j+r-1}\to\mathtt{G}_{j+r}$ be a morphism of groups and set*

$$\mathtt{N}_j=\{(g_j,\ldots,g_{j+r})\in\mathtt{G}_j\times\cdots\times\mathtt{G}_{j+r}\mid g_{j+r}=\psi_j(g_j,\ldots,g_{j+r-1})\} \\ \leqslant \mathtt{G}_j\times\cdots\times\mathtt{G}_{j+r}.$$

Then the morphism

$$\begin{aligned}\phi\colon \mathtt{G}_0\times\mathtt{G}_1\times\cdots\times\mathtt{G}_{i+r} &\longrightarrow ((\mathtt{G}_0\times\cdots\times\mathtt{G}_r)/\mathtt{N}_0)\times\ldots\times((\mathtt{G}_i\times\cdots\times\mathtt{G}_{i+r})/\mathtt{N}_i)\\ (g_0,g_1,\ldots,g_{i+r}) &\longmapsto (\overline{(g_0,\ldots,g_r)},\ldots,\overline{(g_i,\ldots,g_{i+r})})\end{aligned}$$

is surjective.

Proof. — For $j=0,\ldots,i$ let $(g_{j,0},\ldots,g_{j,r})\in\mathtt{G}_j\times\cdots\times\mathtt{G}_{j+r}$. So $h=(\overline{(g_{0,0},\ldots,g_{0,r})},\ldots,\overline{(g_{i,0},\ldots,g_{i,r})})$ is an arbitrary element of the codomain of ϕ. Define $g=(g_0,\ldots,g_{i+r})\in\mathtt{G}_0\times\cdots\times\mathtt{G}_{i+r}$ by $(g_0,\ldots,g_r)=(g_{0,0},\ldots,g_{0,r})$ and then recursively by

$$g_{r+j}=\psi_j\left(g_jg_{j,0}^{-1},g_{j+1}g_{j,1}^{-1},\ldots,g_{j+r-1}g_{j,r-1}^{-1}\right)g_{j,r}$$

for $j=1,\ldots,i$. Then $(g_jg_{j,0}^{-1},g_{j+1}g_{j,1}^{-1},\ldots,g_{j+r}g_{j,r}^{-1})\in\mathtt{N}_j$ and so

$$\overline{(g_j,\ldots,g_{j+r})}=\overline{(g_{j,0},\ldots,g_{j,r})}\in(\mathtt{G}_j\times\cdots\times\mathtt{G}_{j+r})/\mathtt{N}_j.$$

Thus $\phi(g)=h$. □

Definition 6.28. — *Two étale algebraic groups $\mathcal{G}$ and $\mathcal{H}$ are σ-*stably equivalent *if there exist $m,n\in\mathbb{N}$ such that ${}^{\sigma^m}\mathcal{G}\simeq{}^{\sigma^n}\mathcal{H}$.*

Note that this defines an equivalence relation on the class of all étale algebraic groups over k.

Proposition 6.29. — *Let $\mathcal{G}$ be a σ-stably simple étale algebraic group and let N be a proper normal σ-closed subgroup of $G=[\sigma]_k\mathcal{G}$. Then $G/N\simeq[\sigma]_k\mathcal{H}$ for some σ-stably simple étale algebraic group $\mathcal{H}$ σ-stably equivalent to $\mathcal{G}$.*

Proof. — First assume that $\mathcal{G}$ is not commutative. From Corollary 6.25 we know that $N=G_{(r)}$ for some $r\in\mathbb{N}$. So $G/N=G/G_{(r)}\simeq{}^{\sigma^r}G=[\sigma]_k{}^{\sigma^r}\mathcal{G}$ by Corollaries 6.13 and 6.17.

Now assume that $\mathcal{G}$ is commutative. For $i\in\mathbb{N}$ let $N[i]$ denote the i-th order Zariski closure of N in $\mathcal{G}$. Moreover, let $\mathcal{N}_i$ denote the kernel of the projection $\pi_i\colon N[i]\to N[i-1]$. Then $\mathcal{N}_i$ can be identified with a closed subgroup of ${}^{\sigma^i}\mathcal{G}$. Since ${}^{\sigma^i}\mathcal{G}$ is simple and commutative, we have $\mathcal{N}_i\in\{1,{}^{\sigma^i}\mathcal{G}\}$. Let $r\in\mathbb{N}$ be such that $\mathcal{N}_i={}^{\sigma^i}\mathcal{G}$ for $i=1,\ldots,r-1$ and $\mathcal{N}_r=1$. Then $\pi_r\colon N[r]\to N[r-1]$ is an isomorphism and $N[r-1]=\mathcal{G}[r-1]=\mathcal{G}\times\cdots\times{}^{\sigma^{r-1}}\mathcal{G}$. Define $\psi\colon\mathcal{G}\times\cdots\times{}^{\sigma^{r-1}}\mathcal{G}=N[r-1]\xrightarrow{\pi_r^{-1}}N[r]\to{}^{\sigma^r}\mathcal{G}$, where the last map is the projection onto the last coordinate. Then ψ is a morphism of algebraic groups and

$$N[r](T)=\{(g_0,\ldots,g_r)\in\mathcal{G}[i](T)\mid g_r=\psi(g_0,\ldots,g_{r-1})\}\tag{6.2}$$

for any k-algebra T. Moreover,

$$N(R)=\{g\in\mathcal{G}(R)\mid \sigma^r(g)=\psi(g,\dots,\sigma^{r-1}(g))\} \tag{6.3}$$

for any k-σ-algebra R. Set $\mathcal{H}=\mathcal{G}[r]/N[r]$. We claim that the morphism ${}^{\sigma^r}\mathcal{G}\to\mathcal{H},\ g\mapsto\overline{(1,\dots,1,g)}$ is an isomorphism. Clearly, the kernel is trivial and so the claim follows from $|\mathcal{H}|=\frac{|\mathcal{G}[r]|}{|N[r]|}=\frac{|\mathcal{G}|^{r+1}}{|\mathcal{G}|^r}=|{}^{\sigma^r}\mathcal{G}|$.

The inclusion $k[\mathcal{H}]\subseteq k[\mathcal{G}[r]]\subseteq k\{G\}$ of Hopf algebras, gives rise to a morphism $k\{\mathcal{H}\}\to k\{G\}$ of k-σ-Hopf algebras by Lemma 2.5. (Recall that $k\{\mathcal{H}\}=k\{[\sigma]_k\mathcal{H}\}=[\sigma]_k k[\mathcal{H}]$.) Let $\phi\colon G\to[\sigma]_k\mathcal{H}$ be the corresponding morphism of σ-algebraic groups. Note that ϕ can also be described as the composition

$$\begin{aligned}\phi\colon G=[\sigma]_k\mathcal{G}&\to[\sigma]_k\mathcal{G}\times\dots\times[\sigma]_k{}^{\sigma^r}\mathcal{G}\\ &=[\sigma]_k\mathcal{G}[r]\to[\sigma]_k\mathcal{G}[r]/[\sigma]_kN[r]=[\sigma]_k(\mathcal{G}[r]/N[r]),\end{aligned} \tag{6.4}$$

where the first map is given by $g\mapsto(g,\sigma(g),\dots,\sigma^r(g))$ for $g\in\mathcal{G}(R)$ and R a k-σ-algebra.

We claim that $\phi\colon G\to[\sigma]_k\mathcal{H}$ is a quotient map with kernel N. (So $G/N\simeq[\sigma]_k\mathcal{H}$ as desired.) Indeed, $\ker(\phi)=N$ by (6.2), (6.3) and (6.4). To see that ϕ is a quotient map, we have to show that $\phi^*\colon k\{\mathcal{H}\}\to k\{G\}$ is injective. It suffices to show that the restriction of ϕ^* to $k[\mathcal{H}[i]]\to k[\mathcal{G}[i+r]]$ is injective for every $i\in\mathbb{N}$. This restriction corresponds to the morphism

$$\begin{aligned}&\phi_i\colon\mathcal{G}\times\dots\times{}^{\sigma^{i+r}}\mathcal{G}\to\mathcal{H}\times\dots\times{}^{\sigma^i}\mathcal{H},\\ &(g_0,\dots,g_{i+r})\mapsto\left(\overline{(g_0,\dots,g_r)},\overline{(g_1,\dots,g_{1+r})},\dots,\overline{(g_i,\dots,g_{i+r})}\right)\end{aligned}$$

of étale algebraic groups. It suffices to show that ϕ_i is surjective on the k_s-points. But this follows from Lemma 6.27 with $\mathtt{G}_j=({}^{\sigma^j}\mathcal{G})(k_s)$ for $j=0,\dots,i+r$ and $\psi_j\colon\mathtt{G}_j\times\dots\times\mathtt{G}_{j+r-1}\to\mathtt{G}_{j+r}$ the base change of $\psi\colon\mathcal{G}\times\dots\times{}^{\sigma^{r-1}}\mathcal{G}\to{}^{\sigma^r}\mathcal{G}$ via $\sigma^j\colon k\to k$ (and then evaluated at k_s) for $j=0,\dots,i$. $\square$

Corollary 6.30. — *Let $\mathcal{G}$ be a σ-stably simple étale algebraic group. Then* $\mathrm{ld}(N)=1$ *for every proper normal σ-closed subgroup N of $\mathcal{G}$.*

Proof. — In case $\mathcal{G}$ is non-commutative, this follows from Lemma 6.18 and Corollaries 6.25 and 6.5. In case $\mathcal{G}$ is commutative, this follows from the proof of Proposition 6.29 ($\mathcal{N}_r=1$). $\square$

The following lemma provides a converse to Corollary 6.30.

Lemma 6.31. — *Let $\mathcal{G}$ be a non-trivial étale algebraic group. If* $\mathrm{ld}(N)\in\{1,|\mathcal{G}|\}$ *for every normal σ-closed subgroup N of $\mathcal{G}$, then $\mathcal{G}$ is σ-stably simple.*

Proof. — Suppose $\mathcal{G}$ is not σ-stably simple. Then there exists an $r \in \mathbb{N}$ and a closed normal subgroup $\mathcal{N}$ of ${}^{\sigma^r}\mathcal{G}$ such that $1 < |{}^{\sigma^r}\mathcal{G}/\mathcal{N}| < |\mathcal{G}|$. Using Corollary 6.13 and Lemma 6.14 we see that the morphism

$$\phi\colon [\sigma]_k\mathcal{G} \xrightarrow{F^r_{[\sigma]_k\mathcal{G}}} {}^{\sigma^r}([\sigma]_k\mathcal{G}) = [\sigma]_k{}^{\sigma^r}\mathcal{G} \to [\sigma]_k{}^{\sigma^r}\mathcal{G}/[\sigma]_k\mathcal{N} = [\sigma]_k({}^{\sigma^r}\mathcal{G}/\mathcal{N})$$

is a quotient map. Thus, $N = \ker(\phi)$ is a normal σ-closed subgroup of $G = [\sigma]_k\mathcal{G}$ and $\mathrm{ld}(G/N) = \mathrm{ld}([\sigma]_k({}^{\sigma^r}\mathcal{G}/\mathcal{N})) = |{}^{\sigma^r}\mathcal{G}/\mathcal{N}|$ by Example 4.4. So $1 < \mathrm{ld}(N) < |\mathcal{G}|$ by Proposition 2.14; a contradiction. ☐

6.4. The decomposition theorem

Some more preparations are in order before we can finally tackle the proof of the main decomposition theorem (Theorem 6.38). The following proposition provides an important step in the proof. Roughly speaking, it shows that in a subnormal series we can get rid of the top σ-infinitesimal quotient.

For simplicity, we call a σ-étale σ-algebraic group G *σ-stably simple benign* if $G \simeq [\sigma]_k\mathcal{G}$, where $\mathcal{G}$ is a σ-stably simple étale algebraic group.

Proposition 6.32. — *Let G be a σ-algebraic group with a subnormal series*

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

such that G/G_1 is σ-infinitesimal, G_i/G_{i+1} is σ-stably simple benign for $i = 1, \ldots, n$ and G_{n+1} is σ-infinitesimal. Then there exists a subnormal series

$$G \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_n \supseteq 1$$

such that G/H_1 and H_i/H_{i+1} ($i = 1, \ldots, n-1$) are σ-stably simple benign and H_n is σ-infinitesimal.

Proof. — Since G/G_1 is σ-infinitesimal, there exists an $r \in \mathbb{N}$ such that $(G/G_1)_{(r)} = G/G_1$ (Lemma 6.18). It is then clear from the commutative diagram

$$\begin{tikzcd} G \arrow[r] \arrow[d, "F^r_G"'] & G/G_1 \arrow[d, "F^r_{G/G_1}"] \\ {}^{\sigma^r}G \arrow[r] & {}^{\sigma^r}(G/G_1) \end{tikzcd}$$

that $(F^r_G)^{-1}({}^{\sigma^r}G_1) = G$. Define

$$H_i = (F^r_G)^{-1}({}^{\sigma^r}G_{i+1}) \quad \text{for} \quad i = 0, \ldots, n.$$

(So $H_0 = G$.) Because benign σ-algebraic groups are absolutely σ-reduced (Corollary 6.13), it follows from Lemma 6.19 that $H_i/H_{i+1} \simeq {}^{\sigma^r}(G_{i-1}/G_i)$ for $i = 0, \dots, n$. So, if $G_{i-1}/G_i \simeq [\sigma]_k \mathcal{G}_i$ with $\mathcal{G}_i$ a σ-stably simple étale algebraic group, then $H_i/H_{i+1} \simeq {}^{\sigma^r}([\sigma]_k\mathcal{G}_i) = [\sigma]_k {}^{\sigma^r}\mathcal{G}_i$.

Finally, as G_{n+1} is σ-infinitesimal, also ${}^{\sigma^r}G_{n+1}$ is σ-infinitesimal and therefore the σ-algebraic group $H_n = (F_G^r)^{-1}({}^{\sigma^r}G_{n+1})$ is σ-infinitesimal by Lemmas 6.8 and 6.18. □

Lemma 6.33. — *Let G be a σ-étale σ-algebraic group and $\mathcal{G}$ an étale algebraic group. If $\phi\colon G \to [\sigma]_k\mathcal{G}$ is a σ-closed embedding of σ-algebraic groups such that* $\mathrm{ld}(G) = |\mathcal{G}|$, *then ϕ is an isomorphism. In particular, G is benign.*

Proof. — We identify G with $\phi(G)$. For $i \in \mathbb{N}$ let $G[i]$ denote the i-th order Zariski closure of G in $\mathcal{G}$ and let $\mathcal{G}_i \leqslant G[i]$ denote the kernel of the projection $\pi_i\colon G[i] \to G[i-1]$ ($\mathcal{G}_0 = G[0]$). By Proposition 2.9 the sequence $(|\mathcal{G}_i|)_{i\in\mathbb{N}}$ is non-increasing and stabilizes with value $\mathrm{ld}(G) = |\mathcal{G}|$. But as $\mathcal{G}_0$ is an algebraic subgroup of $\mathcal{G}$, we must have $|\mathcal{G}_i| = |\mathcal{G}|$ for all $i \in \mathbb{N}$.

Since $\pi_i\colon G[i] \to G[i-1]$ is a quotient map with kernel $\mathcal{G}_i$, we have $|G[i]| = |G[i-1]| \cdot |\mathcal{G}_i|$ for $i \geqslant 1$. As $\mathcal{G}_0 = \mathcal{G}$, we find

$$|G[i]| = |\mathcal{G}_i| \cdots |\mathcal{G}_0| = |\mathcal{G}|^{i+1}.$$

But $G[i] \leqslant \mathcal{G} \times {}^{\sigma}\mathcal{G} \times \cdots \times {}^{\sigma^i}\mathcal{G} = \mathcal{G}[i]$. Therefore $G[i] = \mathcal{G}[i]$ for all i and it follows that $G = [\sigma]_k\mathcal{G}$ is benign. □

Let G be a σ-étale σ-algebraic group. Let $\mathcal{G}$ be an étale algebraic group and $\phi\colon G \to [\sigma]_k\mathcal{G}$ a morphism of σ-algebraic groups. Then $\phi(G)$ is a σ-étale σ-closed subgroup of $\mathcal{G}$ (Lemma 4.6). Let $\phi(G)[0]$ and $\phi(G)[1]$ denote the Zariski closures of $\phi(G)$ in $\mathcal{G}$ of order 0 and 1 respectively. Then $\phi(G)[0]$ and $\phi(G)[1]$ are étale algebraic groups (Lemma 4.7). Let $\pi_1\colon \phi(G)[1] \to \phi(G)[0]$ be the natural projection (as in the end of Section 2.2). We abbreviate

$$|\phi|_1 := |\ker(\pi_1)|.$$

By Proposition 2.9 we have $|\phi|_1 \leqslant \mathrm{ld}(\phi(G))$. If $\ker(\phi)$ is σ-infinitesimal (e.g., trivial), then

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

by Corollary 6.5. So $|\phi|_1 \leqslant \mathrm{ld}(G)$.

Definition 6.34. — *Let G be a σ-étale σ-algebraic group and $\mathcal{G}$ an étale algebraic group. A morphism $\phi\colon G \to [\sigma]_k\mathcal{G}$ of σ-algebraic groups is* a standard embedding of G (into $\mathcal{G}$) *if*

- *ϕ is a σ-closed embedding,*
- *$\phi(G)$ is Zariski dense in $\mathcal{G}$ and*
- $\operatorname{ld}(G)=|\phi|_1$.

In the context of symbolic dynamics (cf. Remark 5.18) the construction in the proof of the following lemma is known as "passing to a higher block shift" ([19, Section 1.4]).

Lemma 6.35. — *Let G be a σ-étale σ-algebraic group. Then there exists a standard embedding of G.*

Proof. — By Proposition 2.7 there exists an algebraic group $\mathcal{H}$ and a σ-closed embedding $G\to[\sigma]_k\mathcal{H}$ of σ-algebraic groups. By Lemma 4.7 the Zariski closures $G[i]_{\mathcal{H}}$ of G in $\mathcal{H}$ are étale algebraic groups. Let $\mathcal{H}_i$ denote the kernel of the projection $\pi_i\colon G[i]_{\mathcal{H}}\to G[i-1]_{\mathcal{H}}$. By Proposition 2.9 there exists an $m\geqslant 0$ such that $|\mathcal{H}_{m+1}|=\operatorname{ld}(G)$.

Set $\mathcal{G}=G[m]_{\mathcal{H}}$. The inclusion $k[\mathcal{G}]\subseteq k\{G\}$ of k-algebras, induces a surjective morphism $k\{\mathcal{G}\}=[\sigma]_k k[\mathcal{G}]\to k\{G\}$ of k-σ-algebras. Since $k[\mathcal{G}]\subseteq k\{G\}$ is an inclusion of Hopf algebras, $k\{\mathcal{G}\}\to k\{G\}$ is a morphism of k-σ-Hopf algebras (Lemma 2.5). Let $\phi\colon G\to[\sigma]_k\mathcal{G}$ denote the corresponding σ-closed embedding of σ-algebraic groups and for $i\geqslant 0$ let $G[i]_{\mathcal{G}}$ denote the i-th order Zariski closure of G in $\mathcal{G}$. Then $G[i]_{\mathcal{G}}=G[m+i]_{\mathcal{H}}$ for every $i\geqslant 0$. Let $\mathcal{G}_i$ denote the kernel of the projection $\pi_i\colon G[i]_{\mathcal{G}}\to G[i-1]_{\mathcal{G}}$. Then $\mathcal{G}_i=\mathcal{H}_{m+i}$ for $i\geqslant 1$. Therefore $|\phi|_1=|\mathcal{G}_1|=|\mathcal{H}_{m+1}|=\operatorname{ld}(G)$. So ϕ is a standard embedding. $\square$

Definition 6.36. — *Let G be a σ-étale σ-algebraic group and $\mathcal{G}$ an étale algebraic group. A morphism $\phi\colon G\to[\sigma]_k\mathcal{G}$ of σ-algebraic groups is a* substandard embedding *of G (into $\mathcal{G}$) if*

- $\ker(\phi)$ *is σ-infinitesimal,*
- *$\phi(G)$ is Zariski dense in $\mathcal{G}$ and*
- $\operatorname{ld}(G)=|\phi|_1$.

A substandard embedding $G\to[\sigma]_k\mathcal{G}$ of G is minimal *if $|\mathcal{G}|\leqslant|\mathcal{H}|$ for any substandard embedding $G\to[\sigma]_k\mathcal{H}$ of G.*

Note that, despite the name, a substandard embedding need not be a σ-closed embedding. Since a standard embedding is a substandard embedding it is clear from Lemma 6.35 that for any σ-étale σ-algebraic group there exists a minimal substandard embedding.

Lemma 6.37. — *Let G be a σ-étale σ-algebraic group and let $\phi\colon G\to[\sigma]_k\mathcal{G}$ be a minimal substandard embedding. Then for every $r\in\mathbb{N}$ the dimension of $k[\sigma^r(k[\mathcal{G}])]\subseteq k\{G\}$ as a k-vector space equals $|\mathcal{G}|$.*

Proof. — First of all, note that $k[\mathcal{G}]$ can be identified with a k-Hopf subalgebra of $k\{G\}$ because $\phi(G)$ is Zarsiki dense in $\mathcal{G}$. By Corollary 6.13 the σ-algebraic group $[\sigma]_k\mathcal{G}$ is absolutely σ-reduced. It therefore follows from Corollary 6.17 that

$$[\sigma]_k\mathcal{G}/([\sigma]_k\mathcal{G})_{(r)} = {}^{\sigma^r}([\sigma]_k\mathcal{G}) = [\sigma]_k({}^{\sigma^r}\mathcal{G}).$$

The image of $k[{}^{\sigma^r}\mathcal{G}]$ under the dual map of

$$\widetilde{\phi}\colon G \xrightarrow{\phi} [\sigma]_k\mathcal{G} \to [\sigma]_k\mathcal{G}/([\sigma]_k\mathcal{G})_{(r)} = [\sigma]_k({}^{\sigma^r}\mathcal{G})$$

equals $k[\sigma^r(k[\mathcal{G}])]$. Let $\mathcal{G}' \leqslant {}^{\sigma^r}\mathcal{G}$ denote the Zariski closure of $\widetilde{\phi}(G)$ in ${}^{\sigma^r}\mathcal{G}$. Then $k[\mathcal{G}'] = k[\sigma^r(k[\mathcal{G}])]$ and $\widetilde{\phi}$ induces a morphism $\phi'\colon G \to [\sigma]_k\mathcal{G}'$ of σ-algebraic groups.

We will show that ϕ' is a substandard embedding. By construction, $\phi'(G)$ is Zariski dense in $\mathcal{G}'$. Because $\ker(\phi)$ and $([\sigma]\mathcal{G})_{(r)}$ are σ-infinitesimal (Lemma 6.18), it follows from Lemma 6.8 that

$$\ker(\phi') = \ker(\widetilde{\phi}) = \phi^{-1}([\sigma]_k\mathcal{G})_{(r)})$$

is σ-infinitesimal.

Let $\phi(G)[1] \leqslant \mathcal{G} \times {}^{\sigma}\mathcal{G}$ denote the first order Zariski closure of $\phi(G)$ in $\mathcal{G}$ and let $\mathcal{G}_1$ denote the kernel of $\pi_1\colon \phi(G)[1] \to \mathcal{G}$. Then $|\mathcal{G}_1| = \mathrm{ld}(G)$ because ϕ is a substandard embedding. Similarly, let $\phi'(G)[1] \leqslant \mathcal{G}' \times {}^{\sigma}(\mathcal{G}') \leqslant {}^{\sigma^r}\mathcal{G} \times {}^{\sigma^{r+1}}\mathcal{G}$ denote the first order Zariski closure of $\phi'(G)$ in $\mathcal{G}'$ and let $\mathcal{G}_1'$ denote the kernel of $\pi_1\colon \phi'(G)[1] \to \mathcal{G}'$. The surjective morphism of k-algebras

$$\begin{aligned}{}^{\sigma^r}(k[\phi(G)[1]]) = k[k[\mathcal{G}], \sigma(k[\mathcal{G}])] \otimes_k k \to k[\sigma^r(k[\mathcal{G}]), \sigma^{r+1}(k[\mathcal{G}])],\\ f \otimes \lambda \mapsto \sigma^r(f)\lambda\end{aligned}$$

corresponds to a closed embedding $\phi'(G)[1] \to {}^{\sigma^r}(\phi(G)[1])$ of algebraic groups, that maps $\mathcal{G}_1'$ into ${}^{\sigma^r}\mathcal{G}_1$. Therefore $|\mathcal{G}_1'| \leqslant |{}^{\sigma^r}\mathcal{G}_1| = |\mathcal{G}_1| = \mathrm{ld}(G)$. On the other hand, $|\mathcal{G}_1'| \geqslant \mathrm{ld}(\phi'(G))$ by Proposition 2.9 and

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

because $\ker(\phi')$ is σ-infinitesimal and therefore $\mathrm{ld}(\ker(\phi')) = 1$ by Corollary 6.5. It follows that $|\mathcal{G}_1'| \geqslant \mathrm{ld}(G)$ and thus $|\mathcal{G}_1'| = \mathrm{ld}(G)$.

So ϕ' is a substandard embedding. Because ϕ is a minimal substandard embedding, it follows that $|\mathcal{G}'| \geqslant |\mathcal{G}|$. But $\mathcal{G}' \leqslant {}^{\sigma^r}\mathcal{G}$ and so $\mathcal{G}' = {}^{\sigma^r}\mathcal{G}$. Therefore $k[\sigma^r(k[\mathcal{G}])] = k[\mathcal{G}'] = {}^{\sigma^r}(k[\mathcal{G}])$ has dimension $|\mathcal{G}|$ over k. □

Finally, we are prepared for the proof of our decomposition theorem for σ-étale σ-algebraic groups.

Theorem 6.38. — *Let G be a σ-étale σ-algebraic group. Then there exists a subnormal series*

$$G \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_n \supseteq 1 \tag{6.5}$$

such that $G_1 = G^{\sigma o}$, G_n is σ-infinitesimal and $G_i/G_{i+1} \simeq [\sigma]_k \mathcal{G}_i$ for some σ-stably simple étale algebraic group $\mathcal{G}_i$ for $i = 1, \ldots, n-1$.

If

$$G \supseteq H_1 \supseteq H_2 \supseteq \cdots \supseteq H_m \supseteq 1 \tag{6.6}$$

is another subnormal series such that $H_1 = G^{\sigma o}$, H_m is σ-infinitesimal and $H_i/H_{i+1} \simeq [\sigma]_k \mathcal{H}_i$ for some σ-stably simple étale algebraic group $\mathcal{H}_i$ for $i = 1, \ldots, m-1$, then $m = n$ and there exists a permutation τ such that $\mathcal{G}_i$ and $\mathcal{H}_{\tau(i)}$ are σ-stably equivalent.

Proof. — We first handle the existence part. We will prove the existence of the required subnormal series by induction on $\mathrm{ld}(G)$. If $\mathrm{ld}(G) = 1$, then $k\{G\}$ is finitely generated as a k-algebra by Lemma 2.10. Because G is σ-étale, this implies that G is finite. Thus $G^{\sigma o}$ is a finite σ-connected σ-étale σ-algebraic group and therefore σ-infinitesimal by Lemma 6.7. So the subnormal series $G \supseteq G^{\sigma o} \supseteq 1$ has the required properties.

We may thus assume that $\mathrm{ld}(G) > 1$. Replacing G with $G^{\sigma o}$, we may also assume that G is σ-connected (Corollary 3.24).

Step 1. — Assume that there exists no normal σ-closed subgroup N of G such that $1 < \mathrm{ld}(N) < \mathrm{ld}(G)$. We will show that there exists a normal σ-infinitesimal σ-closed subgroup G_2 of G such that $G/G_2 \simeq [\sigma]_k \mathcal{G}$ for a σ-stably simple étale algebraic group $\mathcal{G}$. (Thus the existence part is satisfied with $n = 2$ and $G_1 = G$.)

Let $\phi\colon G \to \mathcal{G}$ be a minimal substandard embedding. We will eventually show that

$$\mathrm{ld}(G) = |\mathcal{G}|. \tag{6.7}$$

Let $\phi(G)[1] \leqslant \mathcal{G} \times {}^{\sigma}\mathcal{G}$ denote the first order Zariski closure of $\phi(G)$ in $\mathcal{G}$. We have morphisms of algebraic groups

$$\mathcal{G} \times {}^{\sigma}\mathcal{G} \to \mathcal{G},\ (g_0, g_1) \mapsto g_0 \quad \text{and} \quad \mathcal{G} \times {}^{\sigma}\mathcal{G} \to {}^{\sigma}\mathcal{G},\ (g_0, g_1) \mapsto g_1$$

that induce morphisms $\pi_1 \colon \phi(G)[1] \to \mathcal{G} (= \phi(G)[0])$ and $\sigma_1 \colon \phi(G)[1] \to {}^{\sigma}\mathcal{G}$. Set $\mathcal{G}_1 = \ker(\pi_1)$ and $\mathcal{G}' = \ker(\sigma_1)$. Then $\mathcal{G}'\mathcal{G}_1$ is a normal closed subgroup of $\phi(G)[1]$ and we define $\mathcal{H} = \phi(G)[1]/\mathcal{G}'\mathcal{G}_1$. We will next show that

$$|\mathcal{G}| = |\mathcal{H}| \cdot \mathrm{ld}(G). \tag{6.8}$$

Because $\mathcal{G}'\mathcal{G}_1 \simeq \mathcal{G}' \times \mathcal{G}_1$, it follows from $|\mathcal{H}| = \frac{|\phi(G)[1]|}{|\mathcal{G}'\mathcal{G}_1|}$ that

$$|\mathcal{H}| \cdot |\mathcal{G}_1| = \frac{|\phi(G)[1]|}{|\mathcal{G}'|} = |\phi(G)[1]/\mathcal{G}'|. \tag{6.9}$$

As ϕ is a substandard embedding, $|\mathcal{G}_1| = \mathrm{ld}(G)$. Since $k[\phi(G)[1]/\mathcal{G}'] = k[\sigma(k[\mathcal{G}])] \subseteq k\{G\}$, it follows from Lemma 6.37 that $|\phi(G)[1]/\mathcal{G}'| = |\mathcal{G}|$. Thus (6.8) follows from (6.9).

We have $k[\phi(G)[1]/\mathcal{G}_1] = k[\mathcal{G}]$ and $k[\phi(G)[1]/\mathcal{G}'] = k[\sigma(k[\mathcal{G}])]$. Therefore

$$k[\mathcal{H}] = k[\mathcal{G}] \cap k[\sigma(k[\mathcal{G}])] \subseteq k\{G\}.$$

Since $k[\mathcal{H}]$ is a Hopf subalgebra of $k\{G\}$, we have an induced morphism $[\sigma]_k k[\mathcal{H}] = k\{\mathcal{H}\} \to k\{G\}$ of k-σ-Hopf algebras (Lemma 2.5) that corresponds to a morphism $\phi' \colon G \to [\sigma]_k\mathcal{H}$ of σ-algebraic groups. Let $N \trianglelefteq G$ denote the kernel of ϕ'. By our assumption on G, we have $\mathrm{ld}(N) = 1$ or $\mathrm{ld}(N) = \mathrm{ld}(G)$. So we have to distinguish these two cases.

Case 1. — Let us first suppose that $\mathrm{ld}(N) = 1$. Then $\mathrm{ld}(G/N) = \mathrm{ld}(G)$. We will show that ϕ' is a substandard embedding. Because $k[\mathcal{H}] \subseteq k\{G\}$, we see that $\phi'(G)$ is Zariski dense in $\mathcal{H}$. Let $\phi'(G)[1] \leqslant \mathcal{H} \times {}^{\sigma}\mathcal{H}$ denote the first order Zariski closure of $\phi'(G)$ in $\mathcal{H}$ and let $\mathcal{H}_1$ denote the kernel of $\pi_1 \colon \phi'(G)[1] \to \mathcal{H}$. Using Proposition 2.9 we see that

$$|\phi'(G)[1]| = |\mathcal{H}| \cdot |\mathcal{H}_1| \geqslant |\mathcal{H}| \cdot \mathrm{ld}(\phi'(G)) = |\mathcal{H}| \cdot \mathrm{ld}(G/N) = |\mathcal{H}| \cdot \mathrm{ld}(G). \tag{6.10}$$

We will show that $\phi'(G)[1] = \phi(G)[1]/\mathcal{G}'$. Because

$$k[\phi'(G)[1]] = k[k[\mathcal{H}], \sigma(k[\mathcal{H}])] \subseteq k[\sigma(k[\mathcal{G}])] = k[\phi(G)[1]/\mathcal{G}'],$$

it suffices to show that $|\phi'(G)[1]| = |\phi(G)[1]/\mathcal{G}'|$. But using Lemma 6.37, we find that

$$|\phi'(G)[1]| \leqslant |\phi(G)[1]/\mathcal{G}'| = \dim_k(k[\sigma(k[\mathcal{G}])]) = |\mathcal{G}| = |\mathcal{H}| \cdot \mathrm{ld}(G). \tag{6.11}$$

The combination of equations (6.10) and (6.11) shows that $|\phi'(G)[1]| = |\mathcal{H}| \cdot \mathrm{ld}(G)$ and that $|\mathcal{H}_1| = \mathrm{ld}(\phi'(G))$. It also follows that $k[k[\mathcal{H}], \sigma(k[\mathcal{H}])] = k[\sigma(k[\mathcal{G}])]$ and therefore

$$k\{G/N\} = k\{k[\mathcal{H}]\} = k\{\sigma(k[\mathcal{G}])\}.$$

We will next show that $N = \ker(\phi')$ is σ-infinitesimal. As $k\{k[\mathcal{G}]\} = k\{\phi(G)\} \subseteq k\{G\}$, it follows that

$$k\{\sigma(k[\mathcal{G}])\} = k[\sigma(k\{\phi(G)\})] = k\{\phi(G)/\phi(G)_{(1)}\} \subseteq k\{G\}.$$

So $k\{G/N\} = k\{\phi(G)/\phi(G)_{(1)}\}$ and therefore N is the kernel of

$$G \xrightarrow{\phi} \phi(G) \to \phi(G)/\phi(G)_{(1)}.$$

Thus N is σ-infinitesimal by Lemmas 6.18 and 6.8. Therefore

$$|\mathcal{H}_1| = \mathrm{ld}(\phi'(G)) = \mathrm{ld}(G/N) = \frac{\mathrm{ld}(G)}{\mathrm{ld}(N)} = \mathrm{ld}(G)$$

by Corollary 6.5. In summary, we have shown that ϕ' is a substandard embedding. But $|\mathcal{H}| < |\mathcal{H}|\cdot\mathrm{ld}(G) = |\mathcal{G}|$ because $\mathrm{ld}(G) > 1$. This contradicts the assumption that ϕ is a minimal substandard embedding. Thus the case $\mathrm{ld}(N) = 1$ cannot occur.

Case 2. — So we must have $\mathrm{ld}(N) = \mathrm{ld}(G)$. Then $\mathrm{ld}(G/N) = 1$ and therefore G/N is finite (Lemma 2.10). Because G is σ-connected, also G/N is σ-connected (Proposition 3.35). So G/N is a finite, σ-connected, σ-étale difference algebraic group and must therefore be σ-infinitesimal by Lemma 6.7. So by Lemma 6.4 there exists an $r \in \mathbb{N}$ such that $\sigma^r(\mathfrak{m}_{G/N}) = 0$. Since $k\{G/N\} = k\{k[\mathcal{H}]\}$, we have $\mathfrak{m}_{\mathcal{H}} \subseteq \mathfrak{m}_{G/N}$, in particular, $\sigma^r(\mathfrak{m}_{\mathcal{H}}) = 0$.

On the other hand, $\mathfrak{m}_{\mathcal{H}} \subseteq k[\mathcal{H}] \subseteq k[\mathcal{G}]$ and by Lemma 6.37 the dimension of $k[\sigma^r(k[\mathcal{G}])]$ as a k-vector space equals $|\mathcal{G}|$. So no non-zero element of $k[\mathcal{G}]$ can map to zero under σ^r. Thus $\mathfrak{m}_{\mathcal{H}} = 0$. This means that $\mathcal{H} = 1$. Thus $|\mathcal{G}| = \mathrm{ld}(G)$ by (6.8) and finally (6.7) is proved.

The σ-algebraic group $G_2 = \ker(\phi)$ is σ-infinitesimal because ϕ is a substandard embedding and Lemma 6.33 applied to the induced embedding $G/G_2 \to [\sigma]_k\mathcal{G}$ shows that $G/G_2 \simeq [\sigma]_k\mathcal{G}$ is benign, because

$$\mathrm{ld}(G/G_2) = \frac{\mathrm{ld}(G)}{\mathrm{ld}(G_2)} = \mathrm{ld}(G) = |\mathcal{G}|$$

by Corollary 6.5. It remains to show that $\mathcal{G}$ is σ-stably simple.

As $\mathrm{ld}(N) \in \{1, \mathrm{ld}(G)\}$ for every normal σ-closed subgroup N of G, we also have $\mathrm{ld}(N) \in \{1, \mathrm{ld}(G/G_2)\}$ for ever normal σ-closed subgroup N of G/G_2 by Theorem 2.20. Thus $\mathcal{G}$ is σ-stably simple by Lemma 6.31 and $G = G_1 \supseteq G_2 \supseteq 1$ is the required subnormal series.

Step 2. — Assume that there exists a normal σ-closed subgroup N of G such that $1 < \mathrm{ld}(N) < \mathrm{ld}(G)$. Because $N^{\sigma o}$ is a characteristic subgroup of N (Theorem 3.31), it follows that $N^{\sigma o}$ also is a normal σ-closed subgroup of G. We have $\mathrm{ld}(N) = \mathrm{ld}(N^{\sigma o})$ by Proposition 3.32. 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 (Proposition 3.35). So 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 σ-stably simple benign for $i = 0, \ldots, n-1$, where $G_0 := G$ (Theorem 2.20).

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} σ-stably simple benign for $i = 0, \ldots, m-1$ ($N_0 := N$). By Proposition 6.32, 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} σ-stably simple benign for $i = 1, \ldots, m-1$ 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 part. We may assume that G is σ-connected, i.e., $G = G_1 = H_1$. By Theorem 2.21 the subnormal series (6.5) and (6.6) have equivalent refinements. Let

$$\begin{aligned} G = G_1 \supseteq G_{1,1} \supseteq G_{1,2} \supseteq \cdots \supseteq G_{1,r_1} \\ \supseteq G_2 \supseteq \cdots \supseteq G_n \supseteq G_{n,1} \supseteq \cdots \supseteq G_{n,r_n} \supseteq 1 \end{aligned} \tag{6.12}$$

be such a refinement (where all the inclusion are strict). Then, for $i = 1, \ldots, n-1$, the σ-algebraic group $G_{i,1}/G_{i+1}$ is a normal proper σ-closed subgroup of $G_i/G_{i+1} \simeq [\sigma]_k \mathcal{G}_i$. By Corollary 6.30 we have $\mathrm{ld}(G_{i,1}/G_{i+1}) = 1$. Thus $\mathrm{ld}(G_{i,j}/G_{i+1}) = 1$ for $j = 1, \ldots, r_i$ and so $\mathrm{ld}(G_{i,1}) = \mathrm{ld}(G_{i,2}) = \cdots = \mathrm{ld}(G_{i,r_i}) = \mathrm{ld}(G_{i+1})$. Therefore, of the factor groups of the subnormal series (6.12), there are exactly $n-1$ with limit degree > 1, namely $G_i/G_{i,1}$ for $i = 1, \ldots, n-1$.

The same argument applied to (6.6), instead of (6.5), shows that in the refinement of (6.6), there are exactly $m-1$ factor groups with limit degree > 1. Since the two refinements are equivalent, we deduce that $n = m$.

Moreover, $G_i/G_{i,1} \simeq [\sigma]_k \mathcal{G}_i'$, where $\mathcal{G}_i'$ is σ-stably equivalent to $\mathcal{G}_i$ by Proposition 6.29. A similar statement holds for the refinement of the subnormal series (6.6). The equivalence of the two refinements combined with Proposition 6.20 yields the sought for permutation τ. $\square$

We conclude the article with some examples illustrating Theorem 6.38. The following simple example shows that in the conclusion of Theorem 6.38 one cannot replace "σ-stably equivalent" with "isomorphic".

Example 6.39. — Let $\mathcal{G}$ be a σ-stably simple étale algebraic group and $G = [\sigma]_k\mathcal{G}$. For every $r \geqslant 1$ the normal σ-closed subgroup $G_{(r)}$ of G is σ-infinitesimal and $G/G_{(r)} \simeq {}^{\sigma^r}G = [\sigma]_k {}^{\sigma^r}\mathcal{G}$ (Lemmas 6.18, 6.14 and Corollary 6.13). Thus, for every r the subnormal series $G \supseteq G_{(r)} \supseteq 1$ is as required by Theorem 6.38.

Example 6.40. — Let $\mathcal{G}$ be an étale algebraic group. We would like to find a subnormal series for $G = [\sigma]_k\mathcal{G}$ as in Theorem 6.38. There exists a subnormal series $\mathcal{G} = \mathcal{G}_0 \supseteq \mathcal{G}_1 \supseteq \cdots \supseteq \mathcal{G}_m = 1$ for $\mathcal{G}$ such that $\mathcal{G}_i/\mathcal{G}_{i+1}$ is simple for $i = 0, \ldots, m-1$. However, $\mathcal{G}_i/\mathcal{G}_{i+1}$ may not be σ-stably simple. Since the length of such a decomposition series for ${}^{\sigma^r}\mathcal{G}$ is bounded by $|\mathcal{G}|$, there exists an $r \in \mathbb{N}$ and a subnormal series ${}^{\sigma^r}\mathcal{G} = \mathcal{G}_0 \supseteq \mathcal{G}_1 \supseteq \cdots \supseteq \mathcal{G}_{n-1} = 1$ for ${}^{\sigma^r}\mathcal{G}$ such that $\mathcal{G}_i/\mathcal{G}_{i+1}$ is σ-stably simple for $i = 0, \ldots, n-2$. Set $G_i = (F_G^r)^{-1}([\sigma]_k\mathcal{G}_{i-1})$ for $i = 2, \ldots, n$. We claim that

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

is a subnormal series as in Theorem 6.38.

First of all, note that G is σ-connected by Example 3.25. So $G = G_1$ is justified. As $F_G^r \colon G \to {}^{\sigma^r}G$ is a quotient map (Lemmas 6.13, 6.14), we see, using Theorem 2.20, that $G_i/G_{i+1} \simeq [\sigma]_k\mathcal{G}_{i-1}/[\sigma]_k\mathcal{G}_i = [\sigma]_k(\mathcal{G}_{i-1}/\mathcal{G}_i)$ is σ-stably simple benign for $i = 1, \ldots, n-1$. Moreover, $G_n = G_{(r)}$ is σ-infinitesimal by Lemma 6.18.

Example 6.41. — Let G be the σ-algebraic group given by

$$G(R) = \{g \in R^\times \mid g^4 = 1,\ \sigma(g)^2 = 1\}$$

for any k-σ-algebra R. We assume that the characteristic of k is not equal to 2, so that G is σ-étale. We already noted in Example 3.36 that G is σ-connected. Let G_2 be the σ-closed subgroup of G given by $G_2(R) = \{g \in R^\times \mid g^4 = 1,\ \sigma(g) = 1\}$ for any k-σ-algebra R. Then $\mathcal{G}$ is σ-infinitesimal and the quotient G/G_2 is benign. Indeed, $G/G_2 = [\sigma]_k\mathcal{G}$, where $\mathcal{G}$ is the algebraic group given by $\mathcal{G}(T) = \{g \in T^\times \mid g^2 = 1\}$ for any k-algebra T. (Cf. Example 3.36.) Since $\mathcal{G}$ is σ-stably simple, we see that

$$G = G^{\sigma o} = G_1 \supseteq G_2 \supseteq 1$$

is a subnormal series as in Theorem 6.38.

The following example is inspired by [14, Example 4].

Example 6.42. — Let G be the σ-closed subgroup of $\mathbb{G}_m^2$ given by

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

for any k-σ-algebra R. Let us assume that the characteristic of k is not equal to two, so that G is σ-étale. Indeed, G is a Zariski dense σ-closed subgroup of the étale algebraic group $\mathcal{G} = \mu_4 \times \mu_2$.

Define a σ-closed subgroup G_2 of G by

$$G_2(R) = \{(g,h) \in G(R) \mid h = 1\} = \{(g,1) \in \mathbb{G}_m^2(R) \mid g^2 = 1\}.$$

So $G_2 \simeq [\sigma]_k\mu_2$ is σ-stably simple benign. The morphism $\phi\colon G \to [\sigma]_k\mathbb{G}_m$, $(g,h) \to h$ has kernel G_2 and $\phi(G) = [\sigma]_k\mu_2$. Thus $G/G_2 \simeq [\sigma]_k\mu_2$ is also σ-stably simple benign. So there exists a short exact sequence

$$1 \to [\sigma]_k\mu_2 \to G \to [\sigma]_k\mu_2 \to 1. \tag{6.13}$$

By Proposition 3.35 and Example 3.25 the σ-algebraic group G is σ-connected. So

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

is a subnormal series as in Theorem 6.38.

Example 6.43. — Let G be the σ-algebraic group given by

$$G(R) = \left\{(g_1,g_2,g_3) \in (R^\times)^3 \mid g_1^4 = g_2^4 = g_3^2 = 1,\ \sigma(g_1) = g_2^2,\ \sigma(g_3) = g_3\right\} \leqslant \mathbb{G}_m(R)^3$$

for any k-σ-algebra R. We assume that the characteristic of k is not equal to 2, so that G is σ-étale. Let G_1, G_2 and G_3 be the σ-closed subgroups of G given by

$$G_1(R) = \left\{(g_1,g_2,1) \in (R^\times)^3 \,\middle|\, g_1^4 = g_2^4 = 1,\ \sigma(g_1) = g_2^2\right\} \leqslant G(R),$$
$$G_2(R) = \left\{(g_1,g_2,1) \in (R^\times)^3 \,\middle|\, g_1^4 = g_2^2 = 1,\ \sigma(g_1) = 1\right\} \leqslant G(R)$$

and

$$G_3(R) = \left\{(g_1,1,1) \in (R^\times)^3 \,\middle|\, g_1^4 = 1,\ \sigma(g_1) = 1\right\} \leqslant G(R)$$

for any k-σ-algebra R. We will show that

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

is a subnormal series for G as in Theorem 6.38.

The quotient map $\phi\colon G_1 \to [\sigma]_k\mu_4$ given by

$$\phi_R\colon G_1(R) \to \mu_4(R),\ (g_1,g_2,1) \mapsto g_2$$

has kernel G_3. So $G_1/G_3 \simeq [\sigma]_k\mu_4$ is benign. As $\phi(G_2) = [\sigma]_k\mu_2 \leqslant [\sigma]_k\mu_4$, we see that $G_1/G_2 \simeq [\sigma]_k\mu_2$ and $G_2/G_3 \simeq [\sigma]_k\mu_2$ are σ-stably simple benign.

Clearly G_3 is σ-infinitesimal. So it remains to show that $G_1 = G^{\sigma o}$. We have an exact sequence

$$1 \to G_3 \to G_1 \to [\sigma]_k\mu_4 \to 1,$$

with G_3 and $[\sigma]_k\mu_4$ σ-connected (Corollary 6.5 and Example 3.25). Therefore G_1 is σ-connected by Proposition 3.35. To show that $G_1 = G^{\sigma o}$, it suffices to show that G/G_1 is strongly σ-étale (Proposition 3.33). Let H be the σ-closed subgroup of $\mathbb{G}_m$ given by

$$H(R) = \{h \in R^\times \mid h^2 = 1,\ \sigma(h) = h\}$$

for any k-σ-algebra R. The quotient map $G \to H,\ (g_1, g_2, g_3) \mapsto g_3$ has kernel G_1 and so $G/G_1 \simeq H$ is strongly σ-étale (Example 3.8).

BIBLIOGRAPHY

[1] A. Bachmayr & M. Wibmer, "Algebraic groups as difference Galois groups of linear differential equations", *J. Pure Appl. Algebra* **226** (2022), no. 2, article no. 106854 (26 pages).

[2] F. Borceux & G. Janelidze, *Galois theories*, Cambridge Studies in Advanced Mathematics, vol. 72, Cambridge University Press, 2001, xiv+341 pages.

[3] N. Bourbaki, *Elements of Mathematics. Algebra. II. Chapters 4–7*, Springer, 1990, translated from the French by P. M. Cohn and J. Howie, vii+461 pages.

[4] M. Boyle & M. Schraudner, "$\mathbb{Z}^d$ group shifts and Bernoulli factors", *Ergodic Theory Dyn. Syst.* **28** (2008), no. 2, p. 367-387.

[5] A. Buium, *Differential algebraic groups of finite dimension*, Lecture Notes in Mathematics, vol. 1506, Springer, 1992, xvi+145 pages.

[6] T. P. Bywaters, H. Glöckner & S. Tornier, "Contraction groups and passage to subgroups and quotients for endomorphisms of totally disconnected locally compact groups", *Isr. J. Math.* **227** (2018), no. 2, p. 691-752.

[7] Z. Chatzidakis & E. Hrushovski, "An invariant for difference field extensions", *Ann. Fac. Sci. Toulouse, Math.* **21** (2012), no. 2, p. 217-234.

[8] R. M. Cohn, *Difference algebra*, Interscience Publishers, 1965, xiv+355 pages.

[9] L. Di Vizio, C. Hardouin & M. Wibmer, "Difference Galois theory of linear differential equations", *Adv. Math.* **260** (2014), p. 1-58.

[10] F. Fagnani, "Some results on the classification of expansive automorphisms of compact abelian groups", *Ergodic Theory Dyn. Syst.* **16** (1996), no. 1, p. 45-50.

[11] A. Giordano Bruno & S. Virili, "Topological entropy in totally disconnected locally compact groups", *Ergodic Theory Dyn. Syst.* **37** (2017), no. 7, p. 2163-2186.

[12] H. Glöckner & C. R. E. Raja, "Expansive automorphisms of totally disconnected, locally compact groups", *J. Group Theory* **20** (2017), no. 3, p. 589-619.

[13] J. C. Jantzen, *Representations of algebraic groups*, Pure and Applied Mathematics, vol. 131, Academic Press Inc., 1987, xiv+443 pages.

[14] B. P. Kitchens, "Expansive dynamics on zero-dimensional groups", *Ergodic Theory Dyn. Syst.* **7** (1987), no. 2, p. 249-261.

[15] ———, *Symbolic dynamics. One-sided, two-sided and countable state Markov shifts*, Universitext, Springer, 1998, x+252 pages.

[16] B. P. Kitchens & K. Schmidt, "Automorphisms of compact groups", *Ergodic Theory Dyn. Syst.* **9** (1989), no. 4, p. 691-735.

[17] E. R. Kolchin, *Differential algebraic groups*, Pure and Applied Mathematics, vol. 114, Academic Press Inc., 1985, xvii+271 pages.

[18] A. Levin, *Difference algebra*, Algebra and Applications, vol. 8, Springer, 2008, xii+519 pages.

[19] D. Lind & B. Marcus, *An introduction to symbolic dynamics and coding*, Cambridge University Press, 1995, xvi+495 pages.

[20] J. S. Milne, *Algebraic groups. The theory of group schemes of finite type over a field*, Cambridge Studies in Advanced Mathematics, vol. 170, Cambridge University Press, 2017, xvi+644 pages.

[21] A. Ovchinnikov & M. Wibmer, "σ-Galois theory of linear difference equations", *Int. Math. Res. Not.* (2015), no. 12, p. 3962-4018.

[22] C. D. Reid, "Endomorphisms of profinite groups", *Groups Geom. Dyn.* **8** (2014), no. 2, p. 553-564.

[23] L. Ribes & P. Zalesskii, *Profinite groups*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, vol. 40, Springer, 2010, xvi+464 pages.

[24] K. Schmidt, *Dynamical systems of algebraic origin*, Progress in Mathematics, vol. 128, Birkhäuser, 1995, xviii+310 pages.

[25] R. Shah, "Expansive automorphisms on locally compact groups", *New York J. Math.* **26** (2020), p. 285-302.

[26] The Stacks Project Authors, "The Stacks project", 2022, `https://stacks.math.columbia.edu`.

[27] W. A. Sutherland, *Introduction to metric and topological spaces*, Oxford University Press, 2009, xii+206 pages.

[28] T. Szamuely, *Galois groups and fundamental groups*, Cambridge Studies in Advanced Mathematics, vol. 117, Cambridge University Press, 2009, x+270 pages.

[29] I. Tomašić & M. Wibmer, "Strongly étale difference algebras and Babbitt's decomposition", *J. Algebra* **504** (2018), p. 10-38.

[30] ———, "Difference Galois theory and dynamics", *Adv. Math.* **402** (2022), article no. 108328 (61 pages).

[31] W. C. Waterhouse, *Introduction to affine group schemes*, Graduate Texts in Mathematics, vol. 66, Springer, 1979, xi+164 pages.

[32] M. Wibmer, "Almost-simple affine difference algebraic groups", *Math. Z.* **299** (2021), no. 1-2, p. 473-526.

[33] ———, "Expansive dynamics on profinite groups", *Fundam. Math.* **256** (2022), no. 1, p. 77-112.

[34] ———, "Finiteness properties of affine difference algebraic groups", *Int. Math. Res. Not.* (2022), no. 1, p. 506-555.

[35] G. A. Willis, "The nub of an automorphism of a totally disconnected, locally compact group", *Ergodic Theory Dyn. Syst.* **34** (2014), no. 4, p. 1365-1394.

[36] ———, "The scale and tidy subgroups for endomorphisms of totally disconnected locally compact groups", *Math. Ann.* **361** (2015), no. 1-2, p. 403-442.

Manuscrit reçu le 11 août 2021,
révisé le 23 juin 2022,
accepté le 17 novembre 2022.

Michael WIBMER
Institute of Analysis and Number Theory
Graz University of Technology
Kopernikusgasse 24
8010 Graz (Austria)
https://sites.google.com/view/wibmer
wibmer@math.tugraz.at