

Affine Difference Algebraic Groups

Habilitationsschrift vorgelegt von

Dr. rer. nat. Michael Wibmer

aus Gaimberg, Österreich

Für Erik und Katarina

Contents

1	Difference algebra and difference algebraic geometry	10
1.1	Difference algebra	10
1.2	Difference algebraic geometry	15
1.3	Other approaches to difference algebraic geometry	21
2	Basic properties of difference algebraic groups	25
2.1	Difference algebraic groups: Definition and examples	25
2.2	Zariski closures of difference algebraic groups and the growth group	30
2.3	Finiteness theorems	35
2.4	The limit degree	38
2.5	Subgroups defined by ideal closures	41
3	Morphisms of difference algebraic groups	46
3.1	Representations of difference algebraic groups	46
3.2	Quotients	48
3.3	Injective and surjective morphisms	54
4	Components	59
4.1	Connected components	59
4.2	Difference connected components	67
5	Group theory	87
5.1	Sheaves	88
5.2	The isomorphism theorems	96
5.3	Jordan-Hölder theorem	97
6	Étale difference algebraic groups	106
6.1	Basic properties of σ -étale difference algebraic groups	106
6.2	Profinite σ -groups	108
6.3	Infinitesimal and finite difference algebraic groups	118
6.4	Babbitt's decomposition for σ -étale difference algebraic groups	128

Introduction

The central objects of study in this thesis are affine difference algebraic groups. Similar to the case of affine algebraic groups, these groups can all be realized as subgroups of some general linear group defined by algebraic difference equations. However, the defining equations here are not simply polynomials in the matrix entries but difference polynomials, i.e., the defining equations involve a difference operator σ which has to be interpreted as a ring endomorphism. For example, if G is the difference algebraic subgroup of GL_n defined by the algebraic difference equations $X\sigma(X)^T = \sigma(X)^T X = I_n$, where $\sigma: \mathbb{C} \rightarrow \mathbb{C}$ is the complex conjugation map, then $G(\mathbb{C})$ is the group of all complex unitary $n \times n$ -matrices. A more classical example of a difference field, i.e., a field equipped with an endomorphism, is $\mathbb{C}(x)$ with $\sigma(f(x)) = f(x+1)$ or $\sigma(f(x)) = f(qx)$ for $q \in \mathbb{C}^\times$. Difference algebra, i.e., the systematic study of solutions of difference equations from an algebraic point of view, grew out of the study of difference equations over $\mathbb{C}(x)$ in much the same way as algebraic geometry grew out of the study of polynomial equations over $\mathbb{Q}$ or $\mathbb{C}$.

Alternatively, affine difference algebraic groups may be described as affine group schemes with a certain additional structure (the difference structure). As schemes they are typically not of finite type, but they enjoy a certain finiteness property with respect to the difference structure; they are “of finite σ -type”. From an algebraic point of view, an affine difference algebraic group G over a difference field k corresponds to a Hopf algebra $k\{G\}$ over k together with a ring endomorphism $\sigma: k\{G\} \rightarrow k\{G\}$ that extends $\sigma: k \rightarrow k$. The structure maps of the Hopf algebra are required to commute with σ , and $k\{G\}$ is required to be finitely σ -generated over k , i.e., there exists a finite set $B \subset k\{G\}$ such that $B, \sigma(B), \sigma^2(B), \dots$ generates $k\{G\}$ as a k -algebra.

Difference algebraic groups are the discrete analog of differential algebraic groups, i.e., groups defined by algebraic differential equations. Differential algebraic groups have always played an important role in differential algebra (see, e.g., [Cas72], [Sit75], [Cas75], [Cas78], [Kol85], [Cas89], [Bui92], [Bui93]) and are an active area of research nowadays. See e.g., [Pil97], [KP00], [CS11], [MO11], [MO13], [Fre], [Min]. See also [Mal10] for a more geometric approach to differential algebraic groups and [Bui98] for an arithmetic analog of difference/differential algebraic groups.

Over the last decade, Galois theories where the Galois groups are differential algebraic groups ([Pil98], [Lan08], [CS07], [HS08]) have given a new impetus to the study of differential algebraic groups. The Galois theories in [CS07] and [HS08] are also known as parameterized Picard-Vessiot theories as they generalize the standard Picard-Vessiot theory ([Kol48], [vdPS03], [vdPS97]) of linear differential and difference equations to linear differential and difference equations depending on (continuous) parameters.

In contrast to the situation in differential algebra, difference algebraic groups have long played no role at all in difference algebra. The author can only speculate why. Maybe one reason is that the traditional definition of a difference variety, which involves a so-called

universal system of difference fields (see [Coh65, Chapter 4]), is not really suitable for studying groups. (For each difference field in the universal system one obtains a group structure but the difference variety itself does not carry a group structure.)

Around the turn of the century a considerable interest in the model theory of difference fields emerged. (See e.g., [Mac97], [CH99], [CHP02].) Groups definable in ACFA, the model companion of the theory of difference fields, played a crucial role in remarkable applications of model theory to number theory, especially regarding the Manin-Mumford conjecture. See [Hru01], [Bou02], [Cha01], [Cha97], [Sca05], [Sca06], [SV99], [KP07].

In [KP02] it is shown that every group definable in ACFA is, in a certain sense, close to being a definable (in the language of difference fields) subgroup of an algebraic group. Here we will show that every affine difference algebraic group is isomorphic to a difference closed subgroup of some general linear group. In [KP02] it is also shown that an affine difference algebraic group whose underlying difference variety is an affine space is isomorphic to a difference closed subgroup of a unipotent algebraic group. A Tannakian approach to affine difference algebraic groups has been introduced in [OWb]. (See also [Kam13].)

Recently, a Galois theory for linear differential equations depending on a discrete parameter has been developed in [DVHW14]. In [OWa] a similar Galois theory has been developed for linear difference equations depending on a discrete parameter. The Galois groups in these Galois theories are affine difference algebraic groups and they measure the difference algebraic relations among the solutions. For example, the difference algebraic relation $xJ_{\alpha+2}(x) - 2(\alpha+1)J_{\alpha+1}(x) + xJ_{\alpha}(x) = 0$ satisfied by the Bessel function $J_{\alpha}(x)$, which solves Bessel's differential equation $x^2\delta^2(y) + x\delta(y) + (x - \alpha^2)y = 0$, is witnessed by the associated Galois group.

As illustrated in [DVHW] and [OWa], these Galois theories make it possible to use structure results about affine difference algebraic groups to analyze and classify the possible difference algebraic relations among the solutions of certain linear differential and difference equations. In this respect the understanding of the Zariski dense difference closed subgroups of a given affine algebraic group is highly relevant. For example, some understanding of the Zariski dense difference closed subgroups of SL_2 , originating from [CHP02], is a key ingredient in proving that any two linearly independent solution of the Airy equation are difference algebraically independent. More precisely ([DVHW, Corollary 6.10]), if $A(x)$ and $B(x)$ are $\mathbb{C}$ -linearly independent solutions of Airy's equation $\delta^2(y) - xy = 0$, then $A(x), B(x), A'(x), A(x+1), B(x+1), A'(x+1), A(x+2), \dots$ are algebraically independent over $\mathbb{C}(x)$.

While the parameterized Picard-Vessiot theory for continuous parameters could draw on a well-established comprehensive theory of differential algebraic groups, the situation for discrete parameters is adverse. But clearly, a well-developed theory of affine difference algebraic groups is indispensable for the parameterized Picard-Vessiot theory with discrete parameters to flourish. Obviously one could not get very far without having fundamental results such as the analogs of the isomorphism theorems for groups at one's disposal. Even though the validity of the isomorphism theorems for affine difference algebraic may not come as a surprise, the proof is far from being obvious. Indeed, even the existence of the quotient of an affine difference algebraic group modulo a normal difference closed subgroup is a highly non-trivial question. A positive answer requires proving that every k - σ -Hopf subalgebra of a finitely σ -generated k - σ -Hopf algebra is finitely σ -generated.

While it will for sure be a long way to lift the theory of difference algebraic groups to a level comparable to the contemporary theory of differential algebraic groups, it is the hope of the author that this thesis may serve as a first major step in this direction.

It is well recognized that a functorial-schematic approach to algebraic groups has its benefits. (See [Wat79], [DG70], [Jan87], [Mil12], [Gro70].) Here we adopt a similar approach for difference algebraic groups. For example, the general linear group GL_n over a difference field k , considered as a difference algebraic group, is the functor that assigns $\mathrm{GL}_n(R)$ to every k - σ -algebra R , that is, R is a k -algebra equipped with an endomorphism $\sigma: R \rightarrow R$ that extends $\sigma: k \rightarrow k$. In the model theoretic approach to difference equations as well as in classical difference algebra ([Coh65], [Lev08]) one is primarily interested in solutions in difference field extensions of k , i.e., R is required to be a field. An affine difference algebraic group is a group object in the category of affine difference varieties. The definition of an affine difference variety used in this thesis is more general than the classical definition of a difference variety (as in [Coh65] and [Lev08]). Our definition is equivalent to what is called a $\underline{D}$ -subscheme of affine space in [MS11] for a suitable choice of $\underline{D}$. Also, our notion of affine difference algebraic group is equivalent to what is called a linear $\mathfrak{M}$ -group in [Kam13] for a suitable choice of $\mathfrak{M}$. The classical difference varieties studied in [Coh65] and [Lev08] correspond precisely to the affine difference varieties that can be recovered from their points over difference fields. Thus, the relation between our affine difference varieties and the classical difference varieties is similar to the relation between affine schemes of finite type and affine varieties. The affine difference varieties that can be recovered from their points over difference fields are those whose defining ideal is perfect, therefore, we call them perfectly σ -reduced. Affine difference algebraic groups that are not perfectly σ -reduced occur quite naturally and frequently as Galois groups of linear differential or difference equations depending on a discrete parameter. There are several examples (Example 4.1.2) of difference algebraic groups G with the property that $G(K)$ is the trivial group for every difference field extension K of k .

In difference algebraic geometry there is a “zoo” of elements playing a role analogous to nilpotent elements in algebraic geometry. They roughly correspond to the following assertions valid for elements in a difference field extension of k but not necessarily valid for elements in a k - σ -algebra:

- $a^n = 0$ implies $a = 0$.
- $\sigma^n(a) = 0$ implies $a = 0$.
- $ab = 0$ implies $a\sigma(b) = 0$.
- $a\sigma(a) = 0$ implies $a = 0$.

In this sense we obtain four difference closed subgroups of an affine difference algebraic group that play a role analogous to the maximal reduced subgroup of an affine algebraic group. The theory of affine algebraic groups runs more smoothly if one allows nilpotent elements in the structure sheaf, and non-reduced algebraic groups play an important role in the representation theory of affine algebraic groups in positive characteristic. The situation for affine difference algebraic groups is similar. The category of affine difference algebraic groups is much better behaved than the category of perfectly σ -reduced affine difference algebraic groups. This, for example, becomes apparent when dealing with extensions of the base field or when dealing with quotients and the analogs of the isomorphism theorems for groups. For example, the morphism of affine difference algebraic groups $\phi: \mathrm{GL}_n \rightarrow \mathrm{GL}_n$ determined by $\phi((g_{ij})) = (\sigma(g_{ij}))$ for $(g_{ij}) \in \mathrm{GL}_n(R)$ and R a k - σ -algebra has a non-trivial kernel, even though $\phi: \mathrm{GL}_n(K) \rightarrow \mathrm{GL}_n(K)$ is injective for every difference field extension of k . In particular, if k is a model of ACFA, then $\phi: \mathrm{GL}_n(k) \rightarrow \mathrm{GL}_n(k)$ is

bijjective but ϕ is not an isomorphism of difference algebraic groups. Here we will show that (with the appropriate conception of injective and surjective) a morphism of affine difference algebraic groups is an isomorphism if and only if it is injective and surjective.

Let us now describe the contents of the thesis in more detail. In the first chapter we recall the basic definitions of difference algebra and we present our formalism of difference algebraic geometry. We also compare our approach to other possible approaches to difference algebraic geometry. Other than some facts about quotients or examples of difference algebraic groups that were already used in the above described Galois theory ([DVHW14],[DVHW],[OWa]) all the results presented after Chapter 1 are new.

The second chapter is the technical heart of this thesis. After defining affine difference algebraic groups and presenting some examples, we prove two important finiteness theorems and we introduce three numerical invariants for affine difference algebraic groups: The σ -dimension, the order and the limit degree. For clarity we state here the fundamental finiteness theorems in the language of Hopf algebras: Let $k\{G\}$ be a k - σ -Hopf algebra that is finitely σ -generated over k and let $\mathbb{I}(H) \subset k\{G\}$ be a σ -Hopf ideal, i.e., a Hopf ideal such that $\sigma(\mathbb{I}(H)) \subset \mathbb{I}(H)$. Then $\mathbb{I}(H)$ is finitely σ -generated, i.e., there exists a finite set $B \subset \mathbb{I}(H)$ such that $B, \sigma(B), \sigma^2(B), \dots$ generates $\mathbb{I}(H)$ as an ideal. This result can be seen as a strengthening (for k - σ -Hopf algebras) of the Ritt-Raudenbush basis theorem in difference algebra. The classical Ritt-Raudenbush basis theorem does not apply in our setting as it only applies to perfect difference ideals. This finiteness result turns out to be extremely useful and is used repeatedly in the subsequent developments. For example, it is used in the proof of the dimension theorem which is also proved in the second chapter. The second finiteness theorem asserts that every k - σ -Hopf subalgebra of $k\{G\}$ is finitely σ -generated.

The definition of the three numerical invariants is intimately connected with the proof of the first finiteness theorem. The crucial connecting result is the existence of the growth group. The growth group is an affine algebraic group that can naturally be associated to any embedding of an affine difference algebraic group into an affine algebraic group (as a difference closed subgroup). We also establish the existence of a Kolchin (or dimension) polynomial for affine difference algebraic groups.

The definition of the limit degree for difference algebraic groups is analogous to the definition of an important invariant of extensions of difference fields also called the limit degree ([Lev08, Section 4.3]). So-called algebraic σ -groups have been introduced and studied in [KP07]. We show that the category of affine algebraic σ -groups is equivalent to the category of affine difference algebraic groups of difference dimension zero and limit degree one.

In the last section of Chapter 2 we deal with the ring elements playing a role analogous to nilpotent elements in algebraic geometry. In particular, we introduce four difference closed subgroups playing a role analogous to the maximal reduced subgroup for algebraic groups.

In the third chapter we study morphisms and representations of affine difference algebraic groups. We prove an analog of a theorem of Chevalley: Every difference closed subgroup of an affine difference algebraic group G is the stabilizer of a line in a suitable representation of G . We also show that the category of representations of a torus (considered as a difference algebraic group) is semi-simple. This is in sharp contrast to what happens in the theory of linear differential algebraic groups. The category of representations of a linear differential algebraic group is semi-simple only for linear differential algebraic groups that are the constant points of a reductive algebraic group ([MO11]).

In the second section of Chapter 2 we establish the existence of quotients and show that the σ -dimension, the order and the limit degree behave on quotients in the expectable way. Then we characterize injective and surjective morphisms and show that every morphism of affine difference algebraic groups factors uniquely as the composition of a surjective morphism followed by an injective morphism.

In Chapter 4 we study the components of affine difference algebraic groups. There are two different types of components: The connected components with respect to the usual Zariski topology and the σ -connected components, i.e., the connected components with respect to a topology that also takes into account the action of the endomorphism σ . An affine difference algebraic group typically has infinitely many components. However, we establish two further finiteness theorems: Firstly we show that a finitely σ -generated k - σ -Hopf algebra has only finitely many minimal prime difference ideals. This proves a special case of a reformulation of a question raised by E. Hrushovski. Secondly, we show that an affine difference algebraic group only has finitely many σ -connected components. We also introduce the identity component and the σ -identity component of an affine difference algebraic group via a study of the associated quotient groups.

In Chapter 5 we study group theoretic properties of affine difference algebraic groups. Sheaves ([DG70, Chapter III]) are a useful tool for dealing with quotients of algebraic groups. We adapt the sheaf theoretic approach to difference algebraic groups and then use it to prove the analogs of the isomorphism theorems for groups. The chapter culminates in an analog of the Jordan-Hölder decomposition theorem. Chapter 5 concludes the study of general properties of affine difference algebraic groups.

In Chapter 6 we study some special classes of affine difference algebraic groups. Our main interest is in so-called σ -étale difference algebraic groups. These are precisely those affine difference algebraic group whose connected component is trivial. In general, the quotient of an affine difference algebraic group by the identity component is σ -étale. The category of étale algebraic groups is equivalent to the category of finite groups with a continuous action of the absolute Galois group of the base field. We prove a difference analog of this result: We show that the category of σ -étale difference algebraic groups is equivalent to a certain category of profinite groups equipped with an endomorphism σ and an action of the absolute Galois group that intertwines with σ . We also study certain analogs of infinitesimal algebraic groups and prove a structure theorem for affine difference algebraic groups G , with the property that $k\{G\}$ is a finite dimensional k -vector space. The final and main result of Chapter 6 is a decomposition theorem for σ -étale difference algebraic groups. This result is loosely analogous to Babbitt's decomposition theorem for algebraic extensions of difference fields ([Lev08, Theorem 5.4.13, p. 336]). The proof of Babbitt's decomposition theorem for difference algebraic groups uses a difference analog of Frobenius kernels and many results and concepts of the previous sections.

I am deeply thankful to Prof. Julia Hartmann for her constant support during my years in Aachen. I also would like to thank Prof. Wilhelm Plesken and Prof. Sebastian Walcher for friendly advice and for supporting my habilitation project.

This thesis greatly profited from stimulating mathematical discussions with several people. I would like to mention my colleagues at "Lehrstuhl für Mathematik (Algebra)" Stefan Ernst, Annette Maier, Daniel Rettstadt and my collaborators Lucia Di Vizio, Charlotte Hardouin, Florian Heiderich, Andreas Maurischat, Alexey Ovchinnikov and Ivan Tomašić. Special thanks go to Annette Maier for her helpful comments on an earlier version of this manuscript and to Ivan Tomašić for explaining me the different notions of étaleness in difference algebra.

Conventions

All rings are assumed to be commutative and unital. The natural numbers contain zero, i.e., $\mathbb{N} = \{0, 1, 2, \dots\}$. The expression $\sigma^0(f)$ is understood to be f and σ^0 is understood to be the identity map. By “algebraic group” we mean an affine group scheme of finite type over a field. In particular, in positive characteristic, an algebraic group need not be reduced.

We always work over a fixed difference ring k , i.e., we consider difference equations with coefficients in k . For most of the time we assume that k is a difference field. More precisely, starting from Section 2.2 we always assume that k is a difference field. The only exception to this rule is the beginning of Subsection 6.3.4.

If X is some object (or morphism) over k and $\sigma: k \rightarrow k$ the endomorphism of k defining the difference structure, then $\sigma^i X$ denotes the object over k obtained from X by base extension via $\sigma^i: k \rightarrow k$ for $i \in \mathbb{N}$.

Chapter 1

Difference algebra and difference algebraic geometry

In the beginning of this chapter we recall some basic definitions and constructions from difference algebra. Then we present the language of difference algebraic geometry that will be used throughout the text. Our approach to difference algebraic geometry is novel and generalizes the classical approach as in the standard textbooks [Lev08] and [Coh65]. In a rudimentary form it has already been used in the σ -Galois theory of linear differential and difference equations. See [DVHW14], [DVHW] and [OWa].

It is well recognized that a functorial-schematic approach to algebraic groups has its benefits. (See [Wat79], [DG70], [Jan87], [Mil12], [Gro70].) Our approach to difference algebraic geometry is a natural adaptation of the approach of the above references from algebra to difference algebra, i.e., from algebraic equations to difference algebraic equations. In the last section of this chapter we compare our approach to other possible approaches to difference algebraic geometry.

1.1 Difference algebra

1.1.1 Basic definitions

Standard references for difference algebra are [Lev08] and [Coh65]. The reader new to difference algebra may also find the lecture notes [Wib13] helpful.

Definition 1.1.1. A difference ring (or σ -ring for short) is a ring¹ R together with a ring endomorphism $\sigma: R \rightarrow R$.

It is customary to use the same symbol σ for diverse endomorphisms (and this should not cause confusion). A *morphism of σ -rings* R and S is a morphism $\psi: R \rightarrow S$ of rings such that

$$\begin{array}{ccc} R & \xrightarrow{\psi} & S \\ \sigma \downarrow & & \downarrow \sigma \\ R & \xrightarrow{\psi} & S \end{array}$$

commutes. Note that in contrast to [Lev08] and [Coh65] we do not require $\sigma: R \rightarrow R$ to be injective in the definition of a difference ring. This added generality allows for a greater

¹Recall that by convention all our rings are commutative.

flexibility in certain constructions but is also required to deal with certain phenomena that occur quite naturally. For example, the action of σ on the coordinate ring of the σ -Galois group a linear differential equation may not be injective ([DVHW14, Example 2.11]). Also, our study of σ -infinitesimal σ -algebraic groups in Section 6.3 would not be meaningful without the possibility to consider non-injective endomorphisms.

If R and S are σ -rings such that R is a subring of S and the inclusion map is a morphism of σ -rings, we say that R is a σ -subring of S . A subset F of a σ -ring R is called σ -stable if $\sigma(F) \subset F$.

A *difference field* (or σ -field for short) is a difference ring whose underlying ring is a field. If K and L are σ -fields such that K is a σ -subring of L , we also say that L is a σ -field extension of K , or that $L|K$ is an *extension of σ -fields*, or that K is a σ -subfield of L .

Let $L|K$ be an extension of σ -fields and $F \subset L$ a subset. The smallest σ -subfield of L that contains K and F is denoted by

$$K\langle F \rangle.$$

As a field extension of K the σ -field $K\langle F \rangle$ is generated by $F, \sigma(F), \sigma^2(F), \dots$. We call $K\langle F \rangle$ the σ -field σ -generated by F over K . If $L = K\langle F \rangle$ for a finite subset F of L we say that L is *finitely σ -generated as a σ -field extension of K* .

Let k be a difference ring. A morphism of difference rings $k \rightarrow R$ is also called a k - σ -algebra. A *morphism of k - σ -algebras* is a morphism of k -algebras that is also a morphism of σ -rings. The category of k - σ -algebras is denoted by

$$k\text{-}\sigma\text{-Alg}.$$

If R and S are k - σ -algebras $R \otimes_k S$ is naturally a σ -ring by $\sigma(r \otimes s) = \sigma(r) \otimes \sigma(s)$ for $r \in R$ and $s \in S$. Indeed, $R \otimes_k S$ is the coproduct of R and S in the category of k - σ -algebras.

A k - σ -subalgebra of a k - σ -algebra R is a k -subalgebra of R that is also σ -subring of R . For a subset $F \subset R$, the smallest k - σ -subalgebra of R that contains F is denoted by

$$k\{F\}.$$

It is called the k - σ -subalgebra of R σ -generated by F (over k). As a k -algebra, $k\{F\}$ is generated by all elements of the form $\sigma^i(f)$ with $i \in \mathbb{N}$ and $f \in F$. A k - σ -algebra R is called *finitely σ -generated* (over k) if there exists a finite set $F \subset R$ such that $R = k\{F\}$.

Basic examples of k - σ -algebras are given by rings of difference polynomials. The *ring of σ -polynomials over a σ -ring k in the σ -variables $y_1, \dots, y_n$* is the polynomial ring

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

in the variables $y_1, \dots, y_n, \sigma(y_1), \dots, \sigma(y_n), \dots$ over k . It is naturally a k - σ -algebra with $\sigma: k\{y\} \rightarrow k\{y\}$ extended from $\sigma: k \rightarrow k$ as suggested by the naming of the variables. If R is a k - σ -algebra, $f \in k\{y\}$ a σ -polynomial and $x = (x_1, \dots, x_n) \in R^n$, the element $f(x) \in R$ is obtained by substituting $\sigma^i(x_j)$ for $\sigma^i(y_j)$. If $f(x) = 0$, we say that x is a *solution of f* .

For example, the fact that the gamma function Γ satisfies the functional equation $\Gamma(z+1) = z\Gamma(z)$ may be expressed by saying that Γ is a solution of the σ -polynomial $\sigma(y_1) - zy_1$. Here we may, for example, choose $k = \mathbb{C}(z)$ and R as the field of meromorphic

functions in the variable z , both equipped with the difference operator σ determined by $\sigma(f(z)) = f(z+1)$.

An ideal $\mathfrak{a}$ of a σ -ring R is called a *difference ideal* (or σ -ideal for short) if $\sigma(\mathfrak{a}) \subset \mathfrak{a}$. In this case $R/\mathfrak{a}$ naturally inherits the structure of a σ -ring such that the canonical map $R \rightarrow R/\mathfrak{a}$ is a morphism of σ -rings.

Definition 1.1.2. Let $\mathfrak{a}$ be a σ -ideal in a σ -ring R . Then $\mathfrak{a}$ is called

- reflexive if $\sigma^{-1}(\mathfrak{a}) = \mathfrak{a}$, i.e., $\sigma(f) \in \mathfrak{a}$ implies $f \in \mathfrak{a}$.
- perfect if $\sigma^{\alpha_1}(f) \cdots \sigma^{\alpha_n}(f) \in \mathfrak{a}$ implies $f \in \mathfrak{a}$ for $\alpha_1, \dots, \alpha_n \geq 0$
- σ -prime if $\mathfrak{a}$ is reflexive and a prime ideal.

One can show ([Wib13, Lemma 1.2.5]) that $\mathfrak{a}$ is perfect if and only if $f\sigma(f) \in \mathfrak{a}$ implies $f \in \mathfrak{a}$.

Let R be a σ -ring and $F \subset R$ a subset. The smallest σ -ideal of R containing F is denoted by

$$[F]$$

and called the σ -ideal σ -generated by F . As an ideal $[F]$ is generated by all elements of R that are of the form $\sigma^i(f)$ with $i \in \mathbb{N}$ and $f \in F$.

A σ -ideal $\mathfrak{a}$ of a σ -ring R is called *finitely σ -generated* if $\mathfrak{a} = [F]$ for a finite subset $F \subset \mathfrak{a}$.

Definition 1.1.3. Let R be a σ -ring R . Then R is called

- σ -reduced if $\sigma: R \rightarrow R$ is injective.
- inversive if $\sigma: R \rightarrow R$ is an automorphism.
- perfectly σ -reduced if the zero ideal of R is perfect, i.e., if $f\sigma(f) = 0$ implies $f = 0$ for $f \in R$.
- a σ -domain if R is an integral domain and σ -reduced.

If R is a σ -ring, then there exists an inversive σ -ring

$$R^*$$

together with a morphism of σ -rings $R \rightarrow R^*$ which is universal among such maps, i.e., for any inversive σ -ring R' and morphism of σ -rings $R \rightarrow R'$ there exists a unique morphism $R \rightarrow R'$ such that

$$\begin{array}{ccc} R & \xrightarrow{\quad} & R^* \\ & \searrow & \swarrow \text{dotted} \\ & R' & \end{array}$$

commutes (see [Wib13, Prop. 1.1.18]). The σ -ring R^* is unique up to a unique isomorphism and is called the *inversive closure* of R . If R is σ -reduced the map $R \rightarrow R^*$ is injective and we can identify R with a σ -subring of R^* (cf. [Wib13, Lemma 1.1.23] and [Lev08, Prop. 2.1.7]). The inversive closure of a σ -field is a σ -field ([Lev08, Prop. 2.1.7]).

For later use we record some simple and well-known facts on extending σ .

Lemma 1.1.4. *Let k be a σ -field and f a separable polynomial with coefficients in k . Then the polynomial ${}^\sigma f$ obtained from f by applying σ to the coefficients is also separable.*

Proof. If 1 lies in the ideal generated by f and its formal derivative, applying σ to the coefficients shows that 1 also lies in the ideal generated by ${}^\sigma f$ and its formal derivative. $\square$

Lemma 1.1.5. *Let k be a σ -field. Then there exists an extension of $\sigma: k \rightarrow k$ to an endomorphism $\sigma: \bar{k} \rightarrow \bar{k}$ on the algebraic closure $\bar{k}$ of k . The separable algebraic closure $k_s \subset \bar{k}$ is stable under σ . In particular, $\sigma: k \rightarrow k$ can be extended to an endomorphism $\sigma: k_s \rightarrow k_s$.*

Proof. The set of all pairs (K, σ) , where K is an intermediate field of $\bar{k}|k$ and $\sigma: K \rightarrow \bar{k}$ an extension of $\sigma: k \rightarrow k \subset \bar{k}$ carries a natural partial order: $(K, \sigma) \leq (K', \sigma')$ if $K \subset K'$ and the restriction of σ' to K is σ . By Zorn's lemma there exists a maximal element (K, σ) . Suppose $K \subsetneq \bar{k}$. Then we may pick $a \in \bar{k} \setminus K$. We can extend $\sigma: K \rightarrow \bar{k}$ to $\sigma: K(a) \rightarrow \bar{k}$ by sending a to a root of the polynomial obtained from the minimal polynomial of a over K by applying σ to the coefficients. This contradicts the maximality of K . So $K = \bar{k}$.

It remains to show that the separable algebraic closure is stable under σ . Let $a \in k_s$ and let f denote the minimal polynomial of a over k . Because ${}^\sigma f(\sigma(a)) = 0$ and ${}^\sigma f$ is a separable polynomial by Lemma 1.1.4, we see that $\sigma(a) \in k_s$. $\square$

Lemma 1.1.6. *Let k be a σ -field. Then there exists an inversive algebraically closed σ -field extension K of k . Indeed, we may take K as the inversive closure of the algebraic closure of k .*

Proof. Let $\bar{k}$ denote the algebraic closure of k . As seen in Lemma 1.1.5 we can extend σ from k to $\bar{k}$. By Proposition 2.1.9 (i) in [Lev08] the inversive closure K of $\bar{k}$ is algebraically closed. $\square$

1.1.2 Difference separable difference algebras

The notion of a σ -separable σ -algebra will turn out to be crucial for defining the σ -identity component of a σ -algebraic group in Section 4.2. This notion does not appear in the standard textbooks [Coh65] and [Lev08], but has turned out to be useful lately. See [Hru04, Section 5.1.], [Wib10, Section 1.5], [DVHW14, Section 4] and [Tom]. In this subsection we collect basic properties of σ -separable σ -algebra that will be needed later.

Definition 1.1.7. *Let k be a σ -field. A k - σ -algebra R is called σ -separable (over k) if $R \otimes_k K$ is σ -reduced for every σ -field extension $K|k$.*

Note that Definition 1.1.7 generalizes the notion of a separable algebra. (See Corollary 1.1.9 for a precise mathematical statement.)

Proposition 1.1.8. *Let k be a σ -field. The following conditions on a k - σ -algebra R are equivalent:*

- (i) R is σ -separable over k .
- (ii) $R \otimes_k K$ is σ -reduced, where $K = k^*$ denotes the inversive closure of k .
- (iii) $R \otimes_k K$ is σ -reduced for some inversive σ -field extension K of k .

- (iv) If $f_1, \dots, f_n \in R$ are k -linearly independent, then also $\sigma(f_1), \dots, \sigma(f_n) \in R$ are k -linearly independent.
- (v) $R \otimes_k S$ is σ -reduced for every σ -reduced k - σ -algebra S .

Proof. Cf. Proposition 1.5.2 in [Wib10] and Theorem 2, Chapter V, §15, No. 4 in [Bou90]. The implications (i) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (iii) are trivial. Let us show that (iii) implies (iv). Assume $\lambda_1 \sigma(f_1) + \dots + \lambda_n \sigma(f_n) = 0$ with $\lambda_1, \dots, \lambda_n \in k$. Because K is inversive, there exist $\mu_1, \dots, \mu_n \in K$ with $\sigma(\mu_i) = \lambda_i$ for $i = 1, \dots, n$. Then

$$\sigma\left(\sum f_i \otimes \mu_i\right) = \sum \sigma(f_i) \otimes \lambda_i = 0 \in R \otimes_k K.$$

Because $R \otimes_k K$ is σ -reduced and the f_i 's are k -linearly independent, this implies that $\mu_i = 0$ for $i = 1, \dots, n$. Thus $\lambda_i = \sigma(\mu_i) = 0$ for $i = 1, \dots, n$.

Next we will show that (iv) implies (v). Assume that $f \in R \otimes_k S$ with $\sigma(f) = 0$. Let (f_i) be a k -basis of R . Then $f = \sum f_i \otimes s_i$ with $s_i \in S$ and $\sum \sigma(f_i) \otimes \sigma(s_i) = \sigma(f) = 0$. Because the $\sigma(f_i)$'s are k -linearly independent we have $\sigma(s_i) = 0$ for all i . But as S is σ -reduced this implies that $s_i = 0$ and therefore $f = 0$.

Finally the implication (v) $\Rightarrow$ (i) is trivial. $\square$

Corollary 1.1.9. *Let k be field of positive characteristic p and let q be a power of p . Let R be a k -algebra and consider k and R as difference rings via the Frobenius endomorphism, i.e., $\sigma(f) = f^q$ for $f \in R$. Then R is σ -separable over k if and only if R is a separable k -algebra.*

Proof. Assume that R is σ -separable over k and let K be a field extension of k . We have to show that $R \otimes_k K$ is reduced. But if we consider K as a σ -field via $\sigma(f) = f^q$, then, by assumption, σ is injective on $R \otimes_k K$. Thus $R \otimes_k K$ is reduced.

Conversely, assume that R is a separable k -algebra. By [Bou90, Theorem 2, Chapter V, §15, No. 4, A.V.123] the elements $f_1^p, \dots, f_n^p$ are k -linearly independent if $f_1, \dots, f_n \in R$ are k -linearly independent. Therefore $\sigma(f_1), \dots, \sigma(f_n)$ are k -linearly independent and it follows from Proposition 1.1.8 that R is σ -separable over k . $\square$

Corollary 1.1.10. *If R and S are σ -separable k - σ -algebras, then also $R \otimes_k S$ is a σ -separable k - σ -algebra.*

Proof. Let K be a σ -field extension of k . Then $S \otimes_k K$ is σ -reduced because S is σ -separable. Therefore $(R \otimes_k S) \otimes_k K = R \otimes_k (S \otimes_k K)$ is σ -reduced by Proposition 1.1.8. $\square$

Corollary 1.1.11. *Let R be a k - σ -algebra and K a σ -field extension of k . Then R is σ -separable over k if and only if $R \otimes_k K$ is σ -separable over K .*

Proof. Let us first assume that R is σ -separable over k . Let L be a σ -field extension of K . Then $(R \otimes_k K)_K L = R \otimes_k L$ is σ -reduced. Thus $R \otimes_k K$ is σ -separable over K .

Conversely, if $R \otimes_k K$ is σ -separable over K , it follows that $(R \otimes_k K) \otimes_K K^* = R \otimes_k K^*$ is σ -reduced. Thus R is σ -separable over k by Proposition 1.1.8. $\square$

Corollary 1.1.12. *Let $K|k$ be an extension of σ -fields. If k is inversive, then K is σ -separable over k .*

Proof. By Proposition 1.1.8 it suffices to note that a σ -field is σ -reduced. $\square$

1.2 Difference algebraic geometry

In this section k is a difference ring.

In this section we present some basic notions from difference algebraic geometry, e.g., the notion of a difference variety. These definitions and results will then be used in the following sections in the study of difference algebraic groups.

In this section k is a difference ring and we will consider difference equations over k . We are mainly interested in the case that k is a difference field. However, for technical reasons (see e.g. Definition 2.1.5) it is beneficial to have the basic definitions also available over rings.

1.2.1 Difference varieties

Essentially, a difference variety (over k) is the set of solutions of a system of algebraic difference equations (over k). Of course, we need to specify more precisely where we are looking for the solutions.

Let R be a k - σ -algebra and $F \subset k\{y\} = k\{y_1, \dots, y_n\}$ a set of σ -polynomials over k . Then we may consider the R -rational solutions of F , that is

$$\mathbb{V}_R(F) = \{x \in R^n \mid f(x) = 0 \text{ for all } f \in F\}.$$

Note that $R \mapsto \mathbb{V}_R(F)$ is naturally a functor from $k\text{-}\sigma\text{-Alg}$ to **Sets**, the category of sets. We denote this functor by $\mathbb{V}(F)$.

Definition 1.2.1. *Let k be a σ -ring. A difference variety (or σ -variety for short) over k is a functor from $k\text{-}\sigma\text{-Alg}$ to **Sets**, that is of the form $\mathbb{V}(F)$, for some $n \geq 1$ and $F \subset k\{y_1, \dots, y_n\}$. A morphism of σ -varieties is a morphism of functors.*

The above definition (in case k is a σ -field) does not agree with the traditional definition of a difference variety as in [Coh65] and [Lev08], since traditionally one is only interested in solutions in σ -field extensions of k . The relation between Definition 1.2.1 and Definition 2.6.1 in [Lev08] is analogous to the relation between the definition of an affine scheme of finite type over a ring and the notion of an affine variety. The relation between our approach and other approaches to difference algebraic geometry is discussed in more detail in Section 1.3.

It may seem more accurate to add the word “affine” into Definition 1.2.1. However, to avoid endless iterations of the word “affine” we have chosen not to do so.

By definition, a morphism $\phi: X \rightarrow Y$ of σ -varieties consists of maps $\phi_R: X(R) \rightarrow Y(R)$ for any k - σ -algebra R , compatible with morphisms of k - σ -algebras. For convenience, we will sometimes drop the R in ϕ_R . In particular, if $x \in X(R)$, we may write $\phi(x)$ for $\phi_R(x) \in Y(R)$.

Let $F, G \subset k\{y\}$ and $X = \mathbb{V}(F)$, $Y = \mathbb{V}(G)$. If $F \subset G$ then $Y(R) \subset X(R)$ for every k - σ -algebra R and Y is a subfunctor of X . We say that Y is a σ -closed σ -subvariety of X and write $Y \subset X$.

Let $X = \mathbb{V}(F)$, $F \subset k\{y\} = k\{y_1, \dots, y_n\}$ be a σ -variety. Then

$$\mathbb{I}(X) = \{f \in k\{y\} \mid f(x) = 0 \text{ for all } k\text{-}\sigma\text{-algebras } R \text{ and all } x \in X(R)\} \quad (1.1)$$

is a σ -ideal of $k\{y\}$. The k - σ -algebra

$$k\{X\} = k\{y\}/\mathbb{I}(X)$$

is called the *coordinate ring* of X . As we may choose $R = k\{y\}/[F]$ in (1.1), we see that $\mathbb{I}(X) = [F] \subset k\{y\}$.

Let R be a k - σ -algebra and let $\bar{y} = (\bar{y}_1, \dots, \bar{y}_n) \in k\{X\}^n$ denote the images of $y_1, \dots, y_n$ in $k\{X\}$. The bijection

$$\mathrm{Hom}(k\{X\}, R) \rightarrow X(R)$$

maps a morphism $\psi: k\{X\} \rightarrow R$ of k - σ -algebras to $\psi(\bar{y})$ is functorial in R . Thus the functor X is represented by $k\{X\}$. Conversely, since every finitely σ -generated k - σ -algebra can be written in the form $k\{y\}/[F]$, we see that a functor from k - σ -Alg to **Sets** that is representable by a finitely σ -generated k - σ -algebra is isomorphic (as a functor) to a σ -variety.

In the sequel we will allow ourselves the little abuse of notation to also call a functor isomorphic to a σ -variety a σ -variety. In particular, we will often identify X with the functor $\mathrm{Hom}(k\{X\}, -)$. Thus a functor X from k - σ -Alg to **Sets** is a σ -variety if and only if it is representable by a finitely σ -generated k - σ -algebra $k\{X\}$. It is then clear from the Yoneda lemma that:

Remark 1.2.2. *The category of σ -varieties over k is anti-equivalent to the category of finitely σ -generated k - σ -algebras.*

If $\phi: X \rightarrow Y$ is a morphism of σ -varieties over k , the dual morphism of k - σ -algebras is denoted by

$$\phi^*: k\{Y\} \rightarrow k\{X\}.$$

As the tensor product is the coproduct in the category of k - σ -algebras it follows that:

Remark 1.2.3. *The category of σ -varieties has products. Indeed, if X and Y are σ -varieties over k , then $k\{X \times Y\} = k\{X\} \otimes_k k\{Y\}$. Moreover, there is a terminal object, namely, the functor represented by the k - σ -algebra k .*

In other words, the functor $R \rightsquigarrow (X \times Y)(R) = X(R) \times Y(R)$ is represented by $k\{X\} \otimes_k k\{Y\}$.

Definition 1.2.4. *A σ -variety X is called*

- *σ -reduced if $k\{X\}$ is σ -reduced.*
- *perfectly σ -reduced if $k\{X\}$ is perfectly σ -reduced.*
- *integral if $k\{X\}$ is an integral domain*
- *σ -integral if $k\{X\}$ is a σ -domain.*

For a k - σ -algebra R let

$$R^\sharp$$

denote the k -algebra obtained from R by forgetting σ .

Similarly, by forgetting σ , a σ -variety X over k gives rise to a scheme

$$X^\sharp$$

over k (or more precisely over $k^\sharp$). That is, $X^\sharp = \mathrm{Spec}(k\{X\})$ (or more precisely $X^\sharp = \mathrm{Spec}(k\{X\}^\sharp)$). Alternatively, $X^\sharp = \mathrm{Hom}(k\{X\}^\sharp, -)$.

1.2.2 Difference subvarieties and morphisms of difference varieties

Let Y be a σ -variety and $f \in k\{Y\}$. Then, for any k - σ -algebra R , we have a well-defined map $f: Y(R) \rightarrow R$ given by evaluating a representative of f in $k\{y_1, \dots, y_n\}$ at an element of $Y(R) \subset R^n$. In a coordinate free manner $f: Y(R) \rightarrow R$ can be described as the map that sends $\psi \in Y(R) = \text{Hom}(k\{Y\}, R)$ to $\psi(f) \in R$.

Let X be a σ -closed σ -subvariety of Y . Then

$$\mathbb{I}(X) = \{f \in k\{Y\} \mid f(x) = 0 \text{ for all } k\text{-}\sigma\text{-algebras } R \text{ and all } x \in X(R)\} \quad (1.2)$$

is a σ -ideal of $k\{Y\}$. We call $\mathbb{I}(X) \subset k\{Y\}$ the *defining ideal of X* (in $k\{Y\}$). This notation is consistent with (1.1) in the sense that $\mathbb{I}(X)$ as defined in (1.1) is the defining ideal of X in $k\{y\} = k\{y_1, \dots, y_n\}$. Moreover, $\mathbb{I}(X) \subset k\{Y\}$ agrees with the image in $k\{Y\} = k\{y\}/\mathbb{I}(Y)$ of the defining ideal of X in $k\{y\}$. So $k\{X\} = k\{Y\}/\mathbb{I}(X)$.

Conversely, let $F \subset k\{Y\}$. Then we can define a σ -closed σ -subvariety $\mathbb{V}(F)$ of Y by

$$\mathbb{V}(F)(R) = \{x \in Y(R) \mid f(x) = 0 \text{ for all } f \in F\}$$

for any k - σ -algebra R .

Lemma 1.2.5. *Let Y be a σ -variety. Then $\mathbb{I}$ and $\mathbb{V}$ are mutually inverse bijections between the set of σ -closed σ -subvarieties of Y and the set of σ -ideals of $k\{Y\}$.*

Proof. Let $\mathfrak{a}$ be a σ -ideal of $k\{Y\}$. Clearly $\mathfrak{a} \subset \mathbb{I}(\mathbb{V}(\mathfrak{a}))$. Since we may choose $R = k\{Y\}/\mathfrak{a}$ in (1.2) it follows that $\mathfrak{a} = \mathbb{I}(\mathbb{V}(\mathfrak{a}))$.

Let X be σ -closed σ -subvariety of Y . Then $X = \mathbb{V}(\mathfrak{a})$ for some σ -ideal $\mathfrak{a}$ of $k\{Y\}$. So $\mathbb{V}(\mathbb{I}(X)) = \mathbb{V}(\mathbb{I}(\mathbb{V}(\mathfrak{a}))) = \mathbb{V}(\mathfrak{a}) = X$. $\square$

Note that if X is a σ -closed σ -subvariety of Y and R a k - σ -algebra, then $X(R) \subset Y(R)$ corresponds to $\{\psi \in \text{Hom}(k\{Y\}, R) \mid \mathbb{I}(X) \subset \ker(\psi)\} \subset \text{Hom}(k\{Y\}, R)$.

If Y and Z are σ -closed σ -subvarieties of a σ -variety X , then we can define a subfunctor

$$Y \cap Z$$

of X by $R \rightsquigarrow Y(R) \cap Z(R)$. Then $Y \cap Z$ is a σ -closed σ -subvariety of X , indeed, $\mathbb{I}(Y \cap Z) \subset k\{X\}$ is the ideal generated by $\mathbb{I}(Y)$ and $\mathbb{I}(Z)$.

If $\phi: X \rightarrow Y$ is a morphism of σ -varieties and $Z \subset Y$ a σ -closed σ -subvariety, we can define a subfunctor

$$\phi^{-1}(Z)$$

of X by $R \rightsquigarrow \phi_R^{-1}(Z(R))$. If $Z = \mathbb{V}(\mathfrak{a})$ for a σ -ideal $\mathfrak{a} \subset k\{Y\}$, then

$$\begin{aligned} \phi^{-1}(Z)(R) &= \{\psi \in \text{Hom}(k\{X\}, R) \mid \mathfrak{a} \subset \ker(\psi\phi^*)\} \\ &= \{\psi \in \text{Hom}(k\{X\}, R) \mid \phi^*(\mathfrak{a}) \subset \ker(\psi)\} = \mathbb{V}(\phi^*(\mathfrak{a}))(R). \end{aligned}$$

Therefore $\phi^{-1}(Z) = \mathbb{V}(\phi^*(\mathfrak{a}))$ is a σ -closed σ -subvariety of X .

If $\phi: X \rightarrow Y$ is a morphism of σ -varieties, we can define a subfunctor

$$\text{Im}(\phi)$$

of Y by $\text{Im}(\phi)(R) = \phi_R(X(R))$ for any k - σ -algebra R . In general, $\text{Im}(\phi)$ will not be a σ -closed σ -subvariety of Y . It is therefore sometimes helpful to use the following notion, analogous to the scheme theoretic image ([Sta14, Tag 01R5]).

Lemma 1.2.6. *Let $\phi: X \rightarrow Y$ be a morphism of σ -varieties. There exists a unique σ -closed σ -subvariety*

$$\phi(X)$$

of Y with the following property. The morphism ϕ factors through $\phi(X)$ and if $Z \subset Y$ is a σ -closed σ -subvariety such that ϕ factors through Z then $\phi(X) \subset Z$.

Proof. Let $\mathfrak{a}$ denote the kernel of $\phi^*: k\{Y\} \rightarrow k\{X\}$ and set $\phi(X) = \mathbb{V}(\mathfrak{a}) \subset Y$. As ϕ^* factors through $k\{Y\} \rightarrow k\{\phi(X)\} = k\{Y\}/\mathfrak{a}$, we see that ϕ factors through $\phi(X)$. If ϕ factors through Z , i.e., ϕ^* factors through $k\{Y\} \rightarrow k\{Z\} = k\{Y\}/\mathbb{I}(Z)$, then clearly $\mathbb{I}(Z) \subset \mathfrak{a}$. So $\phi(X) \subset Z$. $\square$

Note that $\phi(X)$ is the σ -closure of $\text{Im}(\phi)$ in the sense that

$$\mathbb{I}(\phi(X)) = \{f \in k\{Y\} \mid f(a) = 0 \text{ for all } k\text{-}\sigma\text{-algebras } R \text{ and all } a \in \text{Im}(\phi)(R)\}.$$

If $\phi: X \rightarrow Y$ is a morphism of σ -varieties and $Z \subset X$ is a σ -closed σ -subvariety, then we will write $\phi(Z)$ for the σ -closed σ -subvariety $\phi|_Z(Z)$ of Y where $\phi|_Z: Z \rightarrow X \xrightarrow{\phi} Y$.

A morphism $\phi: X \rightarrow Y$ of σ -varieties is called a *σ -closed embedding* if ϕ induces an isomorphism between X and a σ -closed σ -subvariety of Y , i.e., $X \rightarrow \phi(X)$ is an isomorphism. We write

$$\phi: X \hookrightarrow Y$$

to express that ϕ is a σ -closed embedding. In analogy to a well known result in algebraic geometry we have:

Lemma 1.2.7. *A morphism $\phi: X \rightarrow Y$ of σ -varieties is a σ -closed embedding if and only if $\phi^*: k\{Y\} \rightarrow k\{X\}$ is surjective.*

Proof. Let $\mathfrak{a}$ denote the kernel of $\phi^*: k\{Y\} \rightarrow k\{X\}$. The dual map to $X \rightarrow \phi(X)$ is $k\{Y\}/\mathfrak{a} \rightarrow k\{X\}$. It is an isomorphism if and only if ϕ^* is surjective. $\square$

1.2.3 Base extension

In this subsection we explain how to extend the base σ -ring of a σ -variety. This is already one of the first points where our more general definition of σ -varieties pays off. For σ -varieties in the classical sense of [Lev08] and [Coh65] base extension is not at all well-behaved. For example, the system of algebraic difference equations

$$y^2 = 2, \sigma(y) = -y$$

clearly has a solution in a σ -field extension of $\mathbb{Q}$, where we consider $\mathbb{Q}$ as a σ -field via the identity map. However, if we consider the system over the σ -field $\mathbb{C}$, where again σ is the identity map on $\mathbb{C}$, then the system has no solution in a σ -field extension of $\mathbb{C}$. See Chapter 8, Section 6 in [Coh65] for more details on base extension for σ -varieties in the classical sense. Since we consider solutions in arbitrary k - σ -algebras and not just in σ -field extensions of k these problems disappear.

Let k be a σ -ring, k' a k - σ -algebra and X a σ -variety over k . We can define a functor

$$X_{k'}$$

from k' - σ -Alg to Sets by $X_{k'}(R') = X(R')$ for any k' - σ -algebra R' . Then $X_{k'}$ is a σ -variety over k' . Indeed,

$$k'\{X_{k'}\} = k\{X\} \otimes_k k'.$$

In terms of equations, this of course simply means that a system $F \subset k\{y\} = k\{y_1, \dots, y_n\}$ of algebraic difference equations over k is considered as a system $F \subset k'\{y\}$ of algebraic difference equations over k' . So if $k\{X\} = k\{y\}/[F]$ then $k'\{X_{k'}\} = k'\{y\}/[F]$.

1.2.4 Zariski closures

In this subsection we assume that k is a σ -field.

We explain how we consider a variety (over k) as a σ -variety over k . We also define the important Zariski closures of a σ -subvariety of a variety (cf. Sections A.4 and A.5 in [DVHW14] or Section 4.3 in [Hru04]).

Let $\mathcal{X}$ be a variety over k , where, for our purposes, a variety over k is an affine scheme of finite type over k . We can define a functor $[\sigma]_k \mathcal{X}$ from k - σ -Alg to Sets by

$$[\sigma]_k \mathcal{X}(R) = \mathcal{X}(R^\sharp)$$

for any k - σ -algebra R . Our next goal is to show that $[\sigma]_k \mathcal{X}$ is a σ -variety over k . That is, we need to construct $k\{[\sigma]_k \mathcal{X}\}$. By doing so, we also introduce some notation that will be useful later on.

Let A be a k -algebra. For every $i \geq 0$ let

$$\sigma^i A = A \otimes_k k,$$

where the tensor product is formed by using $\sigma^i: k \rightarrow k$ on the right hand side. We consider $\sigma^i A$ as k -algebra via the right factor. We set

$$A[i] = A \otimes_k \sigma^0 A \otimes_k \cdots \otimes_k \sigma^i A.$$

We have inclusions $A[i] \hookrightarrow A[i+1]$ of k -algebras and the limit, i.e, the union

$$[\sigma]_k A$$

of the $A[i]$'s is a k - σ -algebra, where for $(r_0 \otimes \lambda_0) \otimes \cdots \otimes (r_i \otimes \lambda_i) \in \sigma^0 A \otimes_k \cdots \otimes_k \sigma^i A = A[i]$ the map $\sigma: [\sigma]_k A \rightarrow [\sigma]_k A$ is given by

$$\sigma((r_0 \otimes \lambda_0) \otimes \cdots \otimes (r_i \otimes \lambda_i)) = (1 \otimes 1) \otimes (r_0 \otimes \sigma(\lambda_0)) \otimes \cdots \otimes (r_i \otimes \sigma(\lambda_i)) \in A[i+1].$$

The inclusion $A = A[0] \hookrightarrow [\sigma]_k A$ is characterized by the following universal property.

Lemma 1.2.8. *For every k -algebra A there exists a k - σ -algebra $[\sigma]_k A$ and a morphism $\psi: A \rightarrow [\sigma]_k A$ of k -algebras such that for every k - σ -algebra R and every morphism $\psi': A \rightarrow R$ of k -algebras there exists a unique morphism $\varphi: [\sigma]_k A \rightarrow R$ of k - σ -algebras making*

$$\begin{array}{ccc} A & \xrightarrow{\psi} & [\sigma]_k A \\ & \searrow \psi' & \swarrow \varphi \\ & R & \end{array}$$

commutative.

□

In other words,

$$\mathrm{Hom}([\sigma]_k A, R) \simeq \mathrm{Hom}(A, R^\sharp) \quad (1.3)$$

and $[\sigma]_k$ is left adjoint to the forgetful functor $(-)^{\sharp}$.

Example 1.2.9. If $A = k[y_1, \dots, y_n]$, then $[\sigma]_k A = k\{y_1, \dots, y_n\}$. More generally, if $A = k[y_1, \dots, y_n]/(F)$, then $[\sigma]_k A = k\{y_1, \dots, y_n\}/[F]$.

Let $k[\mathcal{X}]$ denote the coordinate ring of the variety $\mathcal{X} = \mathrm{Hom}(k[\mathcal{X}], -)$. Then (1.3) with $A = k[\mathcal{X}]$ shows that $[\sigma]_k \mathcal{X}$ is represented by $[\sigma]_k k[\mathcal{X}]$. If $M \subset k[\mathcal{X}]$ generates $k[\mathcal{X}]$ as a k -algebra, then $M \subset [\sigma]_k k[\mathcal{X}]$ generates $[\sigma]_k k[\mathcal{X}]$ as a k - σ -algebra. Therefore $[\sigma]_k \mathcal{X}$ is a σ -variety over k . Indeed, $k\{[\sigma]_k \mathcal{X}\} = [\sigma]_k k[\mathcal{X}]$. In the sequel, if confusion is unlikely we will often write $\mathcal{X}$ instead of $[\sigma]_k \mathcal{X}$. In particular, we will write $k\{\mathcal{X}\}$ instead of $k\{[\sigma]_k \mathcal{X}\}$ and by a σ -closed σ -subvariety of a variety $\mathcal{X}$, we mean a σ -closed σ -subvariety of $[\sigma]_k \mathcal{X}$.

Of course $[\sigma]_k$ is a functor from the category of varieties over k to the category of σ -varieties over k : If $\phi: \mathcal{X} \rightarrow \mathcal{Y}$ is a morphism of varieties, then we can define $[\sigma]_k(\phi): [\sigma]_k \mathcal{X} \rightarrow [\sigma]_k \mathcal{Y}$ by

$$([\sigma]_k(\phi))_R: ([\sigma]_k \mathcal{X})(R) = \mathcal{X}(R^\sharp) \xrightarrow{\phi_{R^\sharp}} \mathcal{Y}(R^\sharp) = ([\sigma]_k \mathcal{Y})(R)$$

for any k - σ -algebra R .

Next we will define the Zariski closures of a σ -closed σ -subvariety of a variety. We will use notations for varieties similar to the ones introduced for k -algebras above: If $\mathcal{X}$ is a variety over k and $i \geq 0$, then

$$\sigma^i \mathcal{X}$$

denotes the variety over k obtained from $\mathcal{X}$ by base extension via $\sigma^i: k \rightarrow k$. Similarly, if $\phi: \mathcal{X} \rightarrow \mathcal{Y}$ is a morphism of varieties over k , then $\sigma^i \phi: \sigma^i \mathcal{X} \rightarrow \sigma^i \mathcal{Y}$ denotes the morphism of varieties over k obtained from ϕ by base extension via $\sigma^i: k \rightarrow k$. We also set

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

Let Y be a σ -closed σ -subvariety of $\mathcal{X}$. Then Y is defined by a σ -ideal $\mathbb{I}(Y) \subset k\{\mathcal{X}\} = \cup_{i \geq 0} k[\mathcal{X}[i]]$. For $i \geq 0$, the closed subvariety

$$Y[i]$$

of $\mathcal{X}[i]$ defined by $\mathbb{I}(Y) \cap k[\mathcal{X}[i]] \subset k[\mathcal{X}[i]]$ is called the i -th order Zariski closure of Y in $\mathcal{X}$. The 0-th order Zariski closure of Y in $\mathcal{X}$ is also the Zariski closure of Y in $\mathcal{X}$. We say that Y is Zariski dense in $\mathcal{X}$ if the Zariski closure of Y in $\mathcal{X}$ equals $\mathcal{X}$. Note that Y is Zariski dense in $\mathcal{X}$ if and only if $k[\mathcal{X}] \rightarrow k\{Y\}$ is injective.

For $i \geq 1$ we have morphisms of varieties

$$\pi_i: \mathcal{X}[i] \rightarrow \mathcal{X}[i-1], (x_0, \dots, x_i) \mapsto (x_0, \dots, x_{i-1})$$

and

$$\sigma_i: \mathcal{X}[i] \rightarrow \sigma(\mathcal{X}[i-1]) = \sigma \mathcal{X} \times \cdots \times \sigma^i \mathcal{X}, (x_0, \dots, x_i) \mapsto (x_1, \dots, x_i)$$

that form a commutative diagram:

$$\begin{array}{ccc} \mathcal{X}[i] & \xrightarrow{\pi_i} & \mathcal{X}[i-1] \\ \sigma_i \downarrow & & \downarrow \sigma_{i-1} \\ \sigma(\mathcal{X}[i-1]) & \xrightarrow{\sigma \pi_{i-1}} & \sigma(\mathcal{X}[i-2]) \end{array}$$

There are induced morphisms $\pi_i: Y[i] \rightarrow Y[i-1]$ of varieties over k , and since $\mathbb{I}(Y) \subset k\{\mathcal{X}\}$ is a σ -ideal, we also have induced morphisms $\sigma_i: Y[i] \rightarrow \sigma(Y[i-1])$ of varieties over k .

1.3 Other approaches to difference algebraic geometry

There are different approaches to algebraic geometry, e.g., Weil style algebraic geometry, the elementary approach as in the first chapter of Hartshorne's book [Har77], or modern algebraic geometry via schemes and Grothendieck's philosophy.

Similarly, there are different approaches to difference algebraic geometry. The standard textbooks [Coh65] and [Lev08] are written in the style of Weil. Surely each approach has its pros and cons. However, the choice of the approach is more than a mere matter of taste. One approach may facilitate concepts and results that have no counterpart in another approach. So, at least in the opinion of the author, the optimal choice of the approach heavily depends on the mathematical challenge at hand. For example, Hrushovski's proof of the twisted Lang-Weil estimates ([Hru04]) is based on an intrinsic scheme theoretic approach to difference algebraic geometry, rather than on the standard Weil style approach.

The purpose of this section is to briefly sketch approaches to difference algebraic geometry that are different from the one we have presented in the previous section. We also compare these approaches to our approach and motivate our choice.

1.3.1 The standard approach

We start by explaining the approach to difference algebraic geometry employed in the classical literature on difference algebra (as in [Coh65] and [Lev08]).

Let k be a σ -field and let $K = k(x_1, x_2, \dots)$ be the field of rational functions in a denumerable set of indeterminates $x_1, x_2, \dots$ over k . The *universal system* $\mathcal{U} = \mathcal{U}(k)$ of σ -overfields of k is the family of σ -field extensions of k that can be defined on the algebraic closure of K .

For a set $F \subset k\{y_1, \dots, y_n\}$ of σ -polynomials let $\mathcal{M}(F)$ denote the set of solutions of F in the members of $\mathcal{U}$, i.e., $\mathcal{M}(F)$ is the set of n -tuples $a = (a_1, \dots, a_n)$ such that $a_1, \dots, a_n \in K$, where K belongs to $\mathcal{U}$ and $f(a) = 0$ for all $f \in F$. A difference variety in the sense of [Coh65] and [Lev08] is such a set of solutions. To avoid confusion with the terminology introduced in Section 1.2, let us agree to call a set of the form $\mathcal{M}(F)$ a *classical σ -variety*. Because of Proposition 2.6.2 in [Lev08] it would not make a substantial difference to allow arbitrary σ -field extensions of k in the definition of a classical σ -variety.

If b is an element of a difference field such that $b\sigma(b) = 0$, then $b = 0$. From this it follows easily that for a classical σ -variety $\mathcal{M}$ the set

$$F(\mathcal{M}) = \{f \in k\{y_1, \dots, y_n\} \mid f(a) = 0 \ \forall a \in \mathcal{M}\}$$

is a perfect σ -ideal of $k\{y\} = k\{y_1, \dots, y_n\}$.

A basic result is that $F(\mathcal{M}(\mathfrak{a})) = \mathfrak{a}$ for any perfect σ -ideal $\mathfrak{a}$ of $k\{y\}$. It then follows that $\mathfrak{a} \mapsto \mathcal{M}(\mathfrak{a})$ defines a bijection between the perfect σ -ideals of $k\{y\}$ and the classical σ -varieties ([Lev08, Theorem 2.6.4]). The inverse map is given by $\mathcal{M} \mapsto F(\mathcal{M})$.

Remarkably, the standard textbooks do not define the concept of a morphism of difference varieties. However, if one defines a morphism of classical σ -varieties to be a map given in coordinates by σ -polynomials, then one can show that the category of classical σ -varieties is anti-equivalent to the category of perfectly σ -reduced finitely σ -generated k - σ -algebras ([Wib13, Theorem 2.1.21]). It follows that the category of classical σ -varieties is equivalent to the category of perfectly σ -reduced σ -varieties (as defined in Section 1.2). Precisely in this sense our approach encompasses the standard approach.

1.3.2 Intrinsic difference schemes

A Grothendieck style approach to difference algebraic geometry was initiated by E. Hrushovski in his remarkable paper on the Frobenius automorphisms ([Hru04]). To a difference ring R one associates its difference spectrum $\text{Spec}^\sigma(R)$. As a set, the difference spectrum is the set of all σ -prime σ -ideals of R . It is naturally a topological space, say, by restricting the Zariski topology from $\text{Spec}(R)$. The closed subsets of $\text{Spec}^\sigma(R)$ are in bijection with the perfect σ -ideals of R . As in the case of plain rings, there is a naturally defined structure sheaf $\mathcal{O}_X$ of difference rings on $X = \text{Spec}^\sigma(R)$ such that for a σ -prime σ -ideal $\mathfrak{p}$ of R the stalk of $\mathcal{O}_X$ at $\mathfrak{p}$ equals $R_{\mathfrak{p}}$. A *difference scheme* may then be defined as a topological space, equipped with a sheaf of difference rings such that any point has an open neighborhood isomorphic to the difference spectrum of a difference ring. A morphism of difference schemes is a morphism of locally ringed spaces compatible with the difference ring structure.

Despite the obvious analogy to the definition of a scheme, there are some pitfalls here. For example, the difference spectrum of a difference ring may well be empty. This happens, for example, for $R = \mathbb{C} \times \mathbb{C}$ with $\sigma(a, b) = (b, a)$. To avoid such pathologies a certain condition called *well-mixedness* has to be imposed on all difference rings. A difference ring R is called well-mixed if $fg = 0$ implies $f\sigma(g) = 0$ for all $f, g \in R$.

However, even if R is a σ -domain, the canonical map from R into the global sections of $\text{Spec}^\sigma(R)$ need not be an isomorphism. For example, for $R = \mathbb{C}[x]$ with $\sigma(f(x)) = f(x+1)$ the difference spectrum consists of a single point, namely the zero ideal. So the global sections of $\text{Spec}^\sigma(R)$ are $\mathbb{C}(x)$ and the inclusion map $\mathbb{C}[x] \rightarrow \mathbb{C}(x)$ induces an isomorphism of affine difference schemes $\text{Spec}^\sigma(\mathbb{C}(x)) \rightarrow \text{Spec}^\sigma(\mathbb{C}[x])$. The inverse of this isomorphism is not induced by a morphism $\mathbb{C}(x) \rightarrow \mathbb{C}[x]$ of difference rings. In particular, the category of affine difference schemes is not naturally equivalent to some category of difference rings.

1.3.3 Fields with operators

A fairly general formalism for dealing with solutions of differential and difference equations from an algebraic-geometric point of view has been developed in [MS10] and [MS11]. See also [Kam13]. It is based on the modern scheme theoretic language and as opposed to the approach from Subsection 1.3.2 keeps track of the ambient ring. Our approach from Section 1.2 is essentially equivalent to this approach apart from the facts that

- we are restricted to a certain class of operators, namely difference operators, i.e., (one) endomorphism,
- we are restricted to the affine setting,
- we are using a functorial formalism (the functor of points), because this is more appropriate for dealing with groups. As for group schemes, the underlying topological space is not a group, only the functor of points yields groups.

1.3.4 Model theory

Finally, it should not remain unmentioned that model theory naturally provides a setup for doing difference algebraic geometry. The model theory of difference fields has been studied extensively in the last years (e.g., [CH99], [CHP02]) and has found several interesting applications (e.g., [Hru01], [CH08], [MS14]).

A difference field k is called σ -closed (or a model of ACFA) if any system of algebraic difference equations that has a solution in a σ -field extension of k already has a solution in k . Any difference field may be embedded into a σ -closed σ -field but there appears to be no reasonable notion of a “difference closure”.

As one may regard sets definable in the theory of algebraically closed fields as the model theoretic conception of a variety, we may regard sets definable in ACFA (the theory of difference closed fields) as the model theoretic conception of a difference variety. However, as ACFA does not (fully) eliminate quantifiers, the analogy is somewhat limited. A group definable in ACFA may then be regarded as the model theoretic conception of a difference algebraic group.

An advantage of this approach is that one immediately has at one’s disposal several notions from model theory. For example, a model theorist may argue that quotients of groups definable in ACFA exist simply by pointing out that ACFA has elimination of imaginaries. We will prove the existence of quotients in our setting based on some fairly sophisticated difference algebra. It is not always the case that results can be transferred between the different approaches easily. For example, is the quotient of quantifier free definable groups again quantifier free definable? Can one use elimination of imaginaries for ACFA to show that a difference Hopf subalgebra (see Definition 2.1.2) of a finitely σ -generated difference Hopf algebra is itself finitely σ -generated?

The usual model-theoretic habit of fixing a “large” model of ACFA in advance may lead to some differences to the standard and our approach. For example, in our approach, setting

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

for any k - σ -algebra R defines a difference algebraic subgroup of the multiplicative group $\mathbb{G}_m$ (over $\mathbb{Q}$). If one has to replace G with $G(K)$, where K is a model of ACFA containing $\mathbb{Q}$, the group obtained is either the trivial group or the group with three elements, depending on whether or not $\sigma: K \rightarrow K$ acts trivially on the third roots of unity. Thus the model-theoretic approach introduces a non-trivial dependence on the choice of K .

However, all in all, the differences between the standard approach and the model-theoretic approach appear to be more of a technical nature. The main advantage of our approach is that we are not restricted to difference fields. We allow solutions in arbitrary difference algebras and not just in difference field extensions. Or from a more algebraic perspective: We can deal with arbitrary difference ideals geometrically, while the standard and the model-theoretic approach is essentially restricted to perfect difference ideals.

1.3.5 Our approach

To motivate our approach, let us look at a simple example. Whatever the choice of setup is, it seems clear that the following two systems of algebraic difference equations

$$y^2 = 1 \tag{1.4}$$

and

$$y^2 = 1, \sigma(y) = y \tag{1.5}$$

define two objects worthy of the name *difference algebraic subgroup of the multiplicative group* $\mathbb{G}_m$. But are these groups the same? The answer is not obvious. For example, a model theorist might instantly place himself in a large difference field and argue that

$a^2 = 1$ implies that $a = 1$ or $a = -1$ and therefore $\sigma(a) = a$. So clearly, the groups are the same.

On the other hand, one may well argue that the system (1.4) has solutions that are more interesting than just 1 and -1 . For example, if we consider the ring of all sequences $(a_n)_{n \in \mathbb{N}}$ in $\mathbb{C}$ with componentwise addition and multiplication and difference operator defined by $\sigma((a_n)_{n \in \mathbb{N}}) = (a_{n+1})_{n \in \mathbb{N}}$, then any sequence whose entries are plus and minus one is a solution to $y^2 = 1$. However, only the two constant sequences $(1, 1, \dots)$ and $(-1, -1, \dots)$ also solve the system (1.5). So the groups are clearly different.

The above example shows that it is of utmost importance to specify where one is looking for the solutions. The approaches in Subsections 1.3.1 and 1.3.4 only allow solutions in difference fields. The approach in Subsection 1.3.2 allows solutions in well-mixed difference rings. Our approach and the approach in Subsection 1.3.3 allow solutions in arbitrary difference rings.

The generalization from classical σ -varieties (Subsection 1.3.1) to our σ -varieties (Section 1.2) is in some sense similar to the generalization from a reduced scheme of finite type to an arbitrary affine scheme of finite type.

The advantages of working with schemes rather than with varieties in the theory of algebraic groups are manifold. (Cf. the preface of [Mil15].) The situation for difference algebraic groups is similar. In fact, in difference algebra there are several types of elements in a difference ring that play a role analogous to the role of nilpotent ring elements in algebraic geometry. (Cf. page 6 of the introduction.) Many results presented in this thesis, e.g., the isomorphism theorems in Section 5.2, would not be possible in the standard approach to difference algebraic geometry. Some of our constructions would not make sense if we were restricted to solutions in difference fields. Indeed, Chapter 6 would become meaningless without the possibility to consider solutions in general difference rings.

Chapter 2

Basic properties of difference algebraic groups

*Starting from Section 2.2 we assume that the base σ -ring k is a σ -field.*¹

This chapter is the heart of this thesis. We define difference algebraic groups, study their Zariski closures, prove two fundamental finiteness theorems and introduce basic numerical invariants for difference algebraic groups.

2.1 Difference algebraic groups: Definition and examples

In this section we define σ -algebraic groups and present some examples. We also show that every σ -algebraic group is isomorphic to a σ -closed subgroup of some general linear group.

Since the category of σ -varieties has products and a terminal object (Remark 1.2.3) the following definition makes sense.

Definition 2.1.1. *Let k be a σ -ring. A σ -algebraic group over k is a group object in the category of σ -varieties over k .*

In the sequel we usually drop the “over k ”, i.e., a σ -algebraic group is understood to be a σ -algebraic group over k where k is some fixed σ -ring or σ -field. Alternatively, we could define a σ -algebraic group as a functor from k - σ -Alg to Groups, the category of groups, that is representable by a finitely σ -generated k - σ -algebra.

A *morphism of σ -algebraic groups* is of course a morphism of σ -varieties that respects the group structure. A *σ -closed embedding* of σ -algebraic groups is a morphism of σ -algebraic groups that is a σ -closed embedding of σ -varieties. We write

$$\phi: G \hookrightarrow H$$

to express that ϕ is a σ -closed embedding of σ -algebraic groups.

Definition 2.1.2. *Let k be a σ -ring. A k - σ -Hopf algebra is a Hopf algebra A over k with the structure of a k - σ -algebra such that the Hopf-algebra structure maps $\Delta: A \rightarrow A \otimes_k A$, $S: A \rightarrow A$ and $\varepsilon: A \rightarrow k$ are morphisms of k - σ -algebras.*

¹The only exception to this rule is the beginning of Subsection 6.3.4.

A k - σ -Hopf subalgebra of a k - σ -Hopf algebra is a k - σ -subalgebra that is Hopf subalgebra. For a Hopf algebra A we denote the kernel of the counit $\varepsilon: A \rightarrow k$ by $\mathfrak{m}_A$. Similarly, if G is a σ -algebraic group, we will write

$$\mathfrak{m}_G$$

for $\mathfrak{m}_{k\{G\}}$.

Proposition 2.1.3. *The category of σ -algebraic groups over k is anti-equivalent to the category of k - σ -Hopf algebras that are finitely σ -generated over k .*

Proof. This follows from Remark 1.2.2 in an analogous fashion to Theorem 1.4 in [Wat79]. $\square$

Before presenting some examples of σ -algebraic groups, we explain how some well-known constructions from the theory of (abstract) groups carry over to σ -algebraic groups.

Let G be a σ -algebraic group. A σ -closed subgroup H of 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 . Then H itself is a σ -algebraic group. We write

$$H \leq G$$

to express that H is a σ -closed subgroup of G . If H_1 and H_2 are σ -closed subgroups of G , then $H_1 \cap H_2$ is also a σ -closed subgroup of G .

Let A be a k - σ -Hopf algebra. A Hopf ideal of A is called a σ -Hopf ideal if it is a σ -ideal. In analogy to Section 2.1 in [Wat79], we obtain the following lemma from Lemma 1.2.5.

Lemma 2.1.4. *Let G be a σ -algebraic group. There is a one-to-one correspondence between the σ -closed subgroups of G and the σ -Hopf ideals in $k\{G\}$.* $\square$

The σ -Hopf ideal $\mathfrak{m}_G \subset k\{G\}$ corresponds to the trivial subgroup $1 \leq G$. A σ -closed subgroup N of a σ -algebraic group G is called *normal* if $N(R)$ is a normal subgroup of $G(R)$ for any k - σ -algebra R . We write

$$N \trianglelefteq G$$

to express that N is a normal σ -closed subgroup of G .

If G and H are σ -algebraic groups. The product $G \times H$ is naturally a σ -algebraic group: For any k - σ -algebra R , the group $(G \times H)(R) = G(R) \times H(R)$ is the product of the groups $G(R)$ and $H(R)$.

If G is a σ -algebraic group over a σ -ring k and $k \rightarrow k'$ is a morphism of σ -rings, then $G_{k'}$ is naturally a σ -algebraic group over k' . If H is a σ -closed subgroup of G , then $H_{k'}$ is naturally a σ -closed subgroup of $G_{k'}$.

Recall that a subgroup H of an (abstract) group G is called a characteristic subgroup if $\phi(H) = H$ for every automorphism ϕ of G . Since a characteristic subgroup is stable under every inner automorphism, a characteristic subgroup is a normal subgroup.

The naive generalization to σ -algebraic groups is not adequate: As illustrated in Example 5.3.14, there exists a non-normal σ -closed subgroup H of a σ -algebraic group G with the property that every automorphism of G induces an automorphism of H . To remedy this shortcoming we make the following definition (cf. [DG70, Section 3.9, Chapter II, §1, p. 166] or [Mil12, Def. 3.7, Chapter VII, p. 90]).

Definition 2.1.5. A σ -closed subgroup H of a σ -algebraic group G is called a characteristic subgroup of G if for every k - σ -algebra R every automorphism of the σ -algebraic group G_R induces an automorphism of H_R .

By conjugation, an element $g \in G(R)$ induces an automorphism of G_R . Therefore a characteristic subgroup is normal.

From now on we assume that k is a σ -field².

Example 2.1.6. Let V be a finite dimensional k -vector space. For every k - σ -algebra R let $\mathrm{GL}(V)(R)$ denote the group of R -linear automorphisms of $V \otimes_k R$. Then $\mathrm{GL}(V)$ is naturally a functor from k - σ -Alg to Groups. Indeed, $\mathrm{GL}(V)$ is a σ -algebraic group: By choosing a basis $v_1, \dots, v_n$ of V , we can identify $\mathrm{GL}(V)(R)$ with $\mathrm{GL}_n(R)$ and $\mathrm{GL}(V)$ is represented by

$$k\{\mathrm{GL}_n\} = k\{x_{ij}, \frac{1}{\det(x)}\}.$$

More generally:

Example 2.1.7. Every algebraic group over k can be interpreted as a σ -algebraic group over k . Here, as throughout the text, by an algebraic group over k we mean an affine group scheme of finite type over k . Indeed, let $\mathcal{G}$ be an algebraic group over k and as in Section 1.2.4, let $R^\sharp$ denote the k -algebra obtained from the k - σ -algebra R by forgetting σ . Then

$$R \rightsquigarrow \mathcal{G}(R^\sharp)$$

is a functor from k - σ -Alg to Groups, i.e., $[\sigma]_k \mathcal{G}$ is a σ -algebraic group.

We will often write $\mathcal{G}$ instead of $[\sigma]_k \mathcal{G}$. In particular, by a σ -closed subgroup of $\mathcal{G}$ we mean a σ -closed subgroup of $[\sigma]_k \mathcal{G}$ and we write $k\{\mathcal{G}\}$ for $k\{[\sigma]_k \mathcal{G}\} = [\sigma]_k k\{\mathcal{G}\}$.

Example 2.1.8. Let $0 \leq \alpha_1 < \dots < \alpha_n$ and $1 \leq \beta_1, \dots, \beta_n$ be integers. We can define a σ -closed subgroup G of the multiplicative group $\mathbb{G}_m$ by

$$G(R) = \{g \in R^\times \mid \sigma^{\alpha_1}(g)^{\beta_1} \dots \sigma^{\alpha_n}(g)^{\beta_n} = 1\} \leq \mathbb{G}_m(R)$$

for any k - σ -algebra R . Similarly, we can define an endomorphism $\phi: \mathbb{G}_m \rightarrow \mathbb{G}_m$ of the multiplicative group (considered as a σ -algebraic group) by

$$\phi_R: \mathbb{G}_m(R) \rightarrow \mathbb{G}_m(R), \quad g \mapsto \sigma^{\alpha_1}(g)^{\beta_1} \dots \sigma^{\alpha_n}(g)^{\beta_n}$$

for any k - σ -algebra R .

Example 2.1.9. Every homogeneous linear difference equation

$$\sigma^n(y) + \lambda_{n-1}\sigma^{n-1}(y) + \dots + \lambda_0 y = 0$$

over k defines a σ -closed subgroup G of the additive group $\mathbb{G}_a$, i.e.,

$$G(R) = \{g \in R \mid \sigma^n(g) + \lambda_{n-1}\sigma^{n-1}(g) + \dots + \lambda_0 g = 0\} \leq \mathbb{G}_a(R)$$

for any k - σ -algebra R . We can define an endomorphism $\phi: \mathbb{G}_a \rightarrow \mathbb{G}_a$ of the additive group (considered as a σ -algebraic group) by

$$\phi_R: \mathbb{G}_a(R) \rightarrow \mathbb{G}_a(R), \quad g \mapsto \sigma^n(g) + \lambda_{n-1}\sigma^{n-1}(g) + \dots + \lambda_0 g$$

for any k - σ -algebra R .

²The only exception to this rule is the beginning of Subsection 6.3.4.

Example 2.1.10. The equations of the unitary group define a σ -closed subgroup of the general linear group:

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

for any k - σ -algebra R .

Example 2.1.11. We can define a σ -closed subgroup G of SL_n by

$$G(R) = \{g \in \mathrm{SL}_n(R) \mid \sigma^m(g) = g\} \leq \mathrm{SL}_n(R)$$

for any k - σ -algebra R .

Examples 2.1.10 and 2.1.11 can be generalized as follows:

Example 2.1.12. Let k be a σ -field, $m \geq 1$ an integer, $\mathcal{G}$ an algebraic group over k and $\phi: \mathcal{G} \rightarrow \sigma^m \mathcal{G}$ a morphism of algebraic groups over k . There is a morphism $\sigma^m: \mathcal{G} \rightarrow \sigma^m \mathcal{G}$ of σ -algebraic groups over k , which, in terms of equations is given by applying σ^m to the coordinates. In terms of k - σ -algebras this morphism can be described as $\sigma^m(k\{\mathcal{G}\}) = k\{\mathcal{G}\} \otimes_k k \rightarrow k\{\mathcal{G}\}$, $f \otimes \lambda \mapsto \sigma^m(f)\lambda$. We can define a σ -closed subgroup G of $\mathcal{G}$ by

$$G(R) = \{g \in \mathcal{G}(R) \mid \sigma^m(g) = \phi(g)\} \leq \mathcal{G}(R)$$

for any k - σ -algebra R . Note that Example 2.1.10 ($\mathcal{G} = \mathrm{GL}_n$, $m = 1$, $\phi(g) = (g^{-1})^T$) and Example 2.1.11 ($\mathcal{G} = \mathrm{SL}_n$, $\phi(g) = g$) are special cases of this construction.

Example 2.1.13. For a k - σ -algebra R let $G(R) = R \times R^\times$. A straight forward computation shows that setting

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 + h_1 \sigma(h_1)^{-1} n_2, h_1 h_2)$$

for $(n_1, h_1), (n_2, h_2) \in G(R)$ defines a group structure on $G(R)$. Thus G is naturally a σ -algebraic group. See Examples 2.1.18 and 3.3.16 for alternative descriptions of this group.

Example 2.1.14. Let k be a field of positive characteristic p and let q be a power of p . Consider k as a σ -field via the Frobenius, i.e., $\sigma(\lambda) = \lambda^q$ for $\lambda \in k$. An algebraic group $\mathcal{G}$ over k can be considered as a σ -algebraic group over k : We turn $k[\mathcal{G}]$ into a k - σ -algebra by setting $\sigma(f) = f^q$ for $f \in k[\mathcal{G}]$. Then clearly $k[\mathcal{G}]$ is a k - σ -Hopf algebra.

A σ -algebraic group as in Example 2.1.14 will be called a *Frobenius algebraic group*.

Example 2.1.15. Let k be a σ -field, $\mathbf{G}$ a finite group and $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ a group endomorphism. Let A be the k -vector space with basis $(e_g)_{g \in \mathbf{G}}$. We consider it as a k -algebra via

$$(\sum \lambda_g e_g)(\sum \mu_g e_g) = \sum \lambda_g \mu_g e_g.$$

We can define a Hopf algebra structure on A by

$$\Delta(e_g) = \sum_{(g_1, g_2)} e_{g_1} \otimes e_{g_2},$$

where the sum ranges over all pairs $(g_1, g_2) \in \mathbf{G}^2$ such that $g_1 g_2 = g$, $S(e_g) = e_{g^{-1}}$ and $\varepsilon(e_g) = 0$ for $g \neq 1$ and $\varepsilon(e_1) = 1$. The algebraic group corresponding to A is usually called the constant group scheme for $\mathbf{G}$. (See [Wat79, Section 2.3].) Extend $\sigma: k \rightarrow k$ to $\sigma: A \rightarrow A$ by $\sigma(e_g) = \sum_h e_h$, where the sum is taken over all $h \in \mathbf{G}$ such that $\sigma(h) = g$. This defines a k - σ -Hopf algebra structure on A and therefore we obtain an associated σ -algebraic group $G = \mathrm{Hom}(A, -)$.

In Section 6.2 we will see that any σ -algebraic group G such that $k\{G\}$ is an étale k -algebra is up to a suitable action of the absolute Galois group of k of the form described in Example 2.1.15 (Corollary 6.2.17).

Our next goal is to show that any σ -algebraic group is isomorphic to a σ -closed subgroup of some general linear group. For this we need a lemma on Hopf algebras that will also be useful later.

Lemma 2.1.16. *Let A be a k -Hopf algebra, B a k - σ -Hopf algebra and $A \rightarrow B$ a morphism of k -Hopf algebras. Then the morphism $[\sigma]_k A \rightarrow B$ of k - σ -algebras induced by Lemma 1.2.8 is a morphism of k -Hopf algebras.*

Proof. The comultiplication of $[\sigma]_k A$ is $[\sigma]_k(\Delta): [\sigma]_k A \rightarrow [\sigma]_k(A \otimes_k A) = [\sigma]_k A \otimes_k [\sigma]_k A$ where $\Delta: A \rightarrow A \otimes_k A$ is the comultiplication of A . All the subdiagrams with empty interior of

$$\begin{array}{ccc} [\sigma]_k A & \longrightarrow & [\sigma]_k(A \otimes_k A) \\ \uparrow & & \uparrow \\ A & \longrightarrow & A \otimes_k A \\ \downarrow & & \downarrow \\ B & \longrightarrow & B \otimes_k B \end{array}$$

commute. We have to show that the outer diagram commutes. But this follows from the uniqueness statement in Lemma 1.2.8. A similar argument applies for the counit. $\square$

Similar to algebraic groups, σ -algebraic groups can be linearized:

Theorem 2.1.17. *Let G be a σ -algebraic group over k . Then there exists a finite dimensional k -vector space V and a σ -closed embedding $G \hookrightarrow \mathrm{GL}(V)$. In particular, G is isomorphic to a σ -closed subgroup of GL_n for some $n \geq 1$.*

Proof. Assume that $f_1, \dots, f_m \in k\{G\}$ generate $k\{G\}$ as a k - σ -algebra. By [Wat79, Section 3.3, p. 24] there exists a Hopf subalgebra A of $k\{G\}$ that contains $f_1, \dots, f_m$ and is finitely generated as a k -algebra. By [Wat79, Section 3.4, p. 25] there exists an integer $n \geq 1$ and a surjective morphism $k[\mathrm{GL}_n] \rightarrow A$ of Hopf algebras. By Lemma 1.2.8 the morphism $k[\mathrm{GL}_n] \rightarrow A \hookrightarrow k\{G\}$ of k -algebras extends to a morphism $k\{\mathrm{GL}_n\} \rightarrow k\{G\}$ of k - σ -algebras. Indeed, this is a morphism of k - σ -Hopf algebras (Lemma 2.1.16) and since $f_1, \dots, f_m$ lie in the image, it is surjective. Now the claim follows from Lemma 1.2.7. $\square$

Example 2.1.18. Let us find a linearization of the σ -algebraic group G from Example 2.1.13. Let H be the σ -closed subgroup of GL_2 given by

$$H(R) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathrm{GL}_2(R) \mid \sigma(a) = c \right\}$$

for any k - σ -algebra R . It is straight forward to check that the assignment

$$(n, h) \mapsto \begin{pmatrix} h & \sigma(h)n \\ 0 & \sigma(h) \end{pmatrix}$$

defines an isomorphism $G \simeq H$.

2.2 Zariski closures of difference algebraic groups and the growth group

From now on we assume that the base σ -ring k is a σ -field. The only exception to this rule is the beginning of Subsection 6.3.4.

In this section we show that the eventual growth of the Zariski closures of a σ -closed subgroup G of an algebraic group $\mathcal{G}$ is governed by an algebraic group, called the growth group of G (with respect to the σ -closed embedding $G \hookrightarrow \mathcal{G}$). We also introduce the σ -dimension and the order of a σ -algebraic group G .

Let k be a σ -field and $\mathcal{G}$ an algebraic group over k . Then, for every $i \geq 0$, ${}^{\sigma^i}\mathcal{G}$ and $\mathcal{G}[i] = \mathcal{G} \times {}^{\sigma}\mathcal{G} \times \cdots \times {}^{\sigma^i}\mathcal{G}$ (see Section 1.2.4) are naturally algebraic groups over k . For every $i \geq 1$ the maps $\pi_i: \mathcal{G}[i] \rightarrow \mathcal{G}[i-1]$ and $\sigma_i: \mathcal{G}[i] \rightarrow {}^{\sigma}(\mathcal{G}[i-1])$ are morphisms of algebraic groups over k .

Let G be a σ -closed subgroup of $\mathcal{G}$. For every $i \geq 0$ we have an inclusion $k[\mathcal{G}[i]] \subset k\{\mathcal{G}\}$ of Hopf algebras. Since $\mathbb{I}(G) \subset k\{\mathcal{G}\}$ is a Hopf ideal, $\mathbb{I}(G) \cap k[\mathcal{G}[i]]$ is a Hopf ideal of $k[\mathcal{G}[i]]$. So the i -th order Zariski closure $G[i]$ of G in $\mathcal{G}$ is a closed subgroup of $\mathcal{G}[i]$. The maps $\pi_i: G[i] \rightarrow G[i-1]$ and $\sigma_i: G[i] \rightarrow {}^{\sigma}(G[i-1])$ are morphisms of algebraic groups over k and form a commutative diagram:

$$\begin{array}{ccc} G[i] & \xrightarrow{\pi_i} & G[i-1] \\ \sigma_i \downarrow & & \downarrow \sigma_{i-1} \\ {}^{\sigma}(G[i-1]) & \xrightarrow{{}^{\sigma}\pi_{i-1}} & {}^{\sigma}(G[i-2]) \end{array} \quad (2.1)$$

For $i \geq 1$ we set

$$\mathcal{G}_i = \ker(\pi_i) \leq G[i].$$

We also set $\mathcal{G}_0 = G[0]$. Because of (2.1) we have induced morphisms $\sigma_i: \mathcal{G}_i \rightarrow {}^{\sigma}(\mathcal{G}_{i-1})$ of algebraic groups over k .

Proposition 2.2.1. *For every $i \geq 1$ the map $\sigma_i: \mathcal{G}_i \rightarrow {}^{\sigma}(\mathcal{G}_{i-1})$ is a closed embedding and there exists an integer $m \geq 1$ such that $\sigma_i: \mathcal{G}_i \rightarrow {}^{\sigma}(\mathcal{G}_{i-1})$ is an isomorphism for every $i \geq m$.*

Proof. Let us start by describing σ_i in algebraic terms. Assume that $a = (a_1, \dots, a_n)$ generates $k[\mathcal{G}]$ as a k -algebra and let $\bar{a}$ denote the image of a in $k\{G\}$. So

$$k[\mathcal{G}] = k[a] \subset k[a, \sigma(a), \dots] = k\{\mathcal{G}\}$$

and $k[G[i]] = k[\bar{a}, \dots, \sigma^i(\bar{a})]$. The morphism $\sigma_i: G[i] \rightarrow {}^{\sigma}(G[i-1])$ corresponds to the map

$$\sigma(k[\bar{a}, \dots, \sigma^{i-1}(\bar{a})]) \longrightarrow k[\bar{a}, \dots, \sigma^i(\bar{a})], \quad f \otimes \lambda \mapsto \sigma(f)\lambda$$

and the morphism $\sigma_i: \mathcal{G}_i \rightarrow {}^{\sigma}(\mathcal{G}_{i-1})$ corresponds to the map

$$\begin{aligned} {}^{\sigma}(k[\bar{a}, \dots, \sigma^{i-1}(\bar{a})]) \otimes_{k[\bar{a}, \dots, \sigma^{i-2}(\bar{a})]} k &\longrightarrow k[\bar{a}, \dots, \sigma^i(\bar{a})] \otimes_{k[\bar{a}, \dots, \sigma^{i-1}(\bar{a})]} k \\ (f \otimes \lambda) \otimes \mu &\longmapsto \sigma(f) \otimes \sigma(\lambda)\mu \end{aligned}$$

where the tensor products are formed in virtue of the counit $\varepsilon: k\{G\} \rightarrow k$. Since $k[\bar{a}, \dots, \sigma^i(\bar{a})] \otimes_{k[\bar{a}, \dots, \sigma^{i-1}(\bar{a})]} k$ is generated as a k -algebra by the image of $\sigma^i(\bar{a})$, the above map is clearly surjective. Thus $\sigma_i: \mathcal{G}_i \rightarrow {}^{\sigma}(\mathcal{G}_{i-1})$ is a closed embedding.

To prove the second claim of the proposition, let us first assume that k is inversive. The map

$$\begin{aligned} \psi_i: k[\bar{a}, \dots, \sigma^{i-1}(\bar{a})] \otimes_{k[\bar{a}, \dots, \sigma^{i-2}(\bar{a})]} k &\longrightarrow k[\bar{a}, \dots, \sigma^i(\bar{a})] \otimes_{k[\bar{a}, \dots, \sigma^{i-1}(\bar{a})]} k \\ f \otimes \lambda &\longmapsto \sigma(f) \otimes \sigma(\lambda) \end{aligned}$$

is a morphism of rings but it is not a morphism of k -algebras. However, since k is inversive, it is surjective. We thus have a descending chain of closed subschemes

$$\mathcal{G}_0 \hookleftarrow \mathcal{G}_1 \hookleftarrow \mathcal{G}_2 \cdots$$

Since $\mathcal{G}_0$ is of finite type over k , this sequence must stabilize. That is, there exists an integer $m \geq 1$ such that ψ_i is bijective for every $i \geq m$. Since k is inversive,

$$k[\mathcal{G}_i] \rightarrow {}^\sigma(k[\mathcal{G}_i]), \quad f \mapsto f \otimes 1$$

is bijective. It follows that for $i \geq m$, the morphism ${}^\sigma(k[\mathcal{G}_{i-1}]) \rightarrow k[\mathcal{G}_i]$ dual to σ_i is an isomorphism, since it can be obtained as the composition ${}^\sigma(k[\mathcal{G}_{i-1}]) \rightarrow k[\mathcal{G}_{i-1}] \xrightarrow{\psi_i} k[\mathcal{G}_i]$ of two bijective maps. This proves the proposition for k inversive.

The general case can be reduced to the inversive case: Let k^* denote the inversive closure of k ([Lev08, Definition 2.1.6]). So, in particular, k^* is an inversive σ -field extension of k . The formation of Zariski closures and of the $\mathcal{G}_i$ is compatible with base extension. It therefore follows from the inversive case, that there exists an integer $m \geq 1$ such that for every $i \geq m$ the morphism $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$ becomes an isomorphism after base extension from k to k^* . But then already σ_i must be an isomorphism for $i \geq m$. $\square$

Proposition 2.2.1 allows us to associate to the inclusion $G \leq \mathcal{G}$ an algebraic group, that measures the (eventual) growth of the Zariski closures $G[i]$ of G in $\mathcal{G}$.

Definition 2.2.2. Let $\mathcal{G}$ be an algebraic group and $G \leq \mathcal{G}$ a σ -closed subgroup. For $i \geq 1$ let $\mathcal{G}_i$ denote the kernel of the projection $\pi_i: G[i] \rightarrow G[i-1]$ between the Zariski closures of G in $\mathcal{G}$. Let $m \geq 0$ denote the smallest integer such that $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$ is an isomorphism for every $i > m$. Then $\mathcal{G}_m$ is called the growth group of G with respect to the σ -closed embedding $G \hookrightarrow \mathcal{G}$.

Example 2.2.3. Let $0 \leq \alpha_1 < \cdots < \alpha_n$ and $1 \leq \beta_1, \dots, \beta_n$ be integers and $G \leq \mathbb{G}_m$ the σ -closed subgroup of the multiplicative group $\mathbb{G}_m$ given by

$$G(R) = \{g \in R^\times \mid \sigma^{\alpha_1}(g)^{\beta_1} \cdots \sigma^{\alpha_n}(g)^{\beta_n} = 1\}$$

for every k - σ -algebra R . Then the growth group of G with respect to the given embedding $G \hookrightarrow \mathbb{G}_m$ is μ_{β_n} , where $\mu_{\beta_n}(T) = \{g \in T^\times \mid g^{\beta_n} = 1\}$ for any k -algebra T .

Example 2.2.4. Let G be a σ -closed subgroup of the additive group defined by a linear difference equation. (Cf. Example 2.1.9.) Then the growth group with respect to the given embedding $G \hookrightarrow \mathbb{G}_a$ is trivial.

Example 2.2.5. Let $\mathcal{G}$ be an algebraic group. The growth group with respect to the tautological embedding $G = [\sigma]_k \mathcal{G} \hookrightarrow \mathcal{G}$ is $\mathcal{G}$ itself.

The following example shows that the growth group does indeed depend on the embedding $G \hookrightarrow \mathcal{G}$ and therefore is not an invariant of G .

Example 2.2.6. Let $G = \mathbb{G}_m$ (considered as a σ -algebraic group). For $n \geq 1$ the σ -closed embedding

$$G \rightarrow \mathbb{G}_m^2, g \mapsto (g, \sigma(g)^n)$$

identifies G with the σ -closed subgroup $G \leq \mathbb{G}_m^2$ given by

$$G(R) = \{(g_1, g_2) \in \mathbb{G}_m(R)^2 \mid \sigma(g_1)^n = g_2\}$$

for any k - σ -algebra R . The growth group of G with respect to the embedding $G \hookrightarrow \mathbb{G}_m^2$ is $\mu_n \times \mathbb{G}_m$.

Even though the growth group itself does depend on the chosen embedding $G \hookrightarrow \mathcal{G}$, it carries some information which only depends on G . We will now show that the dimension of the growth group does not depend on the embedding $G \hookrightarrow \mathcal{G}$. In Section 2.4 we will see that also the size of the growth group is independent of the chosen embedding.

The following theorem can be seen as a group theoretic analog of the classical theorem on the existence of the so-called dimension polynomial of an extension of σ -fields ([Lev08, Theorem 4.2.1]). See also [Hru04, Lemma 4.21].

Theorem 2.2.7. *Let $\mathcal{G}$ be an algebraic group and $G \leq \mathcal{G}$ a σ -closed subgroup. For $i \geq 0$ let $d_i = \dim(G[i])$ denote the dimension of the i -th order Zariski closure of G in $\mathcal{G}$. Then there exist integers $d, e \geq 0$ such that*

$$d_i = d(i + 1) + e \text{ for } i \gg 0.$$

The integer d only depends on G and not on the choice of $\mathcal{G}$ and the σ -closed embedding $G \hookrightarrow \mathcal{G}$. If $d = 0$, the integer e only depends on G and not on the choice of $\mathcal{G}$ and the σ -closed embedding $G \hookrightarrow \mathcal{G}$.

Proof. Let $\mathcal{G}_i$ denote the kernel of $G[i] \rightarrow G[i - 1]$. Then $\dim(G[i]) = \dim(G[i - 1]) + \dim(\mathcal{G}_i)$. Let $m \geq 0$ denote the smallest integer such that $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$ is an isomorphism for every $i > m$. It follows that for $i \gg 0$

$$\begin{aligned} \dim(G[i]) &= \dim(\mathcal{G}_i) + \cdots + \dim(\mathcal{G}_0) = \\ &= (i - m + 1) \dim(\mathcal{G}_m) + \dim(\mathcal{G}_{m-1}) + \cdots + \dim(\mathcal{G}_0) = \\ &= (i + 1) \dim(\mathcal{G}_m) + \dim(\mathcal{G}_{m-1}) + \cdots + \dim(\mathcal{G}_0) - m \dim(\mathcal{G}_m) = \\ &= d(i + 1) + e. \end{aligned}$$

It follows from Proposition 2.2.1 that $e \geq 0$.

Let us now show that $d = \dim(\mathcal{G}_m)$ is independent of the chosen embedding $G \hookrightarrow \mathcal{G}$. So let $G \hookrightarrow \mathcal{G}'$ be another σ -closed embedding. Let $G[i]'$ denote the i -th order Zariski closure of G in $\mathcal{G}'$ and let d'_i, d', e' have the analogous meaning. We have to show that $d = d'$.

Let a be a finite tuple from $k\{G\}$ which generates $k[G[0]] \subset k\{G\}$ as a k -algebra. Similarly, let a' be a finite tuple from $k\{G\}$ which generates $k[G[0]'] \subset k\{G\}$ as a k -algebra. Then $k[G[i]] = k[a, \dots, \sigma^i(a)]$ and there exists an integer $n \geq 0$ such that all coordinates of a' lie in $k[G[n]]$. Then

$$k[G[i]'] = k[a', \dots, \sigma^i(a')] \subset k[a, \dots, \sigma^{n+i}(a)] = k[G[n + i]].$$

Therefore $d'_i \leq d_{n+i}$ and for $i \gg 0$ we have $d'(i + 1) + e' \leq d(n + i + 1) + e$. Letting i tend to infinity we find $d' \leq d$. By symmetry, $d' = d$.

Let us now assume that $d = 0$. We have to show that e does not depend on the choice of the embedding $G \hookrightarrow \mathcal{G}$. To do this we will show that

$$e = \max \{ \dim(R) \mid R \text{ is a finitely generated } k\text{-subalgebra of } k\{G\} \}. \quad (2.2)$$

For $i \gg 0$ the finitely generated k -subalgebra $k[G[i]]$ of $k\{G\}$ has dimension e . Conversely, if R is a finitely generated k -subalgebra of $k\{G\}$, then R is contained in some $k[G[i]]$ and therefore $\dim(R) \leq e$. This proves (2.2). $\square$

Definition 2.2.8. Let G be a σ -algebraic group. The integer $d \geq 0$ defined in Theorem 2.2.7 above is called the σ -dimension of G and denoted by

$$\sigma\text{-dim}(G).$$

If $\sigma\text{-dim}(G) = 0$, the integer $e \geq 0$ defined in Theorem 2.2.7 is called the order of G and denoted by

$$\text{ord}(G).$$

If G has positive σ -dimension the order of G is defined to be infinity.

Example 2.2.9. Let $n \in \mathbb{N}$ and let G be the σ -closed subgroup of $\mathbb{G}_a^2$ given by

$$G(R) = \{ (g_1, g_2) \in R^2 \mid \sigma^n(g_1) = g_2 \}$$

for any k - σ -algebra R . For $i \geq 0$ let $G[i]$ denote the i -th order Zariski closure of G in $\mathbb{G}_a$. As $k\{G\} = k[y_1, \dots, \sigma^{n-1}(y_1), y_2, \sigma(y_2), \dots]$ we see that $\dim(G[i]) = (i+1) + n$ for $i \gg 0$. In particular, G has σ -dimension one.

Example 2.2.10. Let $\mathcal{G}$ be an algebraic group. Then $\sigma\text{-dim}([\sigma]_k \mathcal{G}) = \dim(\mathcal{G})$. Indeed, if we tautologically consider $G = [\sigma]_k \mathcal{G}$ as a σ -closed subgroup of $\mathcal{G}$, then $G[i] = \mathcal{G} \times \dots \times \sigma^i \mathcal{G}$ and so $\dim(G[i]) = \dim(\mathcal{G})(i+1)$ for every $i \geq 0$. This also shows that either $\text{ord}(G) = \infty$ (if $\dim(\mathcal{G}) > 0$) or $\text{ord}(G) = 0$ (if $\dim(\mathcal{G}) = 0$).

The following example motivates the naming “order”.

Example 2.2.11. Let $f = \sigma^n(y) + \lambda_{n-1}\sigma^{n-1}(y) + \dots + \lambda_0 y$ be a linear difference equation and G the σ -closed subgroup of $\mathbb{G}_a$ defined by f . Then $\text{ord}(G) = n$, i.e., the order of G equals the order of f .

Example 2.2.12. The σ -algebraic group from Example 2.2.3 has σ -dimension zero and order α_n .

Example 2.2.13. Let G be the σ -algebraic group from Example 2.1.12. Then $k\{G\} = k[\mathcal{G} \times \dots \times \sigma^{m-1} \mathcal{G}]$ and therefore $\sigma\text{-dim}(G) = 0$ and $\text{ord}(G) = m \dim(\mathcal{G})$.

Example 2.2.14. The σ -algebraic group from Example 2.1.14 has σ -dimension zero and order equal to the dimension of $\mathcal{G}$.

Example 2.2.15. The σ -algebraic group from Example 2.1.15 has σ -dimension zero and order zero.

A certain numerical invariant analogous to the order and called the total dimension has been introduced in [Hru04] in a different setting. We have chosen to stick to the more traditional naming from [Lev08] and [Coh65]. From the proof of Theorem 2.2.7, we immediately obtain:

Corollary 2.2.16. *Let G be a σ -algebraic group. Then the dimension of the growth group of G with respect to some σ -closed embedding $G \hookrightarrow \mathcal{G}$ of G into some algebraic group $\mathcal{G}$ equals the σ -dimension of G . In particular, the dimension of the growth group does not depend on the choice of the σ -closed embedding $G \hookrightarrow \mathcal{G}$. $\square$*

Recall (Definition 1.2.4) that a σ -algebraic group G is called integral if $k\{G\}$ is an integral domain and σ -integral if $k\{G\}$ is a σ -domain. The field of fractions of a σ -domain is naturally a σ -field.

The σ -transcendence degree of a σ -field extension $K|k$ is the largest integer $n \geq 1$ such that the σ -polynomial ring $k\{y_1, \dots, y_n\}$ may be embedded into K . (If no such integer exists the σ -transcendence degree is infinite.) See Section 4.1 in [Lev08] for more details on the σ -transcendence degree. The following proposition shows that our notions of dimension and order generalize the classical notions. (See page 394 in [Lev08].)

Proposition 2.2.17. *If G is a σ -integral σ -algebraic group, then the σ -dimension of G equals the σ -transcendence degree of the field of fractions of $k\{G\}$ over k .*

If G is an integral σ -algebraic group, then the order of G equals the transcendence degree of the field of fractions of $k\{G\}$ over k .

Proof. Let us first assume that G is σ -integral and let us fix a σ -closed embedding $G \hookrightarrow \mathcal{G}$. Assume that $a = (a_1, \dots, a_n)$ generates $k[G[0]] \subset k\{G\}$ as a k -algebra. Let K denote the field of fractions of $k\{G\}$. Since G is σ -integral K is naturally a σ -field extension of k and a generates K as a σ -field extension of k . Since $\text{trdeg}(k(a, \dots, \sigma^i(a))|k) = \dim(G[i])$, we see that $d(t+1) + e$ (with d and e as in Theorem 2.2.7) is really just the difference dimension polynomial (Definition 4.2.2 in [Lev08]) of the σ -field extension $K|k$ associated with a . It follows from Theorem 4.2.1 (iii) in [Lev08] that $\sigma\text{-dim}(G) = d = \sigma\text{-trdeg}(K|k)$.

Now assume that G is integral. Let K denote the field of fractions of $k\{G\}$. If $\sigma\text{-dim}(G) > 0$, then it is clear from Theorem 2.2.7 that the transcendence degree of K over k is infinite. So $\text{ord}(G) = \text{trdeg}(K|k)$ in this case.

If $\sigma\text{-dim}(G) = 0$, the claim follows from equation (2.2) above. $\square$

Example 2.2.18. Let G be the σ -algebraic group from Example 2.1.13. Then the coordinate ring of G is $k\{G\} = k\{y\} \otimes_k k\{x, x^{-1}\}$. So G is σ -integral and the field of fractions of $k\{G\}$ is the field of fractions of a σ -polynomial ring in two σ -variables. Therefore the field of fractions of $k\{G\}$ has σ -transcendence degree two over k . (Cf. [Lev08, Prop. 4.1.6, p. 248].) Thus $\sigma\text{-dim}(G) = 2$ by Proposition 2.2.17.

The σ -dimension and the order is invariant under extension of the base σ -field.

Lemma 2.2.19. *Let G be a σ -algebraic group and k' a σ -field extension of k . Then $\sigma\text{-dim}(G_{k'}) = \sigma\text{-dim}(G)$ and $\text{ord}(G_{k'}) = \text{ord}(G)$.*

Proof. Let $\mathcal{G}$ be an algebraic group such that G is a σ -closed subgroup of $\mathcal{G}$. Then $G_{k'}$ is a σ -closed subgroup of $\mathcal{G}_{k'}$ and for $i \geq 0$ the i -th order Zariski closure $G_{k'}[i]$ of $G_{k'}$ in $\mathcal{G}_{k'}$ is obtained from the i -th order Zariski closure $G[i]$ of G in $\mathcal{G}$ by base extension, i.e., $G_{k'}[i] = G[i]_{k'}$. Now the claim of the lemma follows from the fact that the usual dimension is invariant under base extension. $\square$

For later use we record:

Lemma 2.2.20. *Let G and H be σ -algebraic groups. Then $G \times H$ is a σ -algebraic group with*

$$\sigma\text{-dim}(G \times H) = \sigma\text{-dim}(G) + \sigma\text{-dim}(H)$$

and

$$\text{ord}(G \times H) = \text{ord}(G) + \text{ord}(H).$$

Proof. Let $\mathcal{G}$ and $\mathcal{H}$ be algebraic groups containing G and H as σ -closed subgroups respectively. Then $G \times H$ is a σ -closed subgroup of $\mathcal{G} \times \mathcal{H}$ and the claim reduces to the similar formula for algebraic groups. $\square$

2.3 Finiteness theorems

There is no direct difference analog of Hilbert's basis theorem: There exist infinite strictly ascending chains of difference ideals in the σ -polynomial ring $k\{y_1, \dots, y_n\}$. (See [Coh65, Example 3, p. 73].) The Ritt-Raudenbush basis theorem in difference algebra ([RR39] or [Lev08, Theorem 2.5.11]) only asserts that every ascending chain of perfect difference ideals in $k\{y_1, \dots, y_n\}$ is finite. However, in our group theoretic setup the situation is better behaved. Indeed, in this section we will prove two important finiteness theorems. Let A be a finitely σ -generated k - σ -Hopf algebra. The first finiteness theorem (Theorem 2.3.1) asserts that every σ -Hopf ideal of A is finitely generated as a σ -ideal. The second finiteness theorem (Theorem 2.3.5) asserts that every k - σ -Hopf subalgebra of A is finitely σ -generated over k . In Chapter 4 we will prove a third finiteness theorem (Theorem 4.1.1): The set of minimal prime σ -ideals of A is finite.

Theorem 2.3.1. *Let H be a σ -algebraic group and $G \leq H$ a σ -closed subgroup. Then the defining ideal $\mathbb{I}(G) \subset k\{H\}$ of G is finitely generated as a σ -ideal.*

Proof. We may embed H as a σ -closed subgroup in some algebraic group $\mathcal{G}$. For example, we may choose $\mathcal{G} = \text{GL}_n$ by Theorem 2.1.17. If the defining ideal of G in $k\{H\}$ is finitely σ -generated, then also the defining ideal of G in $k\{H\} = k\{G\}/\mathbb{I}(H)$ is finitely σ -generated. We can therefore assume that $H = \mathcal{G}$.

As in Section 2.2 let $\mathcal{G}_i$ denote the kernel of the projection $\pi_i: G[i] \rightarrow G[i-1]$ between the Zariski closures of G in $\mathcal{G}$. By Proposition 2.2.1 there exists an integer $m \geq 1$ such that $\sigma_i: \mathcal{G}_i \rightarrow {}^\sigma(\mathcal{G}_{i-1})$ is an isomorphism for every $i > m$. To prove the theorem we will show that $\mathbb{I}(G[m]) = \mathbb{I}(G) \cap k[\mathcal{G}[m]]$ σ -generates $\mathbb{I}(G) \subset k\{G\} = \cup_{i \geq 0} k[\mathcal{G}[i]]$. To do this it is sufficient to show that

$$\mathbb{I}(G[i]) = (\mathbb{I}(G[i-1]), \sigma(\mathbb{I}(G[i-1]))) \subset k[\mathcal{G}[i]] \quad (2.3)$$

for $i > m$. The ideal to the right-hand side of (2.3) defines an algebraic group

$$\mathcal{H}_i = (G[i-1] \times {}^{\sigma^i}\mathcal{G}) \cap (\mathcal{G} \times {}^\sigma(G[i-1])) \leq \mathcal{G}[i] = \mathcal{G} \times {}^\sigma\mathcal{G} \times \dots \times {}^{\sigma^i}\mathcal{G}.$$

Clearly $G[i] \leq \mathcal{H}_i$ and the projection $\pi_i: \mathcal{H}_i \rightarrow G[i-1]$ is surjective³. The kernel of $\pi_i: \mathcal{H}_i \rightarrow G[i-1]$ is $1 \times {}^\sigma(\mathcal{G}_{i-1})$. Since $i > m$ we have $1 \times {}^\sigma(\mathcal{G}_{i-1}) = \mathcal{G}_i$. Thus the

³A morphism $\mathcal{G} \rightarrow \mathcal{H}$ of algebraic groups, i.e., affine group schemes of finite type over k is surjective if the dual map $k[\mathcal{H}] \rightarrow k[\mathcal{G}]$ is injective. See [Mil12, Chapter VII, Section 7] for more details.

downwards arrows in the commutative diagram

$$\begin{array}{ccc} G[i] & \xrightarrow{\quad} & \mathcal{H}_i \\ & \searrow \pi_i \quad \swarrow \pi_i & \\ & G[i-1] & \end{array}$$

have the same kernel. This implies that $G[i] = \mathcal{H}_i$ and identity (2.3) is proved. $\square$

We have actually proved a slightly stronger statement which we record for later use.

Corollary 2.3.2. *Let $\mathcal{G}$ be an algebraic group and $G \leq \mathcal{G}$ a σ -closed subgroup. For $i \geq 0$ let $G[i]$ denote the i -th order Zariski closure of G in $\mathcal{G}$. Then there exists an integer $m \geq 0$ such that $\mathbb{I}(G[i]) = (\mathbb{I}(G[i-1]), \sigma(\mathbb{I}(G[i-1])))$ for $i > m$, i.e., $G[i] = (G[i-1] \times {}^\sigma \mathcal{G}) \cap (\mathcal{G} \times {}^\sigma(G[i-1]))$. $\square$*

Corollary 2.3.3. *Every descending chain of σ -closed subgroups of a σ -algebraic group is finite.*

Proof. A descending chain $H_1 \geq H_2 \geq \dots$ of σ -closed subgroups of a σ -algebraic group G corresponds to an ascending chain $\mathbb{I}(H_1) \subset \mathbb{I}(H_2) \subset \dots$ of σ -Hopf ideals in $k\{G\}$. By Theorem 2.3.1 the union $\bigcup \mathbb{I}(H_i)$ (which corresponds to the intersection $\bigcap H_i$) is finitely generated as a σ -ideal. Thus there exists an integer $n \geq 1$ such that $\bigcup \mathbb{I}(H_i) = \mathbb{I}(H_n)$. Then $H_n = H_{n+1} = \dots$. $\square$

To prove the second finiteness theorem we need a simple lemma on k - σ -Hopf algebras.

Lemma 2.3.4. *Let A be a k - σ -Hopf algebra. Then every finite subset of A is contained in a finitely σ -generated k - σ -Hopf subalgebra.*

Proof. By [Wat79, Section 3.3] a finite subset of A is contained in a Hopf subalgebra B that is finitely generated as a k -algebra. Then $k\{B\} \subset A$ is finitely σ -generated over k and since the comultiplication and the antipode are σ -morphisms, $k\{B\}$ is a Hopf subalgebra. $\square$

Theorem 2.3.5. *Let A be a k - σ -Hopf algebra that is finitely σ -generated over k and $B \subset A$ a k - σ -Hopf subalgebra. Then B is finitely σ -generated over k .*

Proof. For a Hopf subalgebra C of A let $\mathfrak{m}_C \subset C$ denote the kernel of the counit $\varepsilon: C \rightarrow k$. The ideal $(\mathfrak{m}_B) \subset A$ is a σ -Hopf ideal. By Theorem 2.3.1 it is finitely σ -generated. So there exists a finite set $F \subset \mathfrak{m}_B$ such that $[F] = (\mathfrak{m}_B)$. By Lemma 2.3.4 there exists a finitely σ -generated k - σ -Hopf subalgebra C of B containing F . Then $(\mathfrak{m}_C) = (\mathfrak{m}_B)$. By Corollary 3.10 in [Tak72] the mapping $C \mapsto (\mathfrak{m}_C)$ from Hopf subalgebras to Hopf ideals is injective. Thus $B = C$ is finitely σ -generated over k . $\square$

As an application of Corollary 2.3.2, we will prove a dimension theorem, which will then be used in Section 5.3 in the proof of an analog of the Jordan-Hölder theorem. A dimension theorem for differential algebraic groups has been proved in [Sit74]. It is interesting to note that the dimension theorem fails for difference varieties. See [Coh65, Chapter 8, Section 8]. However, it holds for σ -algebraic groups:

Theorem 2.3.6. *Let H_1 and H_2 be σ -closed subgroups of a σ -algebraic group G . Then*

$$\sigma\text{-dim}(H_1 \cap H_2) + \sigma\text{-dim}(G) \geq \sigma\text{-dim}(H_1) + \sigma\text{-dim}(H_2) \quad (2.4)$$

and

$$\text{ord}(H_1 \cap H_2) + \text{ord}(G) \geq \text{ord}(H_1) + \text{ord}(H_2). \quad (2.5)$$

Proof. Let $\mathcal{G}$ be an algebraic group containing G as a σ -closed subgroup. We consider the Zariski closures inside $\mathcal{G}$. By Corollary 2.3.2 there exists an integer $m \geq 0$ such that

$$\mathbb{I}((H_1 \cap H_2)[i]) = (\mathbb{I}((H_1 \cap H_2)[i-1]), \sigma(\mathbb{I}((H_1 \cap H_2)[i-1])))$$

for $i > m$. Since $\mathbb{I}(H_1 \cap H_2) = \mathbb{I}(H_1) + \mathbb{I}(H_2)$ there exists $n \geq m$ such that

$$\mathbb{I}((H_1 \cap H_2)[m]) \subset \mathbb{I}(H_1[n]) + \mathbb{I}(H_2[n]) = \mathbb{I}(H_1[n] \cap H_2[n]).$$

But then

$$\mathbb{I}((H_1 \cap H_2)[m+i]) \subset \mathbb{I}(H_1[n+i] \cap H_2[n+i]) \quad (2.6)$$

for every $i \geq 0$ and so

$$H_1[n+i] \cap H_2[n+i] \leq (H_1 \cap H_2)[m+i] \times \sigma^{m+i+1}\mathcal{G} \times \cdots \times \sigma^{n+i}\mathcal{G}.$$

Therefore

$$\dim(H_1[n+i] \cap H_2[n+i]) \leq \dim((H_1 \cap H_2)[m+i]) + (n-m)\dim(\mathcal{G})$$

and so

$$\begin{aligned} \dim((H_1 \cap H_2)[m+i]) &\geq \dim(H_1[n+i] \cap H_2[n+i]) - (n-m)\dim(\mathcal{G}) \\ &\geq \dim(H_1[n+i]) + \dim(H_2[n+i]) - \dim(G[n+i]) - (n-m)\dim(\mathcal{G}). \end{aligned}$$

Now using Theorem 2.2.7 and comparing the coefficients of i yields identity (2.4).

It remains to prove (2.5). Obviously this is true if $\text{ord}(G) = \infty$. So we can assume $\text{ord}(G) < \infty$, i.e., $\sigma\text{-dim}(G) = 0$. Note that (2.6) implies that the intersection of $\mathbb{I}(H_1[n+i] \cap H_2[n+i])$ with $k[\mathcal{G}[m+i]]$ equals $\mathbb{I}((H_1 \cap H_2)[m+i])$. This means that the morphism of algebraic groups

$$\phi: H_1[n+i] \cap H_2[n+i] \rightarrow (H_1 \cap H_2)[m+i]$$

induced from the projection $\mathcal{G} \times \sigma\mathcal{G} \times \cdots \times \sigma^{n+i}\mathcal{G} \rightarrow \mathcal{G} \times \sigma\mathcal{G} \times \cdots \times \sigma^{m+i}\mathcal{G}$ is surjective. Since $\sigma\text{-dim}(H_1) = 0$, the kernel of the projections $H_1[n+i] \twoheadrightarrow H_1[m+i]$ is finite for $i \gg 0$. Therefore also ϕ has finite kernel and it follows that for $i \gg 0$

$$\begin{aligned} \text{ord}(H_1 \cap H_2) &= \dim((H_1 \cap H_2)[m+i]) = \dim(H_1[n+i] \cap H_2[n+i]) \\ &\geq \dim(H_1[n+i]) + \dim(H_2[n+i]) - \dim(G[n+i]) \\ &= \text{ord}(H_1) + \text{ord}(H_2) - \text{ord}(G). \end{aligned}$$

□

2.4 The limit degree

In this section we introduce an important numerical invariant for σ -algebraic groups (of σ -dimension zero) called the limit degree. We also show that the category of algebraic σ -groups introduced and studied in [KP07] is equivalent to the category of σ -algebraic groups of σ -dimension zero and limit degree one.

By the *size* $|\mathcal{G}|$ of an algebraic group $\mathcal{G}$ we mean the dimension of $k[\mathcal{G}]$ as a k -vector space. So the size is either a non-negative integer or ∞ . In the sequel we will employ the usual rules for calculating with the symbol ∞ . If $\mathcal{G}_1 \xrightarrow{\phi_1} \mathcal{G}_2 \xrightarrow{\phi_2} \mathcal{G}_3$ are surjective morphisms of algebraic groups, then

$$|\ker(\phi_2 \circ \phi_1)| = |\ker(\phi_2)| \cdot |\ker(\phi_1)|. \quad (2.7)$$

Proposition 2.4.1. *Let G be a σ -algebraic group and $G \hookrightarrow \mathcal{G}$ a σ -closed embedding. Then the size of the growth group of G with respect to the embedding $G \hookrightarrow \mathcal{G}$ does not depend on the choice of $\mathcal{G}$ and the σ -closed embedding.*

Proof. For $i \geq 0$ let $G[i]$ denote the i -th order Zariski closure of G in $\mathcal{G}$ and $\mathcal{G}_i$ the kernel of the projection $\pi_i: G[i] \rightarrow G[i-1]$. By Proposition 2.2.1 the integer $d = |\mathcal{G}_i|$ does not depend on i for $i \gg 0$. Let $a = (a_1, \dots, a_n)$ generate $k[G[0]] \subset k\{G\}$ as a k -algebra. Then a generates $k\{G\}$ as a k - σ -algebra.

Let $\mathcal{G}'$ be another algebraic group and $G \hookrightarrow \mathcal{G}'$ a σ -closed embedding. Let $G[i]'$ denote the i -th order Zariski closure of G in $\mathcal{G}'$ and let d' and a' be as above. We have to show that $d = d'$.

Since a , as well as a' , σ -generate $k\{G\}$, there exists an integer $m \geq 1$ such that $a' \in k[a, \dots, \sigma^m(a)]$ and $a \in k[a', \dots, \sigma^m(a')]$. Then, for $i \geq 0$, we have $k[a', \dots, \sigma^i(a')] \subset k[a, \dots, \sigma^{m+i}(a)]$ and $k[a, \dots, \sigma^i(a)] \subset k[a', \dots, \sigma^{m+i}(a')]$. So for $j \geq m$:

$$k[a, \dots, \sigma^i(a)] \subset k[a', \dots, \sigma^{m+i}(a')] \subset k[a', \dots, \sigma^{j+i}(a')] \subset k[a, \dots, \sigma^{m+j+i}(a)].$$

These inclusions of Hopf algebras correspond to surjective morphisms of algebraic groups

$$G[m+j+i] \twoheadrightarrow G[j+i]' \twoheadrightarrow G[m+i]' \twoheadrightarrow G[i].$$

We have $|\ker(G[m+j+i] \twoheadrightarrow G[i])| \geq |\ker(G[j+i]' \twoheadrightarrow G[m+i]')|$ by (2.7). But by (2.7) and Proposition 2.2.1 we also have

$$|\ker(G[m+j+i] \twoheadrightarrow G[i])| = d^{m+j} \quad \text{and} \quad |\ker(G[j+i]' \twoheadrightarrow G[m+i]')| = d'^{j-m}$$

for $i \gg 0$. Consequently, $d^{m+j} \geq d'^{j-m}$. Letting j tend to infinity, we find $d \geq d'$. By symmetry, $d = d'$. $\square$

Definition 2.4.2. *Let G be a σ -algebraic group. Choose an algebraic group $\mathcal{G}$ and a σ -closed embedding $G \hookrightarrow \mathcal{G}$. The size of the growth group of G with respect to the σ -closed embedding $G \hookrightarrow \mathcal{G}$ is called the limit degree of G and is denoted by*

$$\text{ld}(G).$$

By Proposition 2.4.1 the limit degree of G does not depend on the choice of $\mathcal{G}$ and the σ -closed embedding $G \hookrightarrow \mathcal{G}$.

The expression “limit degree” is motivated by the fact that

$$\text{ld}(G) = \lim_{i \rightarrow \infty} \deg(\pi_i),$$

where $\deg(\pi_i)$ denotes the degree of the projection $\pi_i: G[i] \twoheadrightarrow G[i-1]$. The naming is also motivated by Proposition 2.4.7.

Remark 2.4.3. *By Corollary 2.2.16 the limit degree of a σ -algebraic group is finite if and only if it has σ -dimension zero.*

Example 2.4.4. Let $0 \leq \alpha_1 < \dots < \alpha_n$ and $1 \leq \beta_1, \dots, \beta_n$ be integers and $G \leq \mathbb{G}_m$ the σ -closed subgroup of the multiplicative group $\mathbb{G}_m$ given by

$$G(R) = \{g \in R^\times \mid \sigma^{\alpha_1}(g)^{\beta_1} \dots \sigma^{\alpha_n}(g)^{\beta_n} = 1\}$$

for every k - σ -algebra R . Then $\text{ld}(G) = \beta_n$ by Example 2.2.3.

Example 2.4.5. By Example 2.2.4 the limit degree of a σ -closed subgroup of $\mathbb{G}_a$ defined by a linear difference equation is one.

Example 2.4.6. Let $\mathcal{G}$ be an algebraic group. Then $\text{ld}([\sigma]_k \mathcal{G}) = |\mathcal{G}|$ by Example 2.2.5.

Let $K|k$ be an extension of σ -fields. Assume that there exists a finite set $B \subset K$ such that $B, \sigma(B), \dots$ generates K as a field extension of k , then the limit degree $\text{ld}(K|k)$ is the limit $\lim_{i \rightarrow \infty} d_i$, where d_i is the degree of the field extension

$$k(B, \dots, \sigma^i(B))|k(B, \dots, \sigma^{i-1}(B)).$$

The limit exists and does not depend on the choice of B ([Lev08, Section 4.3]). The following proposition shows that our definition of the limit degree generalizes the classical definition ([Lev08, p. 394]) of the limit degree (for irreducible difference varieties in the sense of [Coh65] and [Lev08]).

Proposition 2.4.7. *Let G be a σ -algebraic group. If G is σ -integral, then the limit degree of G equals the limit degree of the field of fractions of $k\{G\}$ over k .*

Proof. Let $\mathcal{G}$ be an algebraic group containing G as a σ -closed subgroup. For $i \geq 0$ let $G[i]$ denote the i -th order Zariski closure of G in $\mathcal{G}$ and let $B \subset k[G[0]]$ be a finite set which generates $k[G[0]] \subset k\{G\}$ as a k -algebra. Let K denote the field of fractions of $k\{G\}$. Then $B, \sigma(B), \dots$ generates K as a field extension of k and $k(B, \sigma(B), \dots, \sigma^i(B))$ is the field of fractions of $k[G[i]]$. Therefore the degree of the field extension

$$k(B, \dots, \sigma^i(B))|k(B, \dots, \sigma^{i-1}(B))$$

equals the degree of the projection $G[i] \twoheadrightarrow G[i-1]$. □

Our next aim is to characterize the algebraic σ -groups introduced in [KP07] within the category of σ -algebraic groups.

Proposition 2.4.8. *Let G be a σ -algebraic group. Then $\text{ld}(G) = 1$ if and only if $k\{G\}$ is finitely generated as a k -algebra.*

Proof. Fix a σ -closed embedding $G \hookrightarrow \mathcal{G}$ and let $G[i]$ denote the i -th order Zariski closure of G in $\mathcal{G}$. So $k\{G\} = \cup_{i \geq 0} k[G[i]]$. If $\text{ld}(G) = 1$ there exists an integer $m \geq 0$ such that $\pi_i: G[i] \rightarrow G[i-1]$ has trivial kernel for $i > m$, so π_i is an isomorphism and therefore $k[G[i]] = k[G[i-1]]$. Consequently, $k\{G\} = k[G[m]]$ is finitely generated as a k -algebra.

Conversely, if $k\{G\}$ is a finitely generated k -algebra, we can consider the algebraic group $\mathcal{G}$ associated with the Hopf algebra $k\{G\}^\#$. So $k[\mathcal{G}] = k\{G\}^\#$. Let R be a k - σ -algebra. Since $G(R) = \text{Hom}(k\{G\}, R)$ is a subgroup of

$$\text{Hom}(k\{G\}^\#, R^\#) = \mathcal{G}(R^\#) = ([\sigma]_k \mathcal{G})(R) = \text{Hom}(k\{\mathcal{G}\}, R)$$

the morphism $k\{\mathcal{G}\} \rightarrow k\{G\}$ of k - σ -algebras induced by Lemma 1.2.8 is a morphism of k - σ -Hopf algebras. With respect to the corresponding σ -closed embedding $G \hookrightarrow \mathcal{G}$ we have $k\{G\} = k[G[0]] = k[G[1]] = \dots$ and therefore the associated growth group is trivial. Thus $\text{ld}(G) = 1$. $\square$

Example 2.4.9. It is clear from Proposition 2.4.8 that the σ -algebraic groups in Examples 2.1.12, 2.1.14 and 2.1.15 have limit degree one.

Let us now recall the definition of algebraic σ -groups from [KP07]. We start by introducing algebraic σ -varieties. Let k be a σ -field and $\mathcal{X}$ a variety over k , where, for our purposes, a variety over k is an affine scheme of finite type over k . As in Section 1.2.4 let ${}^\sigma\mathcal{X}$ denote the variety over k obtained from $\mathcal{X}$ by base extension via $\sigma: k \rightarrow k$. Similarly, if $\phi: \mathcal{X} \rightarrow \mathcal{Y}$ is a morphism of varieties over k , then ${}^\sigma\phi: {}^\sigma\mathcal{X} \rightarrow {}^\sigma\mathcal{Y}$ is the morphism obtained from ϕ by base extension via $\sigma: k \rightarrow k$.

An *algebraic σ -variety* over k is a variety $\mathcal{X}$ over k together with a morphism $\tilde{\sigma}: \mathcal{X} \rightarrow {}^\sigma\mathcal{X}$ of varieties over k . A morphism between algebraic σ -varieties is a morphism $\phi: \mathcal{X} \rightarrow \mathcal{Y}$ of varieties such that

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{\tilde{\sigma}} & {}^\sigma\mathcal{X} \\ \phi \downarrow & & \downarrow {}^\sigma\phi \\ \mathcal{Y} & \xrightarrow{\tilde{\sigma}} & {}^\sigma\mathcal{Y} \end{array}$$

commutes. An *algebraic σ -group* is a group object in the category of algebraic σ -varieties. Equivalently, an algebraic σ -group is an algebraic group $\mathcal{G}$ over k together with a morphism $\tilde{\sigma}: \mathcal{G} \rightarrow {}^\sigma\mathcal{G}$ of algebraic groups.

Theorem 2.4.10. *The category of algebraic σ -groups is equivalent to the category of σ -algebraic groups of σ -dimension zero and limit degree one.*

Proof. Let R be a k -algebra. To define a k - σ -algebra structure on R is equivalent to defining a morphism of k -algebras $\bar{\sigma}: {}^\sigma R \rightarrow R$. Given $\sigma: R \rightarrow R$, we can define

$$\bar{\sigma}: {}^\sigma R \rightarrow R, \quad r \otimes \lambda \mapsto \sigma(r)\lambda.$$

Conversely, given $\bar{\sigma}: {}^\sigma R \rightarrow R$, we can define $\sigma: R \xrightarrow{\text{id} \otimes 1} R \otimes_k k = {}^\sigma R \xrightarrow{\bar{\sigma}} R$. Moreover, if R and S are k - σ -algebras and $\psi: R \rightarrow S$ is a morphism of k -algebras, then ψ is a morphism of k - σ -algebras if and only if

$$\begin{array}{ccc} {}^\sigma R & \xrightarrow{\bar{\sigma}} & R \\ \sigma\psi \downarrow & & \downarrow \psi \\ {}^\sigma S & \xrightarrow{\bar{\sigma}} & S \end{array}$$

commutes.

Dualizing the definition, an algebraic σ -group $\mathcal{G}$ corresponds to a finitely generated Hopf algebra $k[\mathcal{G}]$ together with a morphism of Hopf algebras $\bar{\sigma} = (\tilde{\sigma})^*: {}^\sigma(k[\mathcal{G}]) \rightarrow k[\mathcal{G}]$. By the remark from the beginning of the proof, the statement that $\bar{\sigma}$ is a morphism of Hopf algebras corresponds to the statement that $k[\mathcal{G}]$ is a k - σ -Hopf algebra. Thus the category of algebraic σ -groups is anti-equivalent to the category of k - σ -Hopf algebras that are finitely generated over k . Now the claim follows from Proposition 2.1.3 and Proposition 2.4.8. $\square$

2.5 Subgroups defined by ideal closures

If $\mathcal{G}$ is an algebraic group over a perfect field, then $\mathcal{G}_{\text{red}}$, the associated reduced scheme, is a closed subgroup of $\mathcal{G}$. In difference algebra, there are several closure operations one can define on difference ideals that are in some way similar to taking the radical of an ideal. Therefore we obtain several σ -closed subgroups of a σ -algebraic group that are in some way analogous to $\mathcal{G}_{\text{red}}$. Let us now recall these closure operations on σ -ideals. (Cf. Definition 1.1.2 and [Lev08, Section 2.3].)

Definition 2.5.1. *Let R be a σ -ring and $\mathfrak{a} \subset R$ a σ -ideal. Then $\mathfrak{a}$ is called*

- reflexive if $\sigma^{-1}(\mathfrak{a}) = \mathfrak{a}$, i.e., $\sigma(f) \in \mathfrak{a}$ implies $f \in \mathfrak{a}$.
- mixed if $fg \in \mathfrak{a}$ implies $f\sigma(g) \in \mathfrak{a}$.
- perfect if $\sigma^{\alpha_1}(f) \cdots \sigma^{\alpha_n}(f) \in \mathfrak{a}$ implies $f \in \mathfrak{a}$ for $\alpha_1, \dots, \alpha_n \geq 0$

A σ -ring whose zero ideal is reflexive / mixed / perfect is called σ -reduced / well-mixed / perfectly σ -reduced. Note that a σ -ring that is an integral domain is well-mixed. If it is additionally σ -reduced, i.e., a σ -domain, it is perfectly σ -reduced.

Let $\mathfrak{a}$ be a σ -ideal of a σ -ring R . Since the intersection of reflexive / radical mixed / perfect σ -ideals is a reflexive / radical mixed / perfect σ -ideal there exists a smallest reflexive / radical mixed / perfect σ -ideal of R containing $\mathfrak{a}$. It is called the reflexive closure $\mathfrak{a}^*$ / the radical mixed closure $\{\mathfrak{a}\}_{\text{wm}}$ / the perfect closure $\{\mathfrak{a}\}$ of $\mathfrak{a}$.

It is easy to see that

$$\mathfrak{a}^* = \{f \in R \mid \exists n \in \mathbb{N} : \sigma^n(f) \in \mathfrak{a}\}.$$

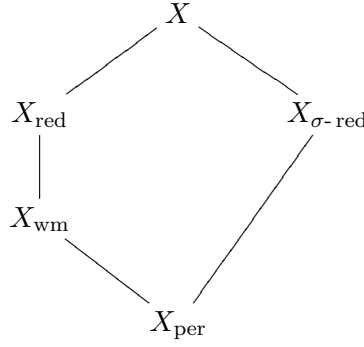
The radical mixed closure and the perfect closure of $\mathfrak{a}$ do not have such a simple elementwise description. Cf. [Lev08, Section 2.3, p. 121ff] and [Lev, Lemma 3.1].

Let X be a σ -variety. We say that X is reduced / σ -reduced / reduced well-mixed / perfectly σ -reduced if $k\{X\}$ has this property. There exists a unique largest σ -closed σ -subvariety

$$X_{\text{red}} / X_{\sigma\text{-red}} / X_{\text{wm}} / X_{\text{per}}$$

of X that is reduced / σ -reduced / reduced well-mixed / perfectly σ -reduced. Its defining ideal is the radical / reflexive closure / radical mixed closure / perfect closure of the zero ideal of $k\{X\}$.

A perfect σ -ideal is radical, mixed and reflexive. Therefore we have the following diagram of inclusions of σ -closed σ -subvarieties of X .



The importance of perfectly σ -reduced σ -varieties stems from the fact that they correspond to the classical difference varieties as studied in [Coh65] and [Lev08], where one is only looking for solutions in σ -field extensions of k . (See Subsection 1.3.1.) Mixed σ -ideals play a crucial role in the theory of difference schemes as developed by E. Hrushovski in [Hru04]. (Cf. 1.3.2). Note that for an arbitrary non-empty σ -variety X_{per} and X_{wm} might be empty. Take for example $k\{X\} = k \times k$ with $\sigma((a, b)) = (\sigma(b), \sigma(a))$. This pathology does not occur for σ -algebraic groups because $\mathfrak{m}_G \subset k\{G\}$ is a σ -prime ideal.

Example 2.5.2. Let k be a σ -field, G a finite group and $\sigma: G \rightarrow G$ a group endomorphism. Let G be the σ -algebraic group from Example 2.1.15. Then G is σ -reduced if and only if σ is an automorphism. Moreover, G is reduced well-mixed if and only if it is perfectly σ -reduced if and only if $\sigma: G \rightarrow G$ is the identity map.

Remark 2.5.3. For a σ -algebraic group G the following statements are equivalent:

- (i) $G(K) = 1$ for every σ -field extension K of k .
- (ii) $G_{\text{per}} = 1$.
- (iii) The ideal $\mathfrak{m}_G$ is the only σ -prime ideal of $k\{G\}$.

Proof. If $g \in G(K) = \text{Hom}(k\{G\}, K)$, then the kernel of g is a σ -prime ideal of $k\{G\}$. Conversely, if $\mathfrak{p}$ is a σ -prime ideal of $k\{G\}$, then the field of fractions K of $k\{G\}/\mathfrak{p}$ is naturally a σ -field and the canonical map $g: k\{G\} \rightarrow K$ belongs to $G(K)$. Therefore (i) and (iii) are equivalent. The equivalence with (ii) follows from the fact that a perfect difference ideal is the intersection of σ -prime ideals ([Coh65, Chapter 3, p. 88]). $\square$

If $\psi: R \rightarrow S$ is a morphism of σ -rings, it is easy to check that $\psi^{-1}(\mathfrak{a})$ is a radical / reflexive / radical mixed / perfect σ -ideal if $\mathfrak{a}$ has the corresponding property. This shows that ψ maps the radical / reflexive closure / radical mixed closure / perfect closure of the zero ideal of R into the radical / reflexive closure / radical mixed closure / perfect closure of the zero ideal of S . Therefore a morphism of σ -varieties $X \rightarrow Y$ induces a morphism

$$X_{\text{red}} \rightarrow Y_{\text{red}} / X_{\sigma\text{-red}} \rightarrow Y_{\sigma\text{-red}} / X_{\text{wm}} \rightarrow Y_{\text{wm}} / X_{\text{per}} \rightarrow Y_{\text{per}}.$$

For later use we record a lemma on perfectly σ -reduced σ -varieties.

Lemma 2.5.4. Let $\phi: X \rightarrow Y$ be a morphism of σ -varieties and let $Z \subset Y$ be a σ -closed σ -subvariety. Assume that X is perfectly σ -reduced. If $\phi_K(X(K)) \subset Z(K)$ for every σ -field extension K of k , then $\phi(X) \subset Z$, i.e., ϕ factors through $Z \hookrightarrow Y$.

Proof. We have to show that $\mathbb{I}(Z) \subset k\{Y\}$ lies in the kernel of $\phi^*: k\{Y\} \rightarrow k\{X\}$. So let $f \in \mathbb{I}(Z)$. We have to show that $\phi^*(f) = 0$. Since the zero ideal of $k\{X\}$ is perfect, it is the intersection of σ -prime ideals ([Coh65, Chapter 3, p. 88]). Therefore, it suffices to show that $\phi^*(f)$ lies in every σ -prime ideal of $k\{X\}$. Let $\mathfrak{p} \subset k\{X\}$ be a σ -prime ideal, then the field of fractions K of $k\{X\}/\mathfrak{p}$ naturally is a σ -field and the canonical map $x: k\{X\} \rightarrow K$ is a morphism of k - σ -algebras. By assumption, $\phi_K(x) \in Z(K)$, i.e., $\mathbb{I}(Z)$ lies in the kernel of $x \circ \phi^*$. So $\phi^*(f) \in \mathfrak{p}$. $\square$

Lemma 2.5.5. *Let R and S be k - σ -algebras.*

- (i) *If k is perfect and R and S are reduced, then $R \otimes_k S$ is reduced.*
- (ii) *If k is inversive and R and S are σ -reduced, then $R \otimes_k S$ is σ -reduced.*
- (iii) *If k is algebraically closed and R and S are well-mixed and reduced, then $R \otimes_k S$ is well-mixed and reduced.*
- (iv) *If k is inversive and algebraically closed and R and S are perfectly σ -reduced, then $R \otimes_k S$ is perfectly σ -reduced.*

Proof. Of course (i) is well-known. See e.g., [Bou90, Theorem 3, Chapter V, §15.5, A.V.125]. Note that (i) is a special case of (ii) as we may take σ as the Frobenius endomorphism. For (ii), note that R and S are σ -separable over k by Proposition 1.1.8 and therefore $R \otimes_k S$ is σ -separable (in particular σ -reduced) by Corollary 1.1.10.

For (iii), note that the zero ideal of a reduced well-mixed σ -ring is the intersection of prime σ -ideals ([Hru04, Lemma 2.10]). If $\mathfrak{p}$ is a prime σ -ideal of R and $\mathfrak{q}$ a prime σ -ideal of S , then $\mathfrak{p} \otimes S + R \otimes \mathfrak{q}$ is a prime σ -ideal of $R \otimes_k S$ since

$$(R \otimes_k S)/(\mathfrak{p} \otimes S + R \otimes \mathfrak{q}) = R/\mathfrak{p} \otimes_k S/\mathfrak{q}$$

and the latter is an integral domain, as the tensor product of integral domains over an algebraically closed field is again an integral domain ([Bou90, Corollary 3, Chapter V, §17.5, A.V.143]). We see that the zero ideal of $R \otimes_k S$ is the intersection of prime σ -ideals of the form $\mathfrak{p} \otimes S + R \otimes \mathfrak{q}$. This shows that $R \otimes_k S$ is well-mixed and reduced.

To prove (iv) we can proceed as in (iii) by noting that a σ -ideal is perfect if and only if it is the intersection of σ -prime ideals and that the tensor product of σ -domains over an inversive algebraically closed σ -field is again a σ -domain by (ii). $\square$

There are counterexamples which show that the conditions on k in Lemma 2.5.5 cannot be relaxed. For example, take $k = \mathbb{R}$ with σ the identity map, $R = \mathbb{C}$ with the identity map and $S = \mathbb{C}$ with σ complex conjugation. Then R and S are perfectly σ -reduced (hence well-mixed) but $R \otimes_k S$ is not well-mixed (hence not perfectly σ -reduced).

If X and Y are σ -varieties, the canonical map $(X \times Y)_{\text{per}} \rightarrow X_{\text{per}} \times Y_{\text{per}}$ need not be an isomorphism as $X_{\text{per}} \times Y_{\text{per}}$ need not be perfectly σ -reduced.

Corollary 2.5.6. *Let X and Y be σ -varieties.*

- (i) *If k is perfect, then $(X \times Y)_{\text{red}} \simeq X_{\text{red}} \times Y_{\text{red}}$.*
- (ii) *If k is inversive, then $(X \times Y)_{\sigma\text{-red}} \simeq X_{\sigma\text{-red}} \times Y_{\sigma\text{-red}}$.*
- (iii) *If k is algebraically closed, then $(X \times Y)_{\text{wm}} \simeq X_{\text{wm}} \times Y_{\text{wm}}$.*

(iv) If k is inversive and algebraically closed, then $(X \times Y)_{\text{per}} \simeq X_{\text{per}} \times Y_{\text{per}}$.

Proof. Exemplarily, let us proof (iv). In terms of k - σ -algebras, we have to show that the canonical map

$$k\{X\}/\{0\} \otimes_k k\{Y\}/\{0\} \rightarrow (k\{X\} \otimes_k k\{Y\})/\{0\}$$

is an isomorphism. As the left hand side is perfectly σ -reduced by Lemma 2.5.5, we see that $\{0\} = \{0\} \otimes k\{Y\} + k\{X\} \otimes \{0\}$. $\square$

Corollary 2.5.7. *Let G be a σ -algebraic group.*

- (i) *If k is perfect, then G_{red} is a σ -closed subgroup of G .*
- (ii) *If k is inversive, then $G_{\sigma\text{-red}}$ is a σ -closed subgroup of G .*
- (iii) *If k is algebraically closed, then G_{wm} is a σ -closed subgroup of G .*
- (iv) *If k is inversive and algebraically closed, then G_{per} is a σ -closed subgroup of G .*

Proof. Again, let us restrict to (iv). The other cases are similar. The multiplication morphism $G \times G \rightarrow G$ induces a morphism $(G \times G)_{\text{per}} \rightarrow G_{\text{per}}$. But by Corollary 2.5.6, the σ -closed σ -subvariety $(G \times G)_{\text{per}}$ of $G \times G$ can be identified with $G_{\text{per}} \times G_{\text{per}} \subset G \times G$. Therefore, the multiplication maps $G_{\text{per}} \times G_{\text{per}}$ into G_{per} . As the inversion $G \rightarrow G$, $g \mapsto g^{-1}$ also passes to G_{per} , we see that G_{per} is a subgroup of G . $\square$

Example 2.5.8. For all the σ -algebraic groups G in Example 4.1.2 G_{per} is the trivial group.

Example 2.5.9. Let $\mathbf{G}$ be a finite group and $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ an endomorphism. Let G be the σ -algebraic group associated to this data as in Example 2.1.15. For $g \in \mathbf{G}$ we have $\sigma^n(e_g) = 0$ if and only if $g \notin \sigma^n(\mathbf{G})$ and so $\mathbb{I}(G_{\sigma\text{-red}}) = (e_g \mid g \notin \cap_{n \in \mathbb{N}} \sigma^n(\mathbf{G})) \subset k\{G\}$. Thus $G_{\sigma\text{-red}}$ corresponds to the subgroup $H = \cap_{n \in \mathbb{N}} \sigma^n(\mathbf{G})$ of $\mathbf{G}$.

The following example shows that $G_{\sigma\text{-red}}$ need to be a subgroup if k is not inversive.

Example 2.5.10. Let k be a σ -field of characteristic zero which is not inversive. So there exists $\lambda \in k$ with $\lambda \notin \sigma(k)$. Let G be the σ -closed subgroup of $\mathbb{G}_a$ given by

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

for any k - σ -algebra R . We will first show that G has no proper, non-trivial σ -closed subgroup other than the one defined by the equation $\sigma(g) = 0$. Suppose that H is a proper, non-trivial σ -closed subgroup of G . By Corollary A.3 in [DVHW] every σ -closed subgroup of $\mathbb{G}_a$ is of the form $\mathbb{V}(f)$, where $f \in k\{y\}$ is the unique monic linear homogeneous difference polynomial of minimal order in $\mathbb{I}(H) \subset k\{\mathbb{G}_a\} = k\{y\}$. As H is non-trivial and properly contained in G , f must have order one, i.e., $f = \sigma(y) + \mu y$ for some $\mu \in k$. But then $\sigma^2(h) + \sigma(\mu)\sigma(h) = 0$ and therefore $(\lambda - \sigma(\mu))\sigma(h) = 0$ for all $h \in H(R)$ for any k - σ -algebra R . Because $\lambda \notin \sigma(k)$ this shows that $\sigma(h) = 0$ for all $h \in H(R)$. Therefore $f = \sigma(y)$.

Suppose $G_{\sigma\text{-red}}$ is a subgroup of G . By the above, then either $G_{\sigma\text{-red}} = G$, $G_{\sigma\text{-red}} = 1$ or $G_{\sigma\text{-red}} = H$, where H is defined by the equation $\sigma(y) = 0$.

Because $\sigma^n(y)$ does not lie in $[\sigma^2(y) + \lambda y]$ for $n \in \mathbb{N}$, the cases $G_{\sigma\text{-red}} = 1$ and $G_{\sigma\text{-red}} = H$ can be excluded. To arrive at a contradiction, it therefore suffices to find a non-zero element in the reflexive closure of the zero ideal of $k\{G\}$.

Assume that $\lambda^2 \in \sigma(k)$. (For example, we can choose $k = \mathbb{C}(\sqrt{x}, \sqrt{x+1}, \dots)$ with action of σ determined by $\sigma(x) = x+1$ and $\lambda = \sqrt{x}$.) We have $k\{G\} = k[y, \sigma(y)]$ and if we choose $\eta \in k$ such that $\sigma(\eta) = \lambda^2$, then $\sigma(y)^2 - \eta y^2$ lies in the reflexive closure of the zero ideal of $k\{G\}$.

The following example shows that the σ -closed subgroups constructed in Corollary 2.5.7 are in general not normal.

Example 2.5.11. Let N be the σ -closed subgroup of $\mathbb{G}_a$ given by $N(R) = \{g \in R \mid \sigma(g) = 0\}$ for any k - σ -algebra R . The σ -algebraic group $H = \mathbb{G}_m$ acts on N by group automorphisms

$$H(R) \times N(R) \rightarrow N(R), (h, n) \mapsto hn.$$

So we can form the semidirect product $G = N \rtimes H$ which is the σ -variety $N \times H$ with group multiplication given by

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 + h_1 n_2, h_1 h_2).$$

Then $k\{G\} = k\{N\} \otimes_k k\{H\} = k[x] \otimes_k k\{y, y^{-1}\}$ with $\sigma(x) = 0$. The reflexive closure of the zero ideal of $k\{G\}$ is the ideal of $k\{G\}$ generated by x . Therefore $G_{\sigma\text{-red}} = H \leq G$. For $h \in H(R)$ and $n \in N(R)$ we have

$$(n, 1)(0, h)(n, 1)^{-1} = (n - hn, h)$$

which shows that $G_{\sigma\text{-red}}$ is not normal in G .

In Lemma 4.1.22 we will show that $\sigma\text{-dim}(G_{\text{red}})$, $\sigma\text{-dim}(G_{\sigma\text{-red}})$, $\sigma\text{-dim}(G_{\text{wm}})$ and $\sigma\text{-dim}(G_{\text{per}})$ are all equal to $\sigma\text{-dim}(G)$. The following example shows that the order of $G_{\sigma\text{-red}}$ might be strictly smaller than the order of G .

Example 2.5.12. Let G be the σ -closed subgroup of $\mathbb{G}_a$ given by

$$G(R) = \{g \in R \mid \sigma^n(g) = 0\}$$

for any k - σ -algebra R . Then G has order n and $G_{\sigma\text{-red}}$ is the trivial group, which has order 0.

Chapter 3

Morphisms of difference algebraic groups

In this chapter we study representations and morphisms of difference algebraic groups. In particular, we establish the existence of the quotient G/N of a σ -algebraic group G modulo a normal σ -closed subgroup N of G and we characterize injective and surjective morphism of difference algebraic groups.

3.1 Representations of difference algebraic groups

In this section we present an application of the first finiteness theorem (Theorem 2.3.1). We prove the difference analog of a theorem of Chevalley for algebraic groups. Namely, we show that every σ -closed subgroup of a σ -algebraic group can be realized as the stabilizer of a line. We also show that the category of representations of $\mathbb{G}_m^n$ as a difference algebraic group is semi-simple.

Categories of representations of σ -algebraic groups have been studied in [OWb]. There the authors introduce σ -tannakian categories, which provide a purely categorical characterization of those categories, that are the category of representations of a σ -algebraic group.

Definition 3.1.1. *Let G be a σ -algebraic group. A representation of G is a pair (V, ϕ) comprising a finite dimensional k -vector space V and a morphism $\phi: G \rightarrow \mathrm{GL}(V)$ of σ -algebraic groups. The representation is called faithful if ϕ is a σ -closed embedding.*

We will often omit ϕ from the notation. A morphism $(V, \phi) \rightarrow (V', \phi')$ of representations of G is a k -linear map $f: V \rightarrow V'$ that is G -equivariant, i.e.,

$$\begin{array}{ccc} V \otimes_k R & \xrightarrow{f \otimes R} & V' \otimes_k R \\ \phi(g) \downarrow & & \downarrow \phi'(g) \\ V \otimes_k R & \xrightarrow{f \otimes R} & V' \otimes_k R \end{array}$$

commutes for every $g \in G(R)$ and any k - σ -algebra R .

Lemma 3.1.2. *Let G be a σ -algebraic group. The category of representations of G is equivalent to the category of finite dimensional comodules over $k\{G\}$.*

Proof. This is similar to Section 3.2 in [Wat79]. $\square$

Lemma 3.1.3. *Let V be a representation of the σ -algebraic group G and $W \leq V$ a linear subspace. Then the stabilizer G_W of W , defined by*

$$G_W(R) = \{g \in G(R) \mid g(W \otimes_k R) \subset W \otimes_k R\}$$

for any k - σ -algebra R , is a σ -closed subgroup of G .

Proof. Let $v_1, \dots, v_n$ be a basis of V such that $v_1, \dots, v_m$ is a basis of W . Moreover, let $\rho: V \rightarrow V \otimes_k k\{G\}$ denote the comodule structure corresponding to the given representation and write $\rho(v_j) = \sum_{i=1}^n v_i \otimes a_{ij} \in V \otimes_k k\{G\}$ for $j = 1, \dots, n$. So for a k - σ -algebra R and $g \in G(R) = \text{Hom}(k\{G\}, R)$ we have $g(v_j \otimes 1) = \sum_{i=1}^n v_i \otimes g(a_{ij}) \in V \otimes_k R$. This shows the $g \in G_W(R)$ if and only if $g(a_{ij}) = 0$ for $j = 1, \dots, m$ and $i = m+1, \dots, n$. Thus

$$G_W = \mathbb{V}([a_{ij} \mid 1 \leq j \leq m, m+1 \leq i \leq n]).$$

$\square$

We know from Theorem 2.1.17 that every σ -algebraic group admits a faithful representation. The following theorem provides a strengthening of this result:

Theorem 3.1.4. *Let G a σ -algebraic group and $H \leq G$ a σ -closed subgroup. Then there exists a faithful representation V of G and a line $L \leq V$ (i.e., a one dimensional k -subspace) such that H is the stabilizer of L , i.e.,*

$$H(R) = \{g \in G(R) \mid g(L \otimes_k R) \subset L \otimes_k R\}$$

for any k - σ -algebra R .

Proof. We will first construct a representation V of G such that H is the stabilizer of a subspace W of V . By Theorem 2.3.1 there exists a finite set $F \subset \mathbb{I}(H) \subset k\{G\}$ such that $\mathbb{I}(H) = [F]$. By Section 3.3 in [Wat79] there exists a finite dimensional subcomodule V of $k\{G\}$ such that $F \subset V$. Let $W = V \cap \mathbb{I}(H) \leq V$. If $v_1, \dots, v_n$ is a basis of V such that $v_1, \dots, v_m$ is a basis of W and $\Delta(v_j) = \sum_{i=1}^n v_i \otimes a_{ij} \in V \otimes_k k\{G\}$ for $j = 1, \dots, n$, then

$$\mathbb{I}(G_W) = [a_{ij} \mid 1 \leq j \leq m, m+1 \leq i \leq n]$$

by the proof of Lemma 3.1.3. Since $\mathbb{I}(H)$ and V are $k\{H\}$ -comodules also $W = \mathbb{I}(H) \cap V$ is a $k\{H\}$ -comodule. So W is stable under H , i.e., $H \leq G_W$, or $\mathbb{I}(G_W) \subset \mathbb{I}(H)$. We have

$$v_j = \sum_{i=1}^n \varepsilon(v_i) a_{ij} = \sum_{i=m+1}^n \varepsilon(v_i) a_{ij},$$

since $\varepsilon(\mathbb{I}(H)) = 0$. This shows that every $f \in F \subset W$ lies in

$$[a_{ij} \mid 1 \leq j \leq m, m+1 \leq i \leq n] = \mathbb{I}(G_W).$$

Therefore $\mathbb{I}(H) = [F] \subset \mathbb{I}(G_W)$ and consequently $H = G_W$.

The m -th exterior power $\wedge^m V$ is naturally a representation of G and $L = \wedge^m W \leq \wedge^m V$ is one dimensional. Moreover $G_L = G_W$. (See Section A.2 in [Wat79].) In case $\wedge^m V$ is not faithful, we can replace it by $\wedge^m V \oplus V'$, where V' is a faithful representation of G . $\square$

An algebraic group $\mathcal{G}$ over a field of characteristic zero is reductive if and only if it is linearly reductive, i.e., every representation of $\mathcal{G}$ is a direct sum of irreducible representations. In differential algebra, the only linearly reductive linear differential algebraic groups are those which are the constant points of a reductive algebraic group ([MO11, Theorem 3.14]). In particular, the linear differential algebraic group $\mathbb{G}_m$ is not linearly reductive. Indeed, the representation

$$\mathbb{G}_m \rightarrow \mathrm{GL}_2, \quad g \mapsto \begin{pmatrix} g & \delta(g) \\ 0 & g \end{pmatrix}$$

is not semi-simple. For difference algebraic groups the situation is fundamentally different. We show here that tori are linearly reductive difference algebraic groups and leave the characterization of the linearly reductive difference algebraic groups for the future.

Theorem 3.1.5. *Every representation of the difference algebraic group $G = \mathbb{G}_m^n$ is a direct sum of one-dimensional representations.*

Proof. Let us denote by X the set of all elements of $k\{G\} = k\{y_1, y_1^{-1}, \dots, y_n, y_n^{-1}\}$ which are products of elements of the form $\sigma^\alpha(y_i)^\beta$ where $\alpha \in \mathbb{N}$, $\beta \in \mathbb{Z}$ and $1 \leq i \leq n$. Then X is a k -basis of $k\{G\}$ and every element $\chi \in X$ is group-like, i.e., $\Delta(\chi) = \chi \otimes \chi$ and $\varepsilon(\chi) = 1$ where $\Delta: k\{G\} \rightarrow k\{G\} \otimes_k k\{G\}$ is the comultiplication and $\varepsilon: k\{G\} \rightarrow k$ the counit.

Let V be a representation of G , $\rho: V \rightarrow V \otimes_k k\{G\}$ the corresponding comodule and $v \in V$. Then we can write

$$\rho(v) = \sum_{\chi \in X} a_\chi \otimes \chi, \quad a_\chi \in V.$$

Applying the comodule identities $(\mathrm{id}_V \otimes \Delta) \circ \rho = (\rho \otimes \mathrm{id}_{k\{G\}}) \circ \rho$ and $(\mathrm{id}_V \otimes \varepsilon) \circ \rho = \mathrm{id}_V$ (see [Wat79, Section 3.2]) to v , we find that

$$\sum_{\chi \in X} a_\chi \otimes \chi \otimes \chi = \sum_{\chi \in X} \rho(a_\chi) \otimes \chi, \quad \text{and} \quad (3.1)$$

$$v = \sum_{\chi \in X} a_\chi. \quad (3.2)$$

Identity (3.1) implies that $\rho(a_\chi) = a_\chi \otimes \chi$. So $g(a_\chi \otimes 1) = a_\chi \otimes g(\chi)$ for $g \in G(R) = \mathrm{Hom}(k\{G\}, R)$ and R a k - σ -algebra. Thus ka_χ is a subrepresentation of V and it follows from (3.2) that V is spanned by all the one-dimensional subrepresentations arising in this way. $\square$

3.2 Quotients

The first goal in this section is to establish the existence of the quotient G/N , where N is a normal σ -closed subgroup of a σ -algebraic group G . We do not address the (highly non-trivial) question of the existence of the quotient G/H where H is an arbitrary σ -closed subgroup. As for (affine) algebraic groups, the quotient G/H will in general not be affine (but rather quasi-projective). For algebraic groups, the analog of Theorem 3.1.4 is a crucial ingredient for constructing the quotient as a quasi-projective variety. Therefore Theorem 3.1.4 already gives some indication that “ G/H is a quasi-projective σ -variety”.

But to even make sense of this statement, one would need to introduce a substantially heavier foundation of difference algebraic geometry than we have done in Section 1.2, where we only deal with the affine setting.

We also show how to compute $\sigma\text{-dim}(G/N)$, $\text{ord}(G/N)$ and $\text{ld}(G/N)$ from the corresponding values for G and N .

Let G be a σ -algebraic group. Recall that a σ -closed subgroup $N \leq G$ is called *normal* if $N(R)$ is a normal subgroup of $G(R)$ for any k - σ -algebra R . We write $N \trianglelefteq G$ to express that N is a normal σ -closed subgroup of G .

If $\phi: G \rightarrow H$ is a morphism of σ -algebraic groups, we define the *kernel* of ϕ

$$\ker(\phi)$$

to be the subfunctor of G given by $R \rightsquigarrow \ker(\phi_R)$. Then $\ker(\phi)$ is a normal σ -closed subgroup of G . Indeed $\ker(\phi) = \phi^{-1}(1)$, where $1 \leq H$ is the trivial σ -closed subgroup of H defined by the kernel $\mathfrak{m}_H$ of the counit $k\{H\} \rightarrow k$. Explicitly we have

$$\mathbb{I}(\ker(\phi)) = (\phi^*(\mathfrak{m}_H)) \subset k\{G\}.$$

Definition 3.2.1. Let G be a σ -algebraic group and $N \trianglelefteq G$ a normal σ -closed subgroup. A morphism of σ -algebraic groups $\pi: G \rightarrow G/N$ such that $N \subset \ker(\pi)$ is called a *quotient* of $G \bmod N$ if it is universal among such maps, i.e., for every morphism of σ -algebraic groups $\phi: G \rightarrow H$ with $N \subset \ker(\phi)$ there exists a unique morphism of σ -algebraic groups $\phi': G/N \rightarrow H$ such that

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/N \\ & \searrow \phi & \swarrow \phi' \\ & H & \end{array}$$

commutes.

Of course, if a quotient of $G \bmod N$ exists, it is unique up to a unique isomorphism. We will therefore usually speak of *the* quotient of $G \bmod N$.

For affine group schemes over a field (not necessarily of finite type), the fundamental theorem on quotients can be formulated in a purely Hopf algebraic manner ([Tak72]). Recall that a Hopf ideal $\mathfrak{a}$ in a Hopf algebra A over k is called *normal* if, using Sweedler notation,

$$\sum f_{(1)} S(f_{(3)}) \otimes f_{(2)} \in A \otimes_k \mathfrak{a}$$

for any $f \in \mathfrak{a}$, where S is the antipode of A . Normal Hopf ideals in A correspond to normal closed subgroup schemes ([Tak72, Lemma 5.1]). Similarly, if G is a σ -algebraic group, then normal σ -Hopf ideals in $k\{G\}$ correspond to normal σ -closed subgroups of G (Cf. Lemma 2.1.4.). Recall that for a Hopf algebra A over k the kernel of the counit $\varepsilon: A \rightarrow k$ is denoted by $\mathfrak{m}_A$.

Theorem 3.2.2 (M. Takeuchi). Let A be a Hopf algebra over k and $\mathfrak{a} \subset A$ a Hopf ideal. Then $A(\mathfrak{a}) = \{f \in A \mid \Delta(f) - f \otimes 1 \in A \otimes_k \mathfrak{a}\}$ is a Hopf subalgebra of A with $(\mathfrak{m}_{A(\mathfrak{a})}) = \mathfrak{a}$. Indeed $A(\mathfrak{a})$ is the unique Hopf subalgebra with this property and the largest Hopf subalgebra with the property that $(\mathfrak{m}_{A(\mathfrak{a})}) \subset \mathfrak{a}$.

Proof. By [Tak72, Lemma 4.4] $A(\mathfrak{a})$ is a Hopf subalgebra. By [Tak72, Lemma 4.7] it is the largest Hopf subalgebra with $(\mathfrak{m}_{A(\mathfrak{a})}) \subset \mathfrak{a}$. Finally, by [Tak72, Theorem 4.3] it is the unique Hopf subalgebra with $(\mathfrak{m}_{A(\mathfrak{a})}) = \mathfrak{a}$. $\square$

The existence of the quotient of $G \bmod N$ can be reduced to Theorem 3.2.2. A similar approach was taken in [DVHW14, Section A.9]. While the result in [DVHW14] is formulated in a slightly more general setup (there the k - σ -Hopf algebras need not be finitely σ -generated over k) the result we prove here is stronger. Indeed, with the aid of the second finiteness theorem (Theorem 2.3.5) we show that G/N is σ -algebraic, i.e., $k\{G/N\}$ is finitely σ -generated over k . This question remained open in [DVHW14].

Theorem 3.2.3. *Let G be a σ -algebraic group and $N \trianglelefteq G$ a σ -closed subgroup. Then the quotient of $G \bmod N$ exists. Moreover, a morphism of σ -algebraic groups $\pi: G \rightarrow G/N$ is the quotient of $G \bmod N$ if and only if $\ker(\pi) = N$ and $\pi^*: k\{G/N\} \rightarrow k\{G\}$ is injective.*

Proof. By Theorem 3.2.2

$$k\{G\}(\mathbb{I}(N)) = \{f \in k\{G\} \mid \Delta(f) - f \otimes 1 \in k\{G\} \otimes_k \mathbb{I}(N)\}$$

is a Hopf subalgebra of $k\{G\}$. Clearly it is also a k - σ -Hopf subalgebra. From Theorem 2.3.5 we know that $k\{G\}(\mathbb{I}(N))$ is finitely σ -generated over k . So we can define G/N as the σ -algebraic group represented by $k\{G\}(\mathbb{I}(N))$, i.e., $k\{G/N\} = k\{G\}(\mathbb{I}(N))$. Let $\pi: G \rightarrow G/N$ be the morphism of σ -algebraic groups corresponding to the inclusion $k\{G/N\} \subset k\{G\}$ of k - σ -Hopf algebras.

Let $\phi: G \rightarrow H$ be a morphism of σ -algebraic groups such that $N \subset \ker(\phi)$. As $\ker(\phi) = \mathbb{V}(\phi^*(\mathfrak{m}_H))$, the Hopf algebraic meaning of $N \subset \ker(\phi)$ is $\phi^*(\mathfrak{m}_H) \subset \mathbb{I}(N)$. To show that π has the required universal property, it suffices to show that $\phi^*(k\{H\}) \subset k\{G/N\}$. We know from Theorem 3.2.2 that $k\{G/N\}$ is the largest Hopf subalgebra of $k\{G\}$ such that $\mathfrak{m}_{k\{G/N\}} \subset \mathbb{I}(N)$. As $\mathfrak{m}_{\phi^*(k\{H\})} = \phi^*(\mathfrak{m}_H) \subset \mathbb{I}(N)$ we find $\phi^*(k\{H\}) \subset k\{G/N\}$.

Clearly π^* is injective. Moreover, $\ker(\pi) = \mathbb{V}(\pi^*(\mathfrak{m}_{G/N})) = \mathbb{V}(\mathbb{I}(N)) = N$ by Theorem 3.2.2.

If $\pi: G \rightarrow G/N$ is a morphism of σ -algebraic groups such that $N = \ker(\pi)$ and $\pi^*: k\{G/N\} \rightarrow k\{G\}$ is injective, then $\pi^*(k\{G/N\})$ is a Hopf subalgebra of $k\{G\}$ such that $(\mathfrak{m}_{\pi^*(k\{G/N\})}) = \mathbb{I}(N)$. Therefore $\pi^*(k\{G/N\}) = k\{G\}(\mathbb{I}(N))$ by Theorem 3.2.2. $\square$

Corollary 3.2.4. *Let $\phi: G \rightarrow H$ be a morphism of σ -algebraic groups. Then the induced morphism $G/\ker(\phi) \rightarrow H$ is a σ -closed embedding.*

Proof. The Hopf subalgebra $\phi^*(k\{H\}) \subset k\{G\}$ satisfies $(\mathfrak{m}_{\phi^*(k\{H\})}) = (\phi^*(\mathfrak{m}_H)) = \mathbb{I}(\ker(\phi))$. Therefore $\phi^*(k\{H\}) = k\{G\}(\mathbb{I}(\ker(\phi))) = k\{G/\ker(\phi)\}$ by Theorem 3.2.2. Consequently $k\{H\} \rightarrow k\{G/\ker(\phi)\}$ is surjective and $G/\ker(\phi) \rightarrow H$ is a σ -closed embedding by Lemma 1.2.7. $\square$

Example 3.2.5. Let G be the σ -closed subgroup of $\mathbb{G}_m$ given by

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

and let N be the normal σ -closed subgroup of G given by

$$N(R) = \{g \in R^\times \mid \sigma(g) = 1\}$$

for any k - σ -algebra R . We would like to determine the quotient G/N . Let H be the σ -algebraic group given by $H(R) = \{g \in R^\times \mid g^2 = 1\}$ and let $\phi: G \rightarrow H$ be the morphism given by

$$\phi_R: G(R) \rightarrow H(R), \quad g \mapsto \sigma(g).$$

Then ϕ has kernel N and the dual map $\phi^*: k\{H\} \rightarrow k\{G\}$ is injective. Thus it follows from Theorem 3.2.3 that ϕ is the quotient of $G \bmod N$, i.e., $G/N = H$.

Example 3.2.6. Let N be the σ -closed subgroup of the additive group $G = \mathbb{G}_a$ defined by a linear difference equation $\sigma^n(y) + \lambda_{n-1}\sigma^{n-1}(y) + \cdots + \lambda_0 y = 0$. The morphism

$$\phi: \mathbb{G}_a \rightarrow \mathbb{G}_a, g \mapsto \sigma^n(g) + \lambda_{n-1}\sigma^{n-1}(g) + \cdots + \lambda_0 g$$

has kernel N and the dual map $\phi^*: k\{y\} \rightarrow k\{y\}$, $y \mapsto \sigma^n(y) + \lambda_{n-1}\sigma^{n-1}(y) + \cdots + \lambda_0 y$ is injective. Therefore, ϕ is the quotient of $G \bmod N$, i.e., $G/N = \mathbb{G}_a$.

As one may expect, the formation of quotients is compatibel with base extension:

Lemma 3.2.7. *Let $N \trianglelefteq G$ be σ -algebraic groups and K a σ -field extension of k . Then $(G/N)_K = G_K/N_K$.*

Proof. It is clear from Theorem 3.2.3 that the kernel of the morphism $G_K \rightarrow (G/N)_K$ obtained from $G \rightarrow G/N$ by base extension is N_K . So by Theorem 3.2.3 again, it suffices to note that the dual map $k\{G/N\} \otimes_k K \rightarrow k\{G\} \otimes_k K$ is injective. $\square$

Let $\psi: R \rightarrow S$ be a morphism of k - σ -algebras. We say that ψ is *faithfully flat* if the underlying morphism $\psi^\sharp: R^\sharp \rightarrow S^\sharp$ of k -algebras is faithfully flat. In this case, we also say that S is a faithfully flat R - σ -algebra.

Let R be a k - σ -algebra and $\pi: G \rightarrow G/N$ a quotient. As for algebraic groups, the map $\pi_R: G(R) \rightarrow (G/N)(R)$ need not be surjective in general. (See Example 3.3.8.) This, at least initially, makes it difficult to transfer constructions familiar from the theory of abstract groups that refer to group elements to σ -algebraic groups. The following lemma is a very useful substitute for the missing surjectivity of π_R . See Chapter 5, in particular Theorem 5.1.12 on how this lemma is used.

Lemma 3.2.8. *Let G be a σ -algebraic group and $N \trianglelefteq G$ a σ -closed subgroup. Let R be a k - σ -algebra and $\bar{g} \in (G/N)(R)$. Then there exists a faithfully flat morphism $R \rightarrow S$ of k - σ -algebras and $g \in G(S)$ such that $G(S) \rightarrow (G/N)(S)$ maps g to the image of $\bar{g}$ in $(G/N)(S)$.*

Proof. We may use $\bar{g} \in (G/N)(R) = \text{Hom}(k\{G/N\}, R)$ to form $S = k\{G\} \otimes_{k\{G/N\}} R$. Since $k\{G\}$ is faithfully flat over $k\{G/N\}$ (See [Wat79, Chapter 14].), it follows that $R \rightarrow S$, $r \mapsto 1 \otimes r$ is faithfully flat ([Wat79, Section 13.3, p. 105]). Let us set $g: k\{G\} \rightarrow S$, $f \mapsto f \otimes 1$. Then the maps $k\{G/N\} \xrightarrow{\bar{g}} R \rightarrow S$ and $k\{G/N\} \rightarrow k\{G\} \xrightarrow{g} S$ are equal. So $g \in G(S)$ has the required property. $\square$

Now that we have established the existence of the quotient G/N we can start to study its properties. To see how the numerical invariants σ -dimension, order and limit degree behave with respect to quotients, we first need to understand how quotients intertwine with Zariski closures.

Lemma 3.2.9. *Let $\mathcal{G}$ be an algebraic group and let $N \leq G \leq \mathcal{G}$ be σ -closed subgroups. For $i \geq 0$ let $G[i]$ and $N[i]$ denote the i -th order Zariski closure of G and N in $\mathcal{G}$ respectively. Then N is normal in G if and only if $N[i]$ is normal in $G[i]$ for every $i \geq 0$.*

Proof. As $k\{G\} = \cup_{i \geq 0} k[G[i]]$ is the union of the Hopf subalgebras $k[G[i]]$, we see that $\mathbb{I}(N)$ is a normal Hopf ideal of $k\{G\}$ if and only if $\mathbb{I}(N) \cap k[G[i]]$ is a normal Hopf ideal of $k[G[i]]$ for every $i \geq 0$. $\square$

Proposition 3.2.10. *Let $\mathcal{G}$ be an algebraic group and $N \trianglelefteq G \leq \mathcal{G}$. For $i \geq 0$ let $G[i]$ and $N[i]$ denote the i -th order Zariski closure of G and N in $\mathcal{G}$ respectively. Then there exists an integer $m \geq 0$ such that G/N is a σ -closed subgroup of $G[m]/N[m]$ and for $i \geq 0$ the i -th order Zariski closure of G/N in $G[m]/N[m]$ is the quotient of $G[i+m]$ mod $N[i+m]$, i.e.,*

$$(G/N)[i] = G[m+i]/N[m+i].$$

Proof. By Theorems 3.2.2 and 3.2.3 we have

$$\begin{aligned} k\{G/N\} &= \{f \in k\{G\} \mid \Delta(f) - f \otimes 1 \in k\{G\} \otimes_k \mathbb{I}(N)\} \\ &= \bigcup_{i \geq 0} \{f \in k[G[i]] \mid \Delta(f) - f \otimes 1 \in k[G[i]] \otimes_k \mathbb{I}(N[i])\} \\ &= \bigcup_{i \geq 0} k[G[i]/N[i]]. \end{aligned}$$

Moreover,

$$k[G[i]/N[i]] \subset k[G[i+1]/N[i+1]] \text{ and } \sigma(k[G[i]/N[i]]) \subset k[G[i+1]/N[i+1]].$$

By Corollary 2.3.2, there exists an integer $m \geq 0$ such that $\mathbb{I}(N[j+1]) = (\mathbb{I}(N[j]), \sigma(\mathbb{I}(N[j])))$, i.e., $N[j+1] = (N[j] \times {}^\sigma \mathcal{G}) \cap (\mathcal{G} \times {}^\sigma(N[j]))$ for $j \geq m$. We claim that

$$k[k[G[m]/N[m]], \dots, \sigma^i(k[G[m]/N[m]))] = k[G[m+i]/N[m+i]] \quad \text{for } i \geq 0. \quad (3.3)$$

The inclusion “ $\subset$ ” is obvious. To prove the inclusion “ $\supset$ ” it suffices to show that

$$\psi_j: k[G[j]/N[j]] \otimes_k {}^\sigma(k[G[j]/N[j])) \longrightarrow k[G[j+1]/N[j+1]], \quad f_1 \otimes (\lambda \otimes f_2) \mapsto f_1 \lambda \sigma(f_2)$$

is surjective for $j \geq m$. With π_{j+1} and σ_{j+1} as in (2.1) the morphisms

$$G[j+1] \xrightarrow{\pi_{j+1}} G[j] \rightarrow G[j]/N[j] \text{ and } G[j+1] \xrightarrow{\sigma_{j+1}} {}^\sigma(G[j]) \rightarrow {}^\sigma(G[j]/N[j])$$

combine to a morphism

$$G[j+1] \rightarrow (G[j]/N[j]) \times {}^\sigma(G[j]/N[j])$$

of algebraic groups with kernel $(N[j] \times {}^\sigma \mathcal{G}) \cap (\mathcal{G} \times {}^\sigma(N[j])) = N[j+1]$. Therefore

$$G[j+1]/N[j+1] \longrightarrow (G[j]/N[j]) \times {}^\sigma(G[j]/N[j])$$

is a closed embedding and so the dual map is surjective, but the dual map is precisely ψ_j . We have thus proved (3.3). It follows from (3.3) that $k\{G[m]/N[m]\} \rightarrow k\{G/N\}$ is surjective, i.e., G/N is a σ -closed subgroup of $G[m]/N[m]$. As the ring to the left hand side of (3.3) is the coordinate ring of the i -th order Zariski closure of G/N in $G[m]/N[m]$, we obtain the required equality of the Zariski closures. $\square$

The following example shows that in general one cannot take $m = 0$ in Proposition 3.2.10.

Example 3.2.11. Let $G = \mathcal{G} = \mathbb{G}_a$ and $N \trianglelefteq G$ the σ -closed subgroup given by $N(R) = \{g \in R \mid \sigma(g) = 0\}$ for any k - σ -algebra R . Then $N[0] = G[0] = \mathbb{G}_a$ and $G[0]/N[0]$ is the trivial group. Therefore G/N cannot be a σ -closed subgroup of $G[0]/N[0]$.

Corollary 3.2.12. *Let G be a σ -algebraic group and $N \trianglelefteq G$ a normal σ -closed subgroup. Then*

$$\sigma\text{-dim}(G) = \sigma\text{-dim}(N) + \sigma\text{-dim}(G/N) \quad (3.4)$$

and

$$\text{ord}(G) = \text{ord}(N) + \text{ord}(G/N). \quad (3.5)$$

Proof. We may assume that G is a σ -closed subgroup of some algebraic group $\mathcal{G}$ (Theorem 2.1.17). For $i \geq 0$ let $G[i]$ and $N[i]$ denote the i -th order Zariski closure of G and N in $\mathcal{G}$ respectively. By Theorem 2.2.7 there exist $e_G, e_N \geq 0$ such that $\dim(G[i]) = \sigma\text{-dim}(G)(i+1) + e_G$ and $\dim(N[i]) = \sigma\text{-dim}(N)(i+1) + e_N$ for $i \gg 0$. Let $m \geq 0$ be as in Proposition 3.2.10 and for $i \geq 0$ let $(G/N)[i]$ denote the i -th order Zariski closure of G/N in $G[m]/N[m]$. By Theorem 2.2.7 there exist $e_{G/N} \geq 0$ such that $\dim((G/N)[i]) = \sigma\text{-dim}(G/N)(i+1) + e_{G/N}$. For $i \gg 0$

$$\begin{aligned} \sigma\text{-dim}(G/N)(i+1) + e_{G/N} &= \dim((G/N)[i]) = \dim(G[m+i]/N[m+i]) = \\ &= \dim(G[m+i]) - \dim(N[m+i]) = \\ &= \sigma\text{-dim}(G)(m+i+1) + e_G - \sigma\text{-dim}(N)(m+i+1) - e_N = \\ &= (\sigma\text{-dim}(G) - \sigma\text{-dim}(N))(i+1) + (\sigma\text{-dim}(G) - \sigma\text{-dim}(N))m + e_G - e_N. \end{aligned}$$

This proves (3.4). As $\text{ord}(G) < \infty$ if and only if $\sigma\text{-dim}(G) = 0$, it follows from (3.4) that (3.5) is valid if $\sigma\text{-dim}(G) > 0$. We can therefore assume that $\sigma\text{-dim}(G) = 0$, and consequently $\sigma\text{-dim}(N) = \sigma\text{-dim}(G/N) = 0$ as well. But then $\text{ord}(G/N) = e_{G/N} = e_G - e_N = \text{ord}(G) - \text{ord}(N)$. $\square$

Next we will show how to compute $\text{ld}(G/N)$ from $\text{ld}(N)$ and $\text{ld}(G)$. For clarity of the exposition, we single out a simple lemma on algebraic groups.

Lemma 3.2.13. *Let $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$ be algebraic groups and $\phi: G_2 \twoheadrightarrow G_1$ a surjective morphism of algebraic groups with kernel $\mathcal{G}$. Assume that the restriction of ϕ to N_2 has kernel $\mathcal{N}$ and maps N_2 surjectively onto N_1 . Then the kernel of the induced map $G_2/N_2 \rightarrow G_1/N_1$ is isomorphic to $\mathcal{G}/\mathcal{N}$.*

Proof. Since ϕ is surjective we may identify G_1 with $G_2/\mathcal{G}$. Note that the (Noether) isomorphism theorems also hold for algebraic groups. (See e.g., [Mil12, Chapter IX]). We have $N_1 = N_2/\mathcal{N} = N_2/\mathcal{G} \cap N_2 = N_2\mathcal{G}/\mathcal{G}$ and so $G_1/N_1 = (G_2/\mathcal{G})/(N_2\mathcal{G}/\mathcal{G}) = G_2/N_2\mathcal{G}$. This shows that the kernel of $G_2/N_2 \rightarrow G_1/N_1 = G_2/N_2\mathcal{G}$ equals $N_2\mathcal{G}/N_2 = \mathcal{G}/N_2 \cap \mathcal{G} = \mathcal{G}/\mathcal{N}$. $\square$

Corollary 3.2.14. *Let G be a σ -algebraic group and $N \trianglelefteq G$ a normal σ -closed subgroup. Then*

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

Proof. By Remark 2.4.3 and Corollary 3.2.12 the claim is valid if $\sigma\text{-dim}(G) > 0$. So we may assume that $\sigma\text{-dim}(G) = 0$ and therefore $\text{ld}(G)$, $\text{ld}(G/N)$ and $\text{ld}(N)$ are all finite. Let $m \geq 0$ be as in Proposition 3.2.10. For $i \geq 1$ we have commutative diagrams

$$\begin{array}{ccc} (G/N)[i] & \xrightarrow{\pi_i} & (G/N)[i-1] \\ \downarrow \simeq & & \downarrow \simeq \\ G[m+i]/N[m+i] & \xrightarrow{\phi_i} & G[m+i-1]/N[m+i-1] \end{array}$$

where ϕ_i is induced from the projection $G[m+i] \twoheadrightarrow G[m+i-1]$. For $i \gg 0$ we have $\text{ld}(G/N) = |\ker(\pi_i)| = |\ker(\phi_i)|$. Let $\mathcal{G}_{m+i}$ and $\mathcal{N}_{m+i}$ be the kernel of

$$G[m+i] \twoheadrightarrow G[m+i-1] \quad \text{and} \quad N[m+i] \twoheadrightarrow N[m+i-1]$$

respectively. It follows from Lemma 3.2.13 that $\ker(\phi_i) = \mathcal{G}_{m+i}/\mathcal{N}_{m+i}$. Therefore

$$\text{ld}(G/N) = |\mathcal{G}_{m+i}/\mathcal{N}_{m+i}| = |\mathcal{G}_{m+i}|/|\mathcal{N}_{m+i}| = \text{ld}(G)/\text{ld}(N).$$

□

3.3 Injective and surjective morphisms

In this section we characterize the analogs of injective and surjective morphisms in the category of groups. Analogous results for algebraic groups are in [Mil12, Chapter VII].

Theorem 3.3.1. *Let $\phi: G \rightarrow H$ be a morphism of σ -algebraic groups. Then the following statements are equivalent:*

- (i) *The kernel of ϕ is trivial.*
- (ii) *The map $\phi_R: G(R) \rightarrow H(R)$ is injective for every k - σ -algebra R .*
- (iii) *The morphism $\phi: G \rightarrow H$ is a σ -closed embedding.*
- (iv) *The dual map $\phi^*: k\{H\} \rightarrow k\{G\}$ is surjective.*
- (v) *The morphism $\phi: G \rightarrow H$ is a monomorphism in the category of σ -algebraic groups, i.e., for every pair $\phi_1, \phi_2: H' \rightarrow G$ of morphisms of σ -algebraic groups with $\phi\phi_1 = \phi\phi_2$ we have $\phi_1 = \phi_2$.*

Proof. Clearly (i) $\Leftrightarrow$ (ii), (iii) $\Rightarrow$ (ii) and (ii) $\Rightarrow$ (v). Moreover, (iii) and (iv) are equivalent by Lemma 1.2.7. So it suffices to show that (v) implies (iv). Define $H' = G \times_H G$ by

$$(G \times_H G)(R) = \{(g_1, g_2) \in G(R) \times G(R) \mid \phi(g_1) = \phi(g_2)\}$$

for any k - σ -algebra R . This is a σ -closed subgroup of $G \times G$. Indeed, $G \times_H G$ is represented by $k\{G\} \otimes_{k\{H\}} k\{G\}$. Let ϕ_1 and ϕ_2 denote the projections onto the first and second coordinate respectively. We have $\phi\phi_1 = \phi\phi_2$ and so by (v) we must have $\phi_1 = \phi_2$. This implies that the maps $f \mapsto f \otimes 1$ and $f \mapsto 1 \otimes f$ from $k\{G\} \rightarrow k\{G\} \otimes_{k\{H\}} k\{G\}$ are equal. As $\phi^*(k\{H\})$ is a Hopf subalgebra of $k\{G\}$ we know that $k\{G\}$ is faithfully flat over $\phi^*(k\{H\})$ ([Wat79, Chapter 14]). Therefore $f \otimes 1 = 1 \otimes f$ in $k\{G\} \otimes_{k\{H\}} k\{G\} = k\{G\} \otimes_{\phi^*(k\{H\})} k\{G\}$ if and only if $f \in \phi^*(k\{H\})$ by [Wat79, Section 13.1, p. 104]. Summarily, we find that $\phi^*: k\{H\} \rightarrow k\{G\}$ is surjective. □

Definition 3.3.2. *A morphism of σ -algebraic groups satisfying the equivalent properties of Theorem 3.3.1 is called injective.*

Example 3.3.3. The morphism $\phi: \mathbb{G}_m \rightarrow \mathbb{G}_m$ given by $\phi_R(g) = \sigma(g)$ for any k - σ -algebra R and $g \in R^\times$ is not injective. Even though ϕ_R is injective for every σ -field extension R of k .

Example 3.3.4. The morphism $\phi: \mathbb{G}_m \rightarrow \mathbb{G}_m^2$ given by

$$\phi_R: \mathbb{G}_m(R) \rightarrow \mathbb{G}_m^2(R), \quad g \mapsto (g\sigma(g), \sigma(g))$$

is injective.

To address the analog of surjective morphisms of abstract groups, recall that in Lemma 1.2.6 we defined $\phi(X)$ for a morphism $\phi: X \rightarrow Y$ of σ -varieties.

Lemma 3.3.5. *Let $\phi: G \rightarrow H$ be a morphism of σ -algebraic groups and G_1 a σ -closed subgroup of G . Then $\phi(G_1)$ is a σ -closed subgroup of H .*

Proof. We may assume that $G_1 = G$. It follows from the proof of Lemma 1.2.6 that $\phi(G) = \mathbb{V}(\mathfrak{a})$, where $\mathfrak{a}$ is the kernel of $\phi^*: k\{H\} \rightarrow k\{G\}$. Since ϕ^* is a morphism of k - σ -Hopf algebras, $\mathfrak{a}$ is a σ -Hopf ideal. So $\phi(G)$ is a σ -closed subgroup of H . $\square$

Theorem 3.3.6. *Let $\phi: G \rightarrow H$ be a morphism of σ -algebraic groups. The following statements are equivalent:*

- (i) $\phi(G) = H$.
- (ii) *The morphism ϕ is a quotient, i.e., there exists a normal σ -closed subgroup N of G such ϕ is the quotient of G mod N .*
- (iii) *The dual map $\phi^*: k\{H\} \rightarrow k\{G\}$ is injective.*
- (iv) *For every k - σ -algebra R and every $h \in H(R)$, there exists a faithfully flat R - σ -algebra S and $g \in G(S)$ such that the image of h in $H(S)$ equals $\phi(g)$.*

Proof. We know from Lemma 1.2.6 that $\phi(G)$ is the σ -closed σ -subvariety of H defined by $\ker(\phi^*)$. Therefore (i) and (iii) are equivalent. It is clear from Theorem 3.2.3 that (iii) and (ii) are equivalent. Moreover (ii) implies (iv) by Lemma 3.2.8. It thus suffices to show that (iv) implies (iii). Take $R = k\{H\}$ and $h = \text{id}_{k\{H\}} \in H(R) = \text{Hom}(k\{H\}, k\{H\})$. By (iv) there exists a faithfully flat morphism $\psi: k\{H\} \rightarrow S$ of k - σ -algebras and an element $g \in G(S) = \text{Hom}(k\{G\}, S)$ such that the image of h in $H(S) = \text{Hom}(k\{H\}, S)$ equals $\phi(g) = g\phi^*$. This means that $\psi = g\phi^*$. As any faithfully flat morphism of rings is injective, ψ is injective. Therefore ϕ^* is injective as well. $\square$

Definition 3.3.7. *A morphism of σ -algebraic groups satisfying the equivalent properties of Theorem 3.3.6 is called surjective.*

We write $\phi: G \twoheadrightarrow H$ to express that ϕ is surjective.

Example 3.3.8. The morphism $\phi: \mathbb{G}_m \rightarrow \mathbb{G}_m$ given by $\phi_R(g) = \sigma(g)$ for any k - σ -algebra R and $g \in R^\times$ is surjective since the dual map $\phi^*: k\{y, y^{-1}\} \rightarrow k\{y, y^{-1}\}$, $y \mapsto \sigma(y)$ is injective. Note that ϕ_R need not be surjective.

Example 3.3.9. The endomorphism of $\mathbb{G}_a$ defined by a linear difference equation is surjective because the dual map is injective. See Example 3.2.6.

Corollary 3.3.10. *A morphism of σ -algebraic groups that is injective and surjective is an isomorphism.*

Proof. By Theorems 3.3.1 and 3.3.6, an injective and surjective morphism of σ -algebraic groups induces a surjective and injective morphism on the σ -coordinate rings. $\square$

Corollary 3.3.11. *Every morphism of σ -algebraic groups factors uniquely as a surjective morphism followed by an injective morphism.*

Proof. Let $\phi: G \rightarrow H$ be a morphism of σ -algebraic groups. The uniqueness means that if $G \twoheadrightarrow H_1 \hookrightarrow H$ and $G \twoheadrightarrow H_2 \hookrightarrow H$ are two factorizations of ϕ , then there exists an isomorphism $H_1 \rightarrow H_2$ of σ -algebraic groups making

$$\begin{array}{ccccc} G & \twoheadrightarrow & H_1 & \hookrightarrow & H \\ \parallel & & \downarrow \simeq & & \parallel \\ G & \twoheadrightarrow & H_2 & \hookrightarrow & H \end{array}$$

commutative. By Theorem 2.3.5 the k - σ -Hopf subalgebra $\phi^*(k\{H\})$ of $k\{G\}$ is finitely σ -generated over k . So we can define H_1 as the σ -algebraic group represented by $\phi^*(k\{H\})$. The claim of the corollary follows immediately by dualizing. $\square$

Note that H_1 has two interpretations, either as $\phi(G)$ or as $G/\ker(\phi)$. See Theorem 5.2.1.

Example 3.3.12. Let $\phi: \mathbb{G}_a \rightarrow \mathbb{G}_a^2$ be the morphism given by

$$\phi_R: \mathbb{G}_a(R) \rightarrow \mathbb{G}_a^2(R), \quad g \mapsto (\sigma(g), \sigma^2(g))$$

for any k - σ -algebra R . Let us determine the factorisation of ϕ according to Corollary 3.3.11. Let H be the σ -closed subgroup of $\mathbb{G}_a^2$ given by

$$H(R) = \{(g_1, g_2) \in R^2 \mid \sigma(g_1) = g_2\}$$

for any k - σ -algebra R . Then H is isomorphic to $\mathbb{G}_a$ (via $(g_1, g_2) \mapsto g_1$) and ϕ maps into H . The dual map of $\phi: \mathbb{G}_a \rightarrow H \simeq \mathbb{G}_a$ is given by $k\{y\} \rightarrow k\{y\}$, $y \mapsto \sigma(y)$, which is injective. So $\phi: \mathbb{G}_a \rightarrow H$ is surjective and $\phi: \mathbb{G}_a \twoheadrightarrow H \hookrightarrow \mathbb{G}_a^2$ is the required factorisation of ϕ .

As we will see in the sequel, point (iv) of Theorem 3.3.6 is very helpful to reduce certain questions to computations with group elements. Let X be a σ -variety. If $R \rightarrow S$ is an injective morphism of k - σ -algebras (e.g., S is a faithfully flat R - σ -algebra), then

$$X(R) = \text{Hom}(k\{X\}, R) \rightarrow \text{Hom}(k\{X\}, S) = X(S)$$

is injective. To simplify the notation, we will, in the sequel, often identify $X(R)$ with its image in $X(S)$.

Lemma 3.3.13. *Let Y be a σ -closed σ -subvariety of a σ -variety X and $R \rightarrow S$ an injective morphism of k - σ -algebras (e.g., $R \rightarrow S$ is faithfully flat). Then*

$$Y(R) = X(R) \cap Y(S),$$

where, using the above described identification, the intersection is understood to take place in $X(S)$.

Proof. The inclusion “ $\subset$ ” is obvious. To prove “ $\supset$ ” it suffices to note that for a morphism $k\{X\} \rightarrow S$ with factorizations $k\{X\} \twoheadrightarrow k\{Y\} \rightarrow S$ and $k\{X\} \rightarrow R \hookrightarrow S$, one has an arrow $k\{Y\} \rightarrow R$ such that

$$\begin{array}{ccc} & k\{Y\} & \\ \nearrow & \vdots & \searrow \\ k\{X\} & & S \\ \searrow & \downarrow & \nearrow \\ & R & \end{array}$$

commutes. $\square$

Lemma 3.3.14. *Let $\phi: G \rightarrow H$ be a morphism of σ -algebraic groups and $G_1 \leq G$ a σ -closed subgroup. Let R be a k - σ -algebra. Then $\phi(G_1)(R)$ equals the set of all $h \in H(R)$ such that there exists a faithfully flat R - σ -algebra S and $g_1 \in G_1(S)$ with $\phi(g_1) = h$.*

Proof. The induced morphism $G_1 \rightarrow \phi(G_1)$ is surjective. So it follows from Theorem 3.3.6 (iv) that for $h \in \phi(G_1)(R)$ there exists a faithfully flat R - σ -algebra S and $g_1 \in G_1(S)$ with $\phi(g_1) = h$.

Conversely, if $h = \phi(g_1)$, then $h \in \phi(G_1(S)) \subset \phi(G_1)(S)$ and we can deduce from $\phi(G_1)(S) \cap H(R) = \phi(G_1)(R)$ (Lemma 3.3.13) that $h \in \phi(G_1)(R)$. $\square$

Lemma 3.3.15. *Let $\phi: G \rightarrow H$ be a surjective morphism of σ -algebraic groups. If N is a normal σ -closed subgroup of G , then $\phi(N)$ is a normal σ -closed subgroup of H .*

Proof. Let R be a k - σ -algebra, $h \in \phi(N)(R)$ and $h_1 \in H(R)$. We have to show that $h_1 h h_1^{-1} \in \phi(N)(R)$. By Theorem 3.3.6, there exists a faithfully flat R - σ -algebra S and $g \in N(S)$ with $\phi(g) = h$. Similarly, there exists a faithfully flat R - σ -algebra S_1 and $g_1 \in G(S_1)$ with $\phi(g_1) = h_1$. Then $S' = S \otimes_R S_1$ is a faithfully flat R - σ -algebra ([Wat79, Section 13.3, p. 106]) and we can consider $G(S)$ and $G(S_1)$ as subgroups of $G(S')$. Since $N(S') \trianglelefteq G(S')$ we see that $g_1 g g_1^{-1} \in N(S')$. Therefore

$$\phi(g_1 g g_1^{-1}) = h_1 h h_1^{-1} \in \phi(N(S')) \subset \phi(N)(S').$$

As $\phi(N)(S') \cap H(R) = \phi(N)(R)$ by Lemma 3.3.13, this shows that $h_1 h h_1^{-1} \in \phi(N)(R)$. $\square$

We finish this chapter with a short digression on semidirect products. Let H and N be σ -algebraic groups such that H acts on N via group automorphisms, i.e., we are given a morphism of functors $H \times N \rightarrow N$ such that $H(R) \times N(R) \rightarrow N(R)$, $(h, n) \mapsto h(n)$ is a group action of $H(R)$ on $N(R)$ with the property that every $h \in H(R)$ is acting on $N(R)$ as a group automorphism for any k - σ -algebra R .

Then we can form the *semidirect product*

$$N \rtimes H$$

of N and H . It is the σ -algebraic group with underlying σ -variety $N \times H$ but with group multiplication given by

$$(n_1, h_1) \cdot (n_2, h_2) = (n_1 h_1(n_2), h_1 h_2).$$

Example 3.3.16. The σ -algebraic group $H = \mathbb{G}_m$ acts on the σ -algebraic group $\mathbb{G}_a$ via group automorphisms by

$$\mathbb{G}_m \times \mathbb{G}_a \rightarrow \mathbb{G}_a, (h, n) \mapsto h\sigma^{-1}(h)n.$$

The associated semidirect product $G = N \rtimes H$ is the σ -algebraic group from Example 2.1.13.

See Example 2.5.11 for another example. A sequence of morphisms of σ -algebraic groups $1 \rightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \rightarrow 1$ is called *exact* if α is injective, β is surjective and $\alpha(N) = \ker(\beta)$.

Lemma 3.3.17. *Let $1 \rightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} H \rightarrow 1$ be an exact sequence of σ -algebraic groups. If there exists a σ -closed subgroup H' of G such that β induces an isomorphism $H' \rightarrow H$, then G is isomorphic to the semidirect product of N and H .*

Proof. We identify N with a σ -closed subgroup of G . Because $N = \ker(\beta)$ we see that N is normal in G . Therefore H' acts on N via conjugation. It suffices to show that the multiplication map

$$\phi_R: N(R) \rtimes H'(R) \rightarrow G(R), (n, h) \mapsto nh$$

is an isomorphism for any k - σ -algebra R . A straight forward (and well-known) computation shows that ϕ_R is a morphism of groups. Since β is an isomorphism on H' it is clear that $N(R) \cap H'(R) = 1$. Therefore ϕ_R is injective. For $g \in G(R)$ let $h \in H'(R)$ be the unique element such that $\beta(h) = \beta(g)$. Then $n = gh^{-1} \in \ker(\beta)(R) = N(R)$ and $g = nh$. Thus ϕ_R is surjective. $\square$

Chapter 4

Components

For a difference algebraic group G there are at least three possible analogs of the identity component of an algebraic group. There is the identity component G^o with respect to the usual (Zariski) topology, there is the σ -identity component $G^{\sigma o}$, i.e., the identity component with respect to a topology that also takes into account the action of σ and there is the strong identity component G^{so} , which is the smallest σ -closed subgroup of G of the same σ -dimension as G . In this chapter we introduce G^o and $G^{\sigma o}$ via a study of the associated quotient groups $\pi_0(G) = G/G^o$ and $\pi_0^\sigma(G) = G/G^{\sigma o}$.

4.1 Connected components

In [Hru04, Section 4.6] E. Hrushovski raised the question whether or not it is possible to strengthen the classical Ritt-Raudenbusch basis theorem ([Lev08, Theorem 2.5.11]). For clarity, let us state the question as a conjecture:

Conjecture 1. *Let k be a σ -field and R a finitely σ -generated k - σ -algebra. Then every ascending chain of radical, mixed σ -ideals in R is finite.*

Recall that a σ -ideal $\mathfrak{a}$ is called mixed, if $ab \in \mathfrak{a}$ implies $a\sigma(b) \in \mathfrak{a}$. E. Hrushovski proved Conjecture 1 under certain additional assumptions on R . (See [Hru04, Lemma 4.35].) In [Lev] A. Levin showed that the conjecture fails if the assumption that the σ -ideals are radical is dropped.

A prime σ -ideal $\mathfrak{p}$ of a σ -ring R is called minimal if for every prime σ -ideal $\mathfrak{q}$ of R with $\mathfrak{q} \subset \mathfrak{p}$ we have $\mathfrak{q} = \mathfrak{p}$. Using [Hru04, Lemma 4.34] one can show that Conjecture 1 is equivalent to the following:

Conjecture 2. *Let k be a σ -field and R a finitely σ -generated k - σ -algebra. Then the set of minimal prime σ -ideals of R is finite.*

One of the main results of this section is a special case of the above conjecture:

Theorem 4.1.1. *Conjecture 2 holds under the additional assumption that R can be equipped with the structure of a k - σ -Hopf algebra.*

The proof of Theorem 4.1.1 is given at the end of this section (after Theorem 4.1.24). More generally, in this section we study the components of a σ -algebraic group. The matter is complicated by the fact that, contrary to the case of algebraic groups or differential

algebraic groups, a σ -algebraic group may have infinitely many components. However, as indicated in Theorem 4.1.1, a σ -algebraic group has only finitely many “ σ -components”.

To be able to speak meaningfully of topological notions, such as connected components, we first need to clarify what is the topological space associated to a σ -algebraic group. By the underlying *topological space of a σ -algebraic group* G we mean the underlying topological space of the scheme $G^\sharp$. In other words, the underlying topological space of G is $\text{Spec}(k\{G\})$. The reader might wonder if not some difference analog of $\text{Spec}(-)$ would provide a more adequate notion. For example (cf. [Hru04] and Subsection 1.3.2), one could consider the space of all σ -prime σ -ideals of $k\{G\}$ instead of the space of all prime ideals of $k\{G\}$. (Recall that a prime σ -ideal $\mathfrak{p}$ is called σ -prime if $\sigma^{-1}(\mathfrak{p}) = \mathfrak{p}$.) However, there often are not “enough” σ -prime σ -ideals. In general, a σ -ring need not contain a σ -prime σ -ideal. This pathology does not occur for σ -algebraic groups, since $\mathfrak{m}_G$, the kernel of the counit $\varepsilon: k\{G\} \rightarrow k$, is a σ -prime σ -ideal. But it may happen that $\mathfrak{m}_G$ is the only σ -prime σ -ideal of $k\{G\}$, even if G is quite far from being the trivial group:

Example 4.1.2. For all the σ -algebraic groups in the following list, the σ -ideal $\mathfrak{m}_G$ is the only σ -prime σ -ideal of $k\{G\}$. (Equivalently, $G(K) = 1$ for every σ -field extension K of k . Cf. Remark 2.5.3.)

- $G(R) = \{g \in \text{GL}_n(R) \mid \sigma(g_{ij}) = \delta_{ij}\} \leq \text{GL}_n(R)$
- $G(R) = \{g \in R \mid \sigma^n(g) = 0\} \leq \mathbb{G}_a(R)$ for some $n \geq 1$.
- $G(R) = \{g \in R \mid g^n = 1, \sigma(g) = 1\} \leq \mathbb{G}_m(R)$ for some $n \geq 1$.
- $G(R) = \{g \in R \mid g^3 = 1, \sigma(g) = g\} \leq \mathbb{G}_m(R)$, where k contains two non-trivial third roots of unity which are permuted by $\sigma: k \rightarrow k$.
- $G(R) = \{g \in R^\times \mid g^p = 1\} \leq \mathbb{G}_m(R)$ where k has characteristic $p > 0$.
- $G(R) = \{g \in R^\times \mid g^p = 1, \sigma^2(g) = g^3\} \leq \mathbb{G}_m(R)$ where k has characteristic $p > 0$.
- Let $\mathbf{G}$ be a finite group and $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ a group endomorphism with only one fixed point (for example, $\sigma(g) = 1$ for $g \in \mathbf{G}$). Let G be the corresponding σ -algebraic group constructed in Example 2.1.15.

As usual, by an *irreducible component* of a topological space we mean a maximal irreducible subset. By a *connected component* of a topological space we mean a maximal connected subset. An irreducible (or connected) component is automatically closed. Every topological space is the disjoint union of its connected components.

By a connected (or irreducible) component of a σ -algebraic group G we mean a connected (or irreducible) component of the underlying topological space of G . If R is a ring and $\mathfrak{a} \subset R$, let us denote by $\mathcal{V}(\mathfrak{a})$ the closed subset of $\text{Spec}(R)$ defined by $\mathfrak{a}$.

Lemma 4.1.3. *Let G be a σ -algebraic group. The connected components and the irreducible components of G coincide. Moreover, if $\mathfrak{p}$ is a prime ideal of $k\{G\}$, then the connected component of G containing $\mathfrak{p}$ equals $\mathcal{V}(\mathfrak{a})$, where $\mathfrak{a}$ is the ideal of $k\{G\}$ generated by all idempotent elements of $k\{G\}$ contained in $\mathfrak{p}$.*

Proof. Let us fix a σ -closed embedding $G \hookrightarrow \mathcal{G}$ of G into some algebraic group $\mathcal{G}$ and for $i \geq 0$ let $G[i]$ denote the i -th order Zariski-closure of G in $\mathcal{G}$. Let $C \subset \text{Spec}(k\{G\})$ denote a connected component of G . Then $C = \mathcal{V}(\mathfrak{a})$ for a unique ideal $\mathfrak{a}$ of $k\{G\}$ generated by

idempotent elements. (See [Sta14, Tag 00EB].) For every $i \geq 0$, the closure of the image of C under the projection $G^\# \rightarrow G[i]$ is connected and equal to $\mathcal{V}(\mathfrak{a} \cap k[G[i]]) \subset G[i]$. So $\mathcal{V}(\mathfrak{a} \cap k[G[i]]) \subset G[i]$ is contained in a connected component of $G[i]$. Assume that $G[i]$ has n_i connected components. Then

$$k[G[i]] = e_{i,1}k[G[i]] \oplus \cdots \oplus e_{i,n_i}k[G[i]]$$

for some primitive idempotent elements $e_{i,1}, \dots, e_{i,n_i} \in k[G[i]]$ and $\mathcal{V}(\mathfrak{a} \cap k[G[i]]) \subset \mathcal{V}(\mathfrak{b}_i)$ where $\mathfrak{b}_i = (e_{i,1}, \dots, e_{i,j_i-1}, e_{i,j_i+1}, \dots, e_{i,n_i}) \subset k[G[i]]$ for a unique $j_i \in \{1, \dots, n_i\}$. We have $\mathfrak{b}_{i+1} \cap k[G[i]] = \mathfrak{b}_i$ for $i \geq 0$ and $\mathfrak{b} := \cup_{i \geq 0} \mathfrak{b}_i$ is an ideal of $k\{G\}$. From $\mathcal{V}(\mathfrak{a} \cap k[G[i]]) \subset \mathcal{V}(\mathfrak{b}_i)$ it follows that $\mathfrak{b}_i$ is contained in the radical of $\mathfrak{a} \cap k[G[i]]$. Since the $e_{i,j}$'s are idempotent this shows that $\mathfrak{b}_i \subset \mathfrak{a}$. So $\mathfrak{b} \subset \mathfrak{a}$.

Since $k\{G\}/\mathfrak{b}$ may be interpreted as the directed union of the algebras $k[G[i]]/\mathfrak{b}_i \simeq e_{i,j_i}k[G[i]]$ which have a prime nilradical, it is clear that $\mathcal{V}(\mathfrak{b})$ is irreducible (and a fortiori connected). As $C = \mathcal{V}(\mathfrak{a}) \subset \mathcal{V}(\mathfrak{b})$ it follows from the maximality of C that $\mathcal{V}(\mathfrak{a}) = \mathcal{V}(\mathfrak{b})$. By the uniqueness of $\mathfrak{a}$ we have $\mathfrak{a} = \mathfrak{b}$.

We have thus shown that every connected component of G is irreducible. So the connected and the irreducible components of G coincide.

The claimed form of the connected component of a prime ideal of $k\{G\}$ follows from the above arguments. $\square$

Since the connected components and the irreducible components of a σ -algebraic group coincide, we will speak simply of the *components of a σ -algebraic group* in the sequel. The components of a σ -algebraic group G are in bijection with the minimal prime ideals of $k\{G\}$. The following simple example shows that a σ -algebraic group can have infinitely many components and that the components need not be open.

Example 4.1.4. Let $G \leq \mathbb{G}_m$ be the σ -algebraic group given by

$$G(R) = \{g \in R^\times \mid g^2 = 1\} \leq \mathbb{G}_m(R)$$

for any k - σ -algebra R . We have

$$k\{G\} = k\{y\}/[y^2 - 1] = k[y, \sigma(y), \dots]/(y^2 - 1, \sigma(y)^2 - 1, \dots).$$

Let us assume that the characteristic of k is not equal to 2. Then the prime ideals of $k\{G\}$ are in bijection with the set of all sequences $(a_i)_{i \in \mathbb{N}}$ such that $a_i \in \{1, -1\}$. Every prime ideal of $k\{G\}$ is its own component. In particular, G has infinitely many components. The open subsets of $\text{Spec}(k\{G\})$ are all infinite, thus the components are not open.

Allowing ourselves a little abuse of notation we denote the canonical map

$$\text{Spec}(k\{G\}) \rightarrow \text{Spec}(k\{G\}), \mathfrak{p} \mapsto \sigma^{-1}(\mathfrak{p})$$

also by σ .

Definition 4.1.5. A component C of a σ -algebraic group is called a σ -component if $\sigma(C) \subset C$.

Example 4.1.6. The σ -algebraic group from Example 4.1.4 has two σ -components, namely the prime ideals corresponding to the sequences $(1, 1, \dots)$ and $(-1, -1, \dots)$.

Lemma 4.1.7. *Let G be a σ -algebraic group and $C \subset \operatorname{Spec}(k\{G\})$ a component of G . Let $\mathfrak{p} \subset k\{G\}$ be the minimal prime ideal and $\mathfrak{a} \subset k\{G\}$ the ideal generated by idempotent elements such that $C = \mathcal{V}(\mathfrak{p}) = \mathcal{V}(\mathfrak{a})$. Then the following conditions are equivalent:*

- (i) *The component C is a σ -component.*
- (ii) *The ideal $\mathfrak{a}$ is a σ -ideal.*
- (iii) *The ideal $\mathfrak{p}$ is a σ -ideal.*
- (iv) *There exists a prime σ -ideal in C .*
- (v) *There exists a σ -prime σ -ideal in C .*
- (vi) *The set of all idempotent elements contained in $\mathfrak{a}$ is stable under σ .*

Proof. The equivalence of (i) and (iii) is straightforward. As $\mathfrak{p}$ is the radical of $\mathfrak{a}$ we see that (ii) implies (iii). Clearly (iii) implies (iv). If $\mathfrak{q}$ is a σ -ideal in C , then its reflexive closure $\mathfrak{q}^* = \{f \in k\{G\} \mid \exists n \geq 0 : \sigma^n(f) \in \mathfrak{q}\}$ is a σ -prime σ -ideal in C (cf. [Lev08, p. 107] and Section 2.5 below). So (iv) implies (v).

Let us next show that (v) implies (vi). If $\mathfrak{q}$ is a σ -prime σ -ideal in C , then by Lemma 4.1.3 we have $C = \mathcal{V}(\mathfrak{a}')$ where $\mathfrak{a}' \subset k\{G\}$ is the ideal generated by all idempotent elements contained in $\mathfrak{q}$. By [Sta14, Tag 00EB] we must have $\mathfrak{a}' = \mathfrak{a}$. Now let $e \in \mathfrak{a}$ be an idempotent. We have to show that $\sigma(e) \in \mathfrak{a}$. But $e \in \mathfrak{q}$ (as $\mathfrak{q} \in C = \mathcal{V}(\mathfrak{a})$) and consequently $\sigma(e) \in \mathfrak{q}$ is also idempotent. So $\sigma(e) \in \mathfrak{a}' = \mathfrak{a}$.

Finally, the implication (vi) $\Rightarrow$ (ii) follows from the simple fact that an ideal generated by a σ -stable set is a σ -ideal. $\square$

Corollary 4.1.8. *Let $k\{G\}$ be a k - σ -Hopf algebra that is finitely σ -generated over k . Then a minimal prime σ -ideal of $k\{G\}$ is a minimal prime ideal of $k\{G\}$.*

Proof. Let $\mathfrak{q} \subset k\{G\}$ be a minimal prime σ -ideal and let $C \subset \operatorname{Spec}(k\{G\})$ be the component that contains $\mathfrak{q}$. Then $C = \mathcal{V}(\mathfrak{p})$ for a minimal prime ideal $\mathfrak{p}$ of $k\{G\}$. Since $\mathfrak{q} \in C$ it follows from Lemma 4.1.7 that $\mathfrak{p}$ is a σ -ideal. Therefore $\mathfrak{q} = \mathfrak{p}$ by the minimality of $\mathfrak{q}$. $\square$

We will next introduce σ -étale σ -algebraic groups. The role of these groups in the theory of σ -algebraic groups is in a certain sense analogous to the role of étale algebraic groups in the theory of algebraic groups. We will study σ -étale σ -algebraic groups in more detail in Chapter 6. For now we will only use them to define the group of components and the identity component of a σ -algebraic group.

Definition 4.1.9. *A finitely σ -generated k - σ -algebra R is called σ -étale (over k) if R is integral over k and a separable k -algebra.*

Thus a finitely σ -generated k - σ -algebra R is σ -étale if and only if for every $r \in R$ there exists a separable polynomial f over k with $f(r) = 0$. Similar notions of étaleness in difference algebra occur in [Tom14] and [Tom] in a slightly different setting.

Definition 4.1.10. *A σ -algebraic group G is called σ -étale if $k\{G\}$ is σ -étale over k .*

Some examples of σ -étale σ -algebraic groups are given at the beginning of Section 6.1.

Recall ([Bou90, Chapter V, §6]) that a k -algebra A is called étale if $A \otimes_k \bar{k}$ is a finite direct product of copies of $\bar{k}$, where $\bar{k}$ denotes the algebraic closure of k . For a k -algebra A we let

$$\pi_0(A)$$

denote the union of all étale k -subalgebras of A . That is, $\pi_0(A)$ consists of all elements of A that annul a separable polynomial over k . Then $\pi_0(A)$ is a k -subalgebra of A . (Cf. Section 6.7 in [Wat79].) Clearly, a σ -algebraic group G is σ -étale if and only if $\pi_0(k\{G\}) = k\{G\}$. Moreover:

Lemma 4.1.11. *Let A and B be k -algebras. Then $\pi_0(A \otimes_k B) = \pi_0(A) \otimes_k \pi_0(B)$.*

Proof. We may assume that A and B are finitely generated as k -algebras. In this case the statement is proved in [Wat79, Section 6.7, p. 50]. $\square$

Theorem 4.1.12. *Let G be a σ -algebraic group. There exists a σ -étale σ -algebraic group $\pi_0(G)$ and a morphism $G \rightarrow \pi_0(G)$ of σ -algebraic groups satisfying the following universal property: If $G \rightarrow H$ is a morphism of σ -algebraic groups with H σ -étale, then there exists a unique morphism $\pi_0(G) \rightarrow H$ such that*

$$\begin{array}{ccc} G & \xrightarrow{\quad} & \pi_0(G) \\ & \searrow & \swarrow \text{dotted} \\ & H & \end{array}$$

commutes.

Proof. The k -subalgebra $\pi_0(k\{G\})$ of $k\{G\}$ is a Hopf subalgebra. (Cf. Section 6.7 in [Wat79].) Let $a \in \pi_0(k\{G\})$ and let f be a separable polynomial over k with $f(a) = 0$. Let ${}^\sigma f$ denote the polynomial obtained from f by applying σ to the coefficients. Then ${}^\sigma f$ is separable by Lemma 1.1.4 and ${}^\sigma f(\sigma(a)) = 0$. This shows that $\pi_0(k\{G\})$ is a k - σ -Hopf subalgebra of $k\{G\}$. Note that $\pi_0(k\{G\})$ is finitely σ -generated over k by Theorem 2.3.5. Let $\pi_0(G)$ denote the σ -étale σ -algebraic group corresponding to $\pi_0(k\{G\})$ and $G \rightarrow \pi_0(G)$ the morphism corresponding to the inclusion $\pi_0(k\{G\}) \subset k\{G\}$.

If $G \rightarrow H$ is a morphism of σ -algebraic groups with H σ -étale, then the image of the dual map $k\{H\} \rightarrow k\{G\}$ consists of elements that annul a separable polynomial. Thus the image lies in $\pi_0(k\{G\})$ and $k\{H\} \rightarrow k\{G\}$ factors uniquely through $\pi_0(k\{G\}) \hookrightarrow k\{G\}$. $\square$

Of course $\pi_0(G)$ is unique up to unique isomorphisms. It is clear from the above proof that $G \rightarrow \pi_0(G)$ is surjective.

Definition 4.1.13. *Let G be a σ -algebraic group. The σ -étale σ -algebraic group $\pi_0(G)$ defined by the universal property from Theorem 4.1.12 is called the group of components of G . The kernel G° of $G \twoheadrightarrow \pi_0(G)$ is called the identity component of G .*

So $G/G^\circ = \pi_0(G)$.

Lemma 4.1.14. *Let G be a σ -algebraic group. There is a one-to-one correspondence between the components of G and the components of $\pi_0(G)$. Under this bijection σ -components correspond to σ -components. Moreover, every component of $\pi_0(G)$ consists of a single point.*

Proof. Every prime ideal of $k\{\pi_0(G)\}$ is maximal and hence also minimal. This shows that the components of $\pi_0(G)$ are points. We identify $k\{\pi_0(G)\}$ with its image in $k\{G\}$. We claim that $\mathfrak{p} \mapsto \mathfrak{p} \cap k\{\pi_0(G)\}$ is a bijection between the minimal prime ideals of $k\{G\}$ and the (minimal) prime ideals of $k\{\pi_0(G)\}$. Every (minimal) prime ideal of $k\{\pi_0(G)\}$ is of the form $\mathfrak{p} \cap k\{\pi_0(G)\}$ for some minimal prime ideal of $k\{G\}$ ([Bou72, Proposition 16, Chapter II, §2.6]). On the other hand, if $\mathfrak{p}$ is a minimal prime ideal of $k\{G\}$, then $\mathfrak{p} = \sqrt{\mathfrak{a}}$ for some ideal $\mathfrak{a}$ of $k\{G\}$ generated by idempotent elements. Since all idempotent elements of $k\{G\}$ lie in $k\{\pi_0(G)\}$, we see that $(\mathfrak{a} \cap k\{\pi_0(G)\}) = \mathfrak{a}$. Therefore $\sqrt{(\mathfrak{p} \cap k\{\pi_0(G)\})} = \mathfrak{p}$.

If $\mathfrak{p}$ is a σ -ideal, then $\mathfrak{p} \cap k\{\pi_0(G)\}$ is a σ -ideal. Conversely, if $\mathfrak{p}' \subset k\{\pi_0(G)\}$ is a σ -ideal, then $\sqrt{(\mathfrak{p}')} \subset k\{G\}$ is a σ -ideal. The claim follows using Lemma 4.1.7. $\square$

Proposition 4.1.15. *The following four conditions on a σ -algebraic group G are equivalent:*

- (i) $G^o = G$.
- (ii) $\pi_0(G) = 1$.
- (iii) *The topological space of G is connected.*
- (iv) *The nilradical of $k\{G\}$ is a prime ideal.*

Proof. Clearly, (i) $\Leftrightarrow$ (ii). We have (ii) $\Leftrightarrow$ (iii) by Lemma 4.1.14. Since the connected components are irreducible (Lemma 4.1.3), it follows from (iii) that $k\{G\}$ has a unique minimal prime ideal, which must then equal the nilradical. Thus (iii) $\Rightarrow$ (iv). On the other hand, (iv) means that the topological space of G is irreducible. So (iv) $\Rightarrow$ (iii). $\square$

Definition 4.1.16. *A σ -algebraic group satisfying the equivalent conditions of Proposition 4.1.15 is called connected.*

Example 4.1.17. Let G be the σ -closed subgroup of $\mathbb{G}_a$ defined the linear difference equation $\sigma^n(y) + \lambda_{n-1}\sigma^{n-1}(y) + \cdots + \lambda_0 y = 0$. Then $k\{G\} = k[y, \sigma(y), \dots, \sigma^{n-1}(y)]$ is an integral domain. Therefore G is connected.

Example 4.1.18. Let G be the unitary σ -algebraic group, i.e.,

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

for any k - σ -algebra R . The defining equations may be written as $\sigma(g) = (g^{-1})^T$. So the coordinate ring $k\{G\} = k[x_{ij}, \frac{1}{\det(x)}]$ is an integral domain. Therefore G is connected.

Note that the identity component G^o of a σ -algebraic group G is, strictly speaking, not a component. It carries more structure than a mere component, in particular it has the structure of a σ -variety. However, as illustrated in the proof of the following lemma, the topological space of G^o can be identified with the component of G that contains the identity $\mathfrak{m}_G$.

Lemma 4.1.19. *Let G be a σ -algebraic group. Then G^o is connected.*

Proof. Every ideal of $k\{\pi_0(G)\}$ is generated by idempotent elements. It follows that $\mathfrak{m}_{\pi_0(G)} = \mathfrak{m}_G \cap k\{\pi_0(G)\}$ is generated by all idempotent elements contained in $\mathfrak{m}_G$. Therefore, $\mathbb{I}(G^o) = (\mathfrak{m}_{\pi_0(G)})$ is the ideal of $k\{G\}$ generated by all idempotent elements of $k\{G\}$ contained in $\mathfrak{m}_G$. It follows from Lemma 4.1.3, that $\mathcal{V}(\mathbb{I}(G^o)) \subset \mathrm{Spec}(k\{G\})$ is connected. As $\mathcal{V}(\mathbb{I}(G^o))$ and $\mathrm{Spec}(k\{G^o\}) = \mathrm{Spec}(k\{G\}/\mathbb{I}(G^o))$ are homeomorphic, this implies that G^o is connected. $\square$

Lemma 4.1.20. *Let G be a σ -closed subgroup of an algebraic group $\mathcal{G}$ and for $i \geq 0$ let $G[i]$ and $G^o[i]$ denote the i -th order Zariski closure of G and G^o in $\mathcal{G}$ respectively. Then*

$$G^o[i] = G[i]^o.$$

In particular, G is connected if and only if all its Zariski closures are connected.

Proof. Both groups are defined by the ideal of $k[G[i]] \subset k\{G\}$ that is generated by all idempotent elements of $k[G[i]]$ contained in the kernel of the counit $k[G[i]] \rightarrow k$. $\square$

Corollary 4.1.21. *Let G be a σ -algebraic group. Then $\sigma\text{-dim}(G^o) = \sigma\text{-dim}(G)$ and $\text{ord}(G^o) = \text{ord}(G)$.*

Proof. Let $\mathcal{G}$ be a σ -algebraic group containing G as a σ -closed subgroup. Then for $i \geq 0$ we have $\dim(G[i]) = \dim(G[i]^o) = \dim(G^o[i])$ by Lemma 4.1.20. Thus the claim follows from Theorem 2.2.7. $\square$

The limit degree of G and G^o are in general distinct. Indeed $\text{ld}(G) = \text{ld}(\pi_0(G)) \cdot \text{ld}(G^o)$ by Corollary 3.2.14.

As announced in Section 2.5, we can now show that the G_{red} , $G_{\sigma\text{-red}}$, G_{wm} and G_{per} all have the same σ -dimension as G .

Lemma 4.1.22. *Let G be a σ -algebraic group. Assume that k has the relevant properties as stated in Corollary 2.5.7 (so that we are dealing with σ -closed subgroups). Then $\sigma\text{-dim}(G_{\text{red}})$, $\sigma\text{-dim}(G_{\sigma\text{-red}})$, $\sigma\text{-dim}(G_{\text{wm}})$ and $\sigma\text{-dim}(G_{\text{per}})$ are all equal to $\sigma\text{-dim}(G)$.*

Proof. As the dimension of a finitely generated k -algebra remains invariant if we factor by the nilradical, it follows easily that $\sigma\text{-dim}(G_{\text{red}}) = \sigma\text{-dim}(G)$.

Since $(G^o)_{\sigma\text{-red}} \leq G_{\sigma\text{-red}}$, $(G^o)_{\text{wm}} \leq G_{\text{wm}}$ and $(G^o)_{\text{per}} \leq G_{\text{per}}$ we may assume that G is connected by Lemma 4.1.21. But then the nilradical of $k\{G\}$ is a prime σ -ideal (Proposition 4.1.15) and therefore $G_{\text{wm}} = G_{\text{red}}$ and thus $\sigma\text{-dim}(G_{\text{wm}}) = \sigma\text{-dim}(G)$ also in this case.

To prove $\sigma\text{-dim}(G_{\text{per}}) = \sigma\text{-dim}(G)$ we may assume that G is reduced. Then the zero ideal of $k\{G\}$ is prime and therefore its reflexive closure $\cup_{i \geq 1} \sigma^{-i}(0)$ is a σ -prime ideal. This shows that $G_{\text{per}} = G_{\sigma\text{-red}}$.

It thus suffices to show that $\sigma\text{-dim}(G_{\sigma\text{-red}}) = \sigma\text{-dim}(G)$. Let $\mathcal{G}$ be an algebraic group containing G as a σ -closed subgroup and for $i \geq 0$ let $G[i]$ and $G_{\sigma\text{-red}}[i]$ denote the i -th order Zariski closure of G and $G_{\sigma\text{-red}}$ in $\mathcal{G}$ respectively. By Corollary 2.3.2 we have

$$\mathbb{I}(G_{\sigma\text{-red}}[i]) = (\mathbb{I}(G_{\sigma\text{-red}}[i-1]), \sigma(\mathbb{I}(G_{\sigma\text{-red}}[i-1]))) \subset k[G[i]] \subset k\{G\}$$

for $i \gg 0$. But $\mathbb{I}(G_{\sigma\text{-red}}) = \{f \in k\{G\} \mid \exists n \geq 1 : \sigma^n(f) = 0\}$. This shows that there exist $f_1, \dots, f_m$ in $k\{G\}$ such that $\mathbb{I}(G_{\sigma\text{-red}}[i]) = (f_1, \dots, f_m) \subset k[G[i]]$ for $i \gg 0$. Therefore $\dim(G[i]) - \dim(G_{\sigma\text{-red}}[i]) \leq m$ for $i \gg 0$ and consequently $\sigma\text{-dim}(G) = \sigma\text{-dim}(G_{\sigma\text{-red}})$. $\square$

We will next show that a σ -algebraic group has only finitely many σ -components.

Lemma 4.1.23. *Let R be a finitely σ -generated k - σ -algebra. If R is σ -étale, then R has only finitely many prime σ -ideals.*

Proof. Since R is σ -étale, every prime ideal of R is maximal and hence also minimal. If $\mathfrak{p}$ is a prime σ -ideal of R , then $\mathfrak{p} \subset \sigma^{-1}(\mathfrak{p})$ and therefore $\mathfrak{p} = \sigma^{-1}(\mathfrak{p})$. So every prime σ -ideal of R is σ -prime. It follows from the Ritt-Raudenbush basis theorem (cf. Theorems 2.5.11 and 2.5.7 in [Lev08]) that a finitely σ -generated k - σ -algebra has only finitely many minimal σ -prime ideals. Since every prime σ -ideal of R is a minimal σ -prime ideal of R , this implies that R has only finitely many prime σ -ideals. $\square$

Theorem 4.1.24. *A σ -algebraic group has only finitely many σ -components.*

Proof. Let G be a σ -algebraic group. By Lemma 4.1.14, the σ -components of G are in bijection with the σ -components of $\pi_0(G)$ and by Lemma 4.1.23 the σ -algebraic group $\pi_0(G)$ has only finitely many σ -components. $\square$

Proof of Theorem 4.1.1. By assumption $R = k\{G\}$ for a σ -algebraic group G . By Corollary 4.1.8 the set of minimal prime σ -ideals of $k\{G\}$ equals the set of minimal prime ideals of $k\{G\}$ which are σ -ideals. The latter set is finite by Theorem 4.1.24. $\square$

Remark 4.1.25. *If G is a σ -algebraic group such that $k\{G\}$ is well-mixed, then G has only finitely many components and they are all σ -components. If G is a σ -algebraic group such that G_{wm} is a σ -closed subgroup of G (e.g., k is algebraically closed, see Corollary 2.5.7), then the σ -components of G are in bijection with the components of G_{wm} .*

Proof. By [Hru04, Lemma 2.10] a radical mixed σ -ideal is the intersection of prime σ -ideals. If $k\{G\}$ is well-mixed, the nilradical of $k\{G\}$ is mixed and therefore it is the intersection of the minimal prime σ -ideals. Since there are only finitely many minimal prime σ -ideals in $k\{G\}$ (Theorem 4.1.1) we see that there are only finitely many minimal prime ideals in $k\{G\}$ and all of them are σ -ideals.

Assume that G is a σ -algebraic group such that G_{wm} is a σ -closed subgroup of G . The set of minimal prime ideals of $k\{G\}$ which are σ -ideals equals the set of minimal prime σ -ideals of $k\{G\}$ (Corollary 4.1.8) and the latter is the set of all prime ideals of $k\{G\}$ which are minimal above $\{0\}_{\text{wm}}$. $\square$

Our next goal is to show that G° is a characteristic subgroup of G (in the sense of Definition 2.1.5). To this end we record a simple lemma which we will also use in the proof of Theorem 4.2.40.

Lemma 4.1.26. *Let G be a σ -algebraic group and $N \trianglelefteq G$ a normal σ -closed subgroup. If for every k - σ -algebra R , every automorphism of the R - σ -Hopf algebra $k\{G\} \otimes_k R$ maps $k\{G/N\} \otimes_k R$ into $k\{G/N\} \otimes_k R$, then N is a characteristic subgroup of G .*

Proof. Let ϕ be an automorphism of G_R . We have to show that ϕ induces an automorphism of N_R , i.e., for every R - σ -algebra R' the map $\phi_{R'}$ maps $N_R(R') = N(R')$ bijectively onto $N(R')$. The dual map ϕ^* is an automorphism of the R - σ -Hopf algebra $k\{G\} \otimes_k R$ and because $k\{G/N\} \otimes_k R$ is mapped into $k\{G/N\} \otimes_k R$ by the inverse of ϕ^* , it follows that ϕ^* induces an automorphism of $k\{G/N\} \otimes_k R$. This yields a commutative diagram

$$\begin{array}{ccc} G(R') & \longrightarrow & (G/N)(R') \\ \phi_{R'} \downarrow & & \downarrow \\ G(R') & \longrightarrow & (G/N)(R') \end{array}$$

where the vertical arrows are isomorphisms. The claim now follows from the fact that the kernel of $G(R') \rightarrow (G/N)(R')$ is $N(R')$ (Theorem 3.2.3). $\square$

Theorem 4.1.27. *Let G be a σ -algebraic group. Then G° is a characteristic subgroup of G .*

Proof. By Lemma 4.1.26 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 $\pi_0(k\{G\}) \otimes_k R$ into $\pi_0(k\{G\}) \otimes_k R$. Using Lemma 4.1.11, we have

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

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

4.2 Difference connected components

In this section we study the connected components of a σ -algebraic group, however, not with respect to the usual Zariski topology as in Section 4.1, but with respect to a topology that also takes into account the action of σ . In particular, we will introduce the σ -identity component of a σ -algebraic group. The main tool for this is a generalization (of a slight variation) of the core of an extension of σ -fields (see [Lev08, Def. 4.3.17]).

4.2.1 The difference topology

We start with some general “ σ -topological” definitions and observations.

Definition 4.2.1. *A σ -topological space is a topological space X together with a continuous map $\sigma: X \rightarrow X$. A morphism between σ -topological spaces X and Y is a continuous map $\phi: X \rightarrow Y$ such that*

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

commutes.

A subset V of a σ -topological space X is called σ -closed if it is closed and σ -stable, i.e., $\sigma(V) \subset V$. Clearly, a finite union of σ -closed sets is σ -closed, and an arbitrary intersection of σ -closed sets is σ -closed. Since the empty set and X are σ -closed, we see that the σ -closed sets are the closed sets of a topology on X . This topology is called the σ -topology on X .

A σ -topological space is σ -connected if it is connected with respect to the σ -topology. The connected components with respect to the σ -topology are called the σ -connected components.

For the time being, we are mainly interested in the following example of a σ -topological space: Let R be a σ -ring, then $\text{Spec}(R)$ is naturally a σ -topological space. The topology on $\text{Spec}(R)$ is the usual Zariski topology and

$$\sigma: \text{Spec}(R) \rightarrow \text{Spec}(R), \mathfrak{p} \mapsto \sigma^{-1}(\mathfrak{p})$$

is the continuous map induced by $\sigma: R \rightarrow R$.

If $\mathfrak{a}$ is a σ -ideal of R and $\mathfrak{p}$ a prime ideal of R with $\mathfrak{p} \in \mathcal{V}(\mathfrak{a})$, i.e., $\mathfrak{a} \subset \mathfrak{p}$. Then $\mathfrak{a} \subset \sigma^{-1}(\mathfrak{a}) \subset \sigma^{-1}(\mathfrak{p})$. Therefore $\mathcal{V}(\mathfrak{a})$ is σ -closed.

Conversely, if $V \subset \operatorname{Spec}(R)$ is σ -closed, then $V = \mathcal{V}(\mathfrak{a})$ for a unique radical ideal $\mathfrak{a}$ of R . Indeed, $\mathfrak{a} = \bigcap_{\mathfrak{p} \in V} \mathfrak{p}$. Since V is σ -stable, $\sigma^{-1}(\mathfrak{p}) \in V$ for any $\mathfrak{p} \in V$. Therefore,

$$\sigma^{-1}(\mathfrak{a}) = \bigcap_{\mathfrak{p} \in V} \sigma^{-1}(\mathfrak{p}) \supset \bigcap_{\mathfrak{p} \in V} \mathfrak{p} = \mathfrak{a}.$$

So $\mathfrak{a}$ is a σ -ideal. In summary, we find that $\mathfrak{a} \mapsto \mathcal{V}(\mathfrak{a})$ induces a bijection between the set of radical σ -ideals of R and the set of σ -closed subsets of $\operatorname{Spec}(R)$.

Our next goal is to express the property that $\operatorname{Spec}(R)$ is σ -connected via difference algebraic conditions on R . In the algebraic setting, the connected components of the spectrum of a ring are closely related to idempotent elements. For example, $\operatorname{Spec}(R)$ is connected if and only if R contains no non-trivial idempotent element ([Mil12, Lemma 1.1, Chapter XIII, p. 204]). We will prove a difference analog of the latter result. Before, let us recall some terminology related to idempotent elements.

Let R be a ring. An element $e \in R$ is called *idempotent* if $e^2 = e$. The trivial idempotents are 0 and 1. Idempotents $e_1, \dots, e_n \in R$ are called *orthogonal* if $e_i e_j = 0$ for $i \neq j$. An idempotent element is called *primitive* if it cannot be written as a sum of two non-trivial orthogonal idempotent elements. A finite set $\{e_1, \dots, e_n\}$ of orthogonal idempotent elements is called *complete* if $e_1 + \dots + e_n = 1$.

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

$$R^\sigma.$$

Proposition 4.2.2. *Let R be a σ -ring. If $e \in R$ is a non-trivial constant idempotent element, then*

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

is a decomposition of $\operatorname{Spec}(R)$ into disjoint non-empty σ -closed subsets. Conversely, if $\operatorname{Spec}(R) = X \uplus Y$ is a decomposition of $\operatorname{Spec}(R)$ 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 $\mathfrak{p} \in \operatorname{Spec}(R)$ 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 $\operatorname{Spec}(R)$ 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 $\mathcal{V}(e) = \operatorname{Spec}(R)$. Then e must lie in the nilradical of R . Because e is idempotent this implies $e = 0$; again a contradiction.

Now assume that $\operatorname{Spec}(R) = X \uplus Y$ is a decomposition of $\operatorname{Spec}(R)$ into disjoint non-empty σ -closed subsets. It is known that any decomposition of $\operatorname{Spec}(R)$ into two disjoint non-empty closed subsets arises from a pair e, e' of non-trivial idempotent elements with $ee' = 0$ and $e + e' = 1$ ([Mil12, Prop. 1.2, Chapter XIII, p. 204]). 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 -stable, $\sigma^{-1}(\mathfrak{p}) \in X$, i.e., $e \in \sigma^{-1}(\mathfrak{p})$. Thus $\sigma(e) \in \mathfrak{p}$ and $\mathcal{V}(e) \subset \mathcal{V}(\sigma(e))$. Similarly, one shows $\mathcal{V}(e') \subset \mathcal{V}(\sigma(e'))$. Because $\sigma(e)\sigma(e') = 0$ and $\sigma(e) + \sigma(e') = 1$ we have $\operatorname{Spec}(R) = \mathcal{V}(\sigma(e)) \uplus \mathcal{V}(\sigma(e'))$. 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 $a \in R$. Because $(1 - \sigma(e))\sigma(e) = 0$ 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 $\sigma(e) = e$. $\square$

From Proposition 4.2.2 we immediately obtain:

Corollary 4.2.3. *Let R be a σ -ring. Then $\text{Spec}(R)$ is σ -connected if and only if R contains no non-trivial constant idempotent element.* $\square$

Proposition 4.2.4. *Let R be a σ -ring and let $e_1, \dots, e_n \in R$ be constant orthogonal idempotent elements with $e_1 + \dots + e_n = 1$ 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 $\text{Spec}(R)$ are $\mathcal{V}(1 - e_1), \dots, \mathcal{V}(1 - e_n)$. Moreover, $e_i R$ is naturally a σ -ring and $\text{Spec}(e_i R)$ is isomorphic to $\mathcal{V}(1 - e_i)$ as a σ -topological space.*

Proof. Note that $e_i R$ is a σ -ideal of R , rather than a σ -subring of R . However, $e_i R$ is also σ -ring with identity element e_i . As $e_i R$ and $R/(1 - e_i)$ are isomorphic as σ -rings, we see that $\text{Spec}(e_i R)$ and $\mathcal{V}(1 - e_i)$ are isomorphic as σ -topological spaces.

Assume $e \in e_i R$ is a constant idempotent element. Then $e_i = e_i e + e_i(1 - e)$ expresses e_i as a sum of orthogonal constant idempotent elements. By assumption $e_i e = e_i$ or $e_i e = 0$. But $e_i e = e$, so $e = e_i$ or $e = 0$. It follows from Corollary 4.2.3 that $\mathcal{V}(1 - e_i) \simeq \text{Spec}(e_i R)$ is σ -connected.

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

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

Proposition 4.2.5. *Let T be a k -algebra. Then $([\sigma]_k T)^\sigma = k^\sigma$.*

Proof. Let $(v_i)_{i \in I}$ be a k -basis of $T \subset [\sigma]_k T$ that contains 1. For $n \geq 0$ and $\mathbf{i} = (i_0, \dots, i_n) \in I^{n+1}$ define $v_{\mathbf{i}} = v_{i_0} \sigma(v_{i_1}) \cdots \sigma^n(v_{i_n})$. By construction of $T[n]$ (cf. Subsection 1.2.4), $V_n := (v_{\mathbf{i}})_{\mathbf{i} \in I^{n+1}}$ is a k -basis of $T[n]$. Because $(v_i)_{i \in I}$ contains 1, we have $V_n \subset V_{n+1}$ and $\sigma(V_n) \subset V_{n+1}$.

Let a be a constant element of $[\sigma]_k T$. Suppose a does not lie in k . Let $n \geq 0$ 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 $v \in V_n \setminus V_{n-1}$, the coefficient λ_v is non-zero. As a is constant

$$a = \sum_{v \in V_n} \sigma(\lambda_v) \sigma(v) \quad (4.1)$$

If $v \in V_n \setminus V_{n-1}$, then $\sigma(v) \in V_{n+1} \setminus V_n$. Therefore equation (4.1) shows that $a \notin T[n]$, a contradiction. $\square$

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

Corollary 4.2.6. *Let T be a k -algebra. Then $\text{Spec}([\sigma]_k T)$ is σ -connected.*

Proof. By Corollary 4.2.3 it suffices to show that $[\sigma]_k T$ has no non-trivial constant idempotent element. But by Proposition 4.2.5 every constant idempotent of $[\sigma]_k T$ belongs to k and must therefore be trivial. $\square$

4.2.2 Strongly σ -étale k - σ -algebras and $\pi_0^\sigma(R)$

In the previous subsection we have seen that constant idempotent elements are closely related to σ -connected components. So if R is a k - σ -algebra, the k - σ -subalgebra of R σ -generated by all constant idempotent elements contains some information about the σ -connected components of $\text{Spec}(R)$. However, this k - σ -subalgebra is in some sense “too small”: It does not take into account the periodic idempotent elements, i.e., the constant idempotent elements with respect to σ^d ($d \in \mathbb{N}$, $d \geq 1$). Moreover, some constant idempotent elements may only become visible after an extension of the base σ -field k . Indeed, if G is a σ -algebraic group and K a σ -field extension of k , then G_K may have more σ -connected components than G . (See Example 4.2.48).

The main goal of this subsection is to define a k - σ -subalgebra $\pi_0^\sigma(R)$ of R that contains all the periodic idempotent elements and is well-behaved with respect to extensions of the base σ -field. In fact, we will define $\pi_0^\sigma(R)$ as the union of all strongly σ -étale (Definition 4.2.7) k - σ -subalgebras of R . In the next subsection we will then use the properties of $\pi_0^\sigma(R)$ proved in this subsection to define the σ -identity component $G^{\sigma\sigma}$ of a σ -algebraic group G . Indeed, eventually we will arrive at $\pi_0^\sigma(k\{G\}) = k\{G/G^{\sigma\sigma}\}$.

Recall ([Bou90, Chapter V, §6]) that an algebra R over a field k is called *étale* if $R \otimes_k \bar{k}$ is isomorphic to a finite direct product of copies of the algebraic closure $\bar{k}$ of k . (In particular, R is finite dimensional as a k -vector space.) The following definition introduces a difference analog of étale algebras.

Definition 4.2.7. *A k - σ -algebra is called strongly σ -étale if it is σ -separable over k and étale as a k -algebra.*

Clearly a strongly σ -étale k - σ -algebra is σ -étale. Note that by Proposition 1.1.8, over an inversive σ -field k , a k - σ -algebra whose underlying k -algebra is étale is strongly σ -étale if and only if it is inversive.

Similar to the use of étale algebras (and étale algebraic groups) in the study of the connected components of algebraic groups, we will use strongly σ -étale k - σ -algebras in the study of the σ -connected components of σ -algebraic groups. To achieve this we need several lemmas on strongly σ -étale k - σ -algebras.

Lemma 4.2.8. *Let R be a k - σ -algebra and K a σ -field extension of k . Then R is a strongly σ -étale k - σ -algebra if and only if $R \otimes_k K$ is a strongly σ -étale K - σ -algebra.*

Proof. By [Wat79, Cor. 6.2, p. 47] or [Bou90, Cor. 2, Chapter V, §6, No. 5, A.V.32] the k -algebra R is étale if and only if the K -algebra $R \otimes_k K$ is étale. Similarly, by Corollary 1.1.11 the k - σ -algebra R is σ -separable if and only if the K - σ -algebra $R \otimes_k K$ is σ -separable. $\square$

Let R be a σ -ring. Following [Lev08] an element $f \in R$ is called *periodic* if $\sigma^n(f) = f$ for some $n \geq 1$.

Lemma 4.2.9. *Let R be a strongly σ -étale k - σ -algebra. Then σ induces a bijection on the set of primitive idempotent elements of R . Moreover, every idempotent element of R is periodic.*

Proof. Let ${}^\sigma R = R \otimes_k k$ be the k - σ -algebra obtained from R by base extension via $\sigma: k \rightarrow k$. Because R is σ -separable over k it follows from Proposition 1.1.8 that

$$\psi: {}^\sigma R = R \otimes_k k \rightarrow R, \quad f \otimes \lambda \mapsto \sigma(f)\lambda$$

is injective. As R is a finite dimensional k -vector space, this implies that ψ is an isomorphism of k -algebras. Let $e_1, \dots, e_n$ denote the primitive idempotent elements of R . Then there are precisely n primitive idempotent elements in ${}^\sigma R$. These must be $e_1 \otimes 1, \dots, e_n \otimes 1 \in {}^\sigma R = R \otimes_k k$ and they are mapped bijectively onto the e_i 's under ψ . This shows that $e \mapsto \sigma(e)$ defines a bijection on $\{e_1, \dots, e_n\}$. In particular, each e_i is periodic. Since an arbitrary idempotent element of R is a sum of certain e_i 's, it follows that any idempotent element of R is periodic. $\square$

Lemma 4.2.10. *A k - σ -algebra σ -generated by finitely many periodic idempotent elements is strongly σ -étale.*

Proof. Let R be k - σ -algebra σ -generated by finitely many periodic idempotent elements. Because the σ -generators are periodic, R is in fact generated as a k -algebra by finitely many idempotent elements. For a non-trivial idempotent element $e \in R$ we have $k[e] \simeq k \times k$, which is an étale k -algebra. Thus a k -algebra generated by finitely many idempotent elements can be written as a quotient of a finite tensor product of étale k -algebras. Since quotients and tensor products of étale k -algebras are étale ([Bou90, Chapter V, §6]) it follows that R is étale. Moreover, R is generated as a k -vector space by periodic idempotent elements.

To show that R is σ -separable over k it suffices to show that

$$\psi: {}^\sigma R = R \otimes_k k \rightarrow R, \quad r \otimes \lambda \mapsto \lambda \sigma(r)$$

is injective (Proposition 1.1.8). Let $e_1, \dots, e_n$ be the primitive idempotent elements in R . These are a k -basis of R and therefore $e_1 \otimes 1, \dots, e_n \otimes 1 \in R \otimes_k k$ is a k -basis of ${}^\sigma R$. Moreover, the primitive idempotent elements in ${}^\sigma R$ are $e_1 \otimes 1, \dots, e_n \otimes 1$. Thus every idempotent element in ${}^\sigma R$ is of the form $e \otimes 1$ for some idempotent element $e \in R$. Every ideal in ${}^\sigma R$ is generated by an idempotent element. Therefore the kernel of ψ is generated by an element of the form $e \otimes 1$, where $e \in R$ is idempotent. So $\sigma(e) = 0$.

There exists a k -basis $d_1, \dots, d_n$ of R consisting of periodic idempotent elements. We can find an integer $m \geq 1$ such that $\sigma^m(d_i) = d_i$ for $i = 1, \dots, n$. We may write $e = \lambda_1 d_1 + \dots + \lambda_n d_n$ for $\lambda_1, \dots, \lambda_n \in k$. Then

$$0 = \sigma^m(e) = \sigma^m(\lambda_1) d_1 + \dots + \sigma^m(\lambda_n) d_n.$$

Therefore $\sigma^m(\lambda_1) = \dots = \sigma^m(\lambda_n) = 0$ and consequently also $e = 0$. This shows that ψ is injective. $\square$

In the sequel it will often be convenient to assume to the base σ -field k is algebraically closed or separably algebraically closed. This will be achieved by passing to the (separable) algebraic closure. Recall (Lemma 1.1.5) that $\sigma: k \rightarrow k$ can always be extended to an endomorphism on the (separable) algebraic closure.

The following proposition provides a sort of converse to the last lemma.

Proposition 4.2.11. *The R be a k - σ -algebra that is finite dimensional as a k -vector space. Let k_s denote the separable algebraic closure of k , equipped with an extension of σ . Then R is strongly σ -étale if and only if $R \otimes_k k_s$ is generated as a k_s -vector space by periodic idempotent elements.*

Proof. By Lemma 4.2.8 we may assume $k = k_s$.

Let us first assume that R is strongly σ -étale. Since $k = k_s$ and R is an étale k -algebra, R is generated as a k -vector space by idempotent elements (cf. [Wat79, Theorem 6.2]). By Lemma 4.2.9 every idempotent element of R is periodic.

Conversely, if R is generated by periodic idempotent elements, then it follows from Lemma 4.2.10 that R is strongly σ -étale. $\square$

Lemma 4.2.12. *A k - σ -subalgebra of a strongly σ -étale k - σ -algebra is strongly σ -étale. The tensor product of two strongly σ -étale k - σ -algebras is strongly σ -étale. The quotient of a strongly σ -étale k - σ -algebra by a σ -ideal is a strongly σ -étale k - σ -algebra.*

Proof. The first statement follows from the fact that a k -subalgebra of an étale k -algebra is étale ([Bou90, Prop. 3, Chapter V, §6, No. 4, A.V.30]) and the obvious fact that a k - σ -subalgebra of a σ -separable k - σ -algebra is σ -separable.

The second statement follows from the fact that the tensor product of two étale k -algebras is étale ([Bou90, Cor. 1, Chapter V, §6, No. 5, A.V.32]) and the fact that the tensor product of two σ -separable k - σ -algebras is σ -separable (Corollary 1.1.10).

Finally we prove the third statement. Let R be a strongly σ -étale k - σ -algebra and $\mathfrak{a}$ a σ -ideal of R . Let k_s denote the separable algebraic closure of k , equipped with an extension of σ . Then

$$(R/\mathfrak{a}) \otimes_k k_s = (R \otimes_k k_s) / (\mathfrak{a} \otimes_k k_s).$$

It follows from Proposition 4.2.11, that the right-hand side is generated as a k_s -vector space by periodic idempotent elements. Applying the proposition again yields the conclusion. $\square$

The core of an extension of σ -fields is an important concept in difference algebra ([Lev08, Def. 4.3.17]). Let us recall the definition:

Definition 4.2.13. *Let $K|k$ be an extension of σ -fields. The core*

$$\text{core}(K|k)$$

of $K|k$ is the union of all intermediate σ -fields of $K|k$, whose underlying field is a finite separable field extension of k .

The core $\text{core}(K|k)$ is a σ -subfield of K . It plays a fairly prominent role in classical difference algebra, for example in the study of compatibility of σ -field extensions ([Lev08, Theorem 5.4.22, p. 342]) or in questions related to extending specializations ([Coh65, Theorem XI, Chapter 7, p. 227]).

We need to generalize the definition of the core to arbitrary k - σ -algebras. One may argue that when passing from fields to algebras, étale k -algebras are the suitable generalization of finite separable field extensions. This motivates the following definition:

Definition 4.2.14. *Let R be a k - σ -algebra. The core*

$$\text{core}(R|k)$$

of R is the union of all k - σ -subalgebras of R , whose underlying k -algebra is étale.

It is not hard to see that $\text{core}(R|k)$ is a k - σ -subalgebra of R . (Cf. the remark after Definition 4.2.16.) Because an étale k -subalgebra of a field extension K of k is the same as a finite separable intermediate field of $K|k$, we see that Definition 4.2.14 generalizes Definition 4.2.13. However, it turns out that $\text{core}(R|k)$ is not the “correct” object for our purpose. Indeed, the following example shows that $\text{core}(R|k)$ may not be a Hopf subalgebra of R if R is a k - σ -Hopf algebra.

Example 4.2.15. Let G be the σ -algebraic subgroup of $\mathbb{G}_m^2$ given by

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

for any k - σ -algebra R . We will show that $\text{core}(k\{G\}|k)$ is not a k - σ -Hopf subalgebra of $k\{G\}$.

Let us assume that the characteristic of k is not equal to 2, so that G is σ -étale. 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 $k\{H_1\} = ke_1 \oplus ke_2$ for orthogonal idempotent elements $e_1, e_2 \in k\{H_1\}$ with $\sigma(e_1) = 1$ and $\sigma(e_2) = 0$. 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 an étale k -algebra. This shows that $e_2 \otimes k\{H_2\}$ is contained in $\text{core}(k\{G\}|k)$. In particular, $\text{core}(k\{G\}|k)$ has infinite dimension as a k -vector space.

Suppose $\text{core}(k\{G\}|k)$ is a k - σ -Hopf subalgebra of $k\{G\}$. Then $\text{core}(k\{G\}|k)$ is finitely σ -generated over k by Theorem 2.3.5 and it follows that $\text{core}(k\{G\}|k)$ is a finite dimensional k -vector space; a contradiction. So $\text{core}(k\{G\}|k)$ is not a k - σ -Hopf subalgebra of $k\{G\}$.

Definition 4.2.16. Let R be a k - σ -algebra. We define

$$\pi_0^\sigma(R) = \pi_0^\sigma(R|k)$$

as the union of all strongly σ -étale k - σ -subalgebras of R .

If R_1 and R_2 are strongly σ -étale k - σ -subalgebras of a k - σ -algebra R , then also $R_1 R_2$ is a strongly σ -étale k - σ -algebra by Lemma 4.2.12, since $R_1 R_2$ may be written as a quotient of $R_1 \otimes_k R_2$. This shows that $\pi_0^\sigma(R)$ is a k - σ -subalgebra of R . Clearly $\pi_0^\sigma(R)$ is σ -separable over k . However, $\pi_0^\sigma(R)$ need not be strongly σ -étale in general. Indeed, $\pi_0^\sigma(R)$ is strongly σ -étale if and only if $\pi_0^\sigma(R)$ is finitely σ -generated over k . This is also equivalent to $\pi_0^\sigma(R)$ being finite dimensional as a k -vector space. It is unclear to the author if $\pi_0^\sigma(R)$ is strongly σ -étale for an arbitrary finitely σ -generated k - σ -algebra R . We will see later (Corollary 4.2.32) that $\pi_0^\sigma(R)$ is a strongly σ -étale k - σ -subalgebra of R if R is a finitely σ -generated k - σ -Hopf algebra.

Example 4.2.17. For the σ -algebraic group G from Example 4.2.15 we have $\pi_0^\sigma(k\{G\}) = k$. (So G is σ -connected in the sense of Definition 4.2.36.) While it seems possible to prove this with a direct computation, we will give a more systematic proof which uses properties of π_0^σ proved below. With the notation of Example 4.2.15, 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 Proposition 4.2.43 that $\pi_0^\sigma(k\{H_2\}) = k$. Finally, using Lemma 4.2.23 we find

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

Remark 4.2.18. Let $K|k$ be a σ -field extension. If k is inversive, then

$$\pi_0^\sigma(K|k) = \text{core}(K|k).$$

Proof. This is clear because a σ -field extension of an inversive σ -field is automatically σ -separable (Corollary 1.1.12). $\square$

The results presented below will make it clear that $\pi_0^\sigma(R|k)$, rather than $\text{core}(R|k)$, is a useful generalization of the core of a σ -field extension.

Lemma 4.2.19. Let R be a k - σ -algebra. If k is separably algebraically closed, then $\pi_0^\sigma(R)$ is the k -subvector space of R generated by all periodic idempotent elements of R .

Proof. It is clear from Proposition 4.2.11 that $\pi_0^\sigma(R)$ is contained in the k -subvector space of R generated by all periodic idempotent elements of R .

On the other hand, $k\{e\} \subset \pi_0^\sigma(R)$ for every periodic idempotent element $e \in R$ by Lemma 4.2.10. $\square$

We will need a simple algebraic (rather than difference algebraic) lemma on idempotent elements.

Lemma 4.2.20. Let k be an algebraically closed field, K a field extension of k and R a k -algebra. Then every idempotent element e of $R \otimes_k K$ is of the form $e = f \otimes 1$ for some idempotent element $f \in R$.

Proof. A field extension of an algebraically closed field is geometrically connected (in the sense of Definition [Sta14, Tag 037T]). The claim thus follows from [Sta14, Tag 037W]. $\square$

Our next important goal is to show that the formation of π_0^σ is compatible with extension of the base σ -field. To prove this for the extension $k_s|k$, where k_s denotes the separable algebraic closure of k we will use Galois descent. In this connection we need to introduce an action of σ on the absolute Galois group of k that will also be relevant in Section 6.2, where we consider certain actions of the absolute Galois group that intertwine with σ .

To define the action of σ on the Galois group we need a simple lemma on field extensions. Because of lack of a suitable reference we include the proof.

Lemma 4.2.21. Let K be a σ -field, L a Galois extension of k and $\sigma_1, \sigma_2: L \rightarrow L$ two extensions of $\sigma: K \rightarrow K$. Then there exists a unique element τ in the Galois group of $L|K$ such that $\sigma_2 = \sigma_1\tau$.

Proof. The uniqueness of τ follows from the injectivity of σ_1 . Let $\mathcal{M}$ denote the set of all pairs (M, τ) where M is an intermediate field of $L|K$ and $\tau: M \rightarrow L$ a morphism of field extensions of K satisfying $\sigma_2(a) = \sigma_1(\tau(a))$ for all $a \in M$. By Zorn's Lemma there exists a maximal element (M, τ) in $\mathcal{M}$. Suppose that M is properly contained in L . Choose $a \in L \setminus M$ and let f denote the minimal polynomial of a over M . Let ${}^\tau f$ denote the polynomial obtained from f by applying τ to the coefficients. As L is Galois over K , we see that ${}^\tau f$ cannot have a root outside L . Thus ${}^\tau f$ has all its roots in L . Since $\sigma_2 f = \sigma_1 {}^\tau f$ we see that σ_1 maps the roots of ${}^\tau f$ onto the roots of $\sigma_2 f$. As $\sigma_2(a) \in L$ is a root of $\sigma_2 f$ this shows that there exists a root $b \in L$ of ${}^\tau f$ such that $\sigma_1(b) = \sigma_2(a)$. So we can extend τ to $\tau: M(a) \rightarrow L$ by setting $\tau(a) = b$; a contradiction. $\square$

Let k be a σ -field and let k_s denote the separable algebraic closure of k . Let $\mathcal{G}$ denote the Galois group of $k_s|k$. By Lemma 1.1.5 there exists an extension of $\sigma: k \rightarrow k$ to an endomorphism of k_s . Let us fix such an extension. For $\tau \in \mathcal{G}$ the maps σ and $\tau\sigma$ are extensions of $\sigma: k \rightarrow k$ to k_s . By Lemma 4.2.21 there exists a unique $\tau^\sigma \in \mathcal{G}$ such that

$$\tau\sigma = \sigma\tau^\sigma.$$

Then

$$\sigma: \mathcal{G} \rightarrow \mathcal{G}, \tau \mapsto \tau^\sigma$$

is a morphism of groups.

If k and therefore also k_s is inversive, this action of σ on the Galois group agrees with the action employed in [Lev08, Section 8.1], where the formula $\tau^\sigma = \sigma^{-1}\tau\sigma$ is used as the definition. Note, however, that this formula does not make sense in our context because σ need not be invertible.

The formation of $\pi_0^\sigma(R)$ is compatible with extension of the base σ -field:

Lemma 4.2.22. *Let R be a k - σ -algebra and K a σ -field extension k . Then*

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

Proof. The inclusion “ $\supset$ ” is clear from Lemma 4.2.8. We will prove the equality in several steps.

Step 1: Assume $K = k_s$ is the separable algebraic closure of k equipped with an extension of $\sigma: k \rightarrow k$. Let $\mathcal{G}$ denote the Galois group of $k_s|k$. As explained above there is an action of σ on $\mathcal{G}$ denoted by $\tau \mapsto \tau^\sigma$. There also is a natural action of $\mathcal{G}$ on $R \otimes_k k_s$ via the right factor: $\tau(r \otimes \lambda) = r \otimes \tau(\lambda)$ for $\tau \in \mathcal{G}$, $r \in R$ and $\lambda \in k$. For $f \in R \otimes_k k_s$ and $\tau \in \mathcal{G}$ we have $\tau(\sigma(f)) = \sigma(\tau^\sigma(f))$.

We will show that $\pi_0^\sigma(R \otimes_k k_s|k_s) \subset R \otimes_k k_s$ is stable under the $\mathcal{G}$ -action. We know from Lemma 4.2.19 that $\pi_0^\sigma(R \otimes_k k_s|k_s)$ is generated as a k_s -vector space by the periodic idempotent elements of $R \otimes_k k_s$. It therefore suffices to show that $\tau(e)$ is periodic and idempotent for every periodic idempotent element $e \in R \otimes_k k_s$ and every $\tau \in \mathcal{G}$. As τ defines an automorphism of $R \otimes_k k_s$, clearly also $\tau(e)$ is idempotent. Assume $\sigma^n(e) = e$. For $i \in \mathbb{N}$ we have

$$\tau(e) = \tau(\sigma^{ni}(e)) = \sigma^{ni}(\tau^{\sigma^{ni}}(e)). \quad (4.2)$$

Since every orbit of $\mathcal{G}$ on k_s is finite, also every orbit of $\mathcal{G}$ on $R \otimes_k k_s$ is finite. Therefore $\{\tau(e), \tau^{\sigma^n}(e), \tau^{\sigma^{2n}}(e), \dots\}$ is a finite set. It follows that there exist $i < j$ such that $\tau^{\sigma^{ni}}(e) = \tau^{\sigma^{nj}}(e)$. Then

$$\tau(e) = \sigma^{ni}(\tau^{\sigma^{ni}}(e)) = \sigma^{ni}(\tau^{\sigma^{nj}}(e)) = \tau^{\sigma^{n(j-i)}}(\sigma^{ni}(e)) = \tau^{\sigma^{n(j-i)}}(e).$$

Thus, replacing i with $j - i$ in equation (4.2), we obtain $\tau(e) = \sigma^{n(j-i)}(\tau(e))$. Therefore $\tau(e)$ is periodic as required.

So $\pi_0^\sigma(R \otimes_k k_s|k_s) \subset R \otimes_k k_s$ is stable under the $\mathcal{G}$ -action and it follows from Galois descent ([Bou90, Prop. 6, Chapter V, §10, No. 4, A.V.62] or [Spr09, Prop. 11.1.4, p. 186]) that $\pi_0^\sigma(R \otimes_k k_s|k_s) = S \otimes_k k_s$, where S is the k - σ -subalgebra of R given by $S = R \cap \pi_0^\sigma(R \otimes_k k_s|k_s)$. It now suffices to show that $k\{s\}$ is strongly σ -étale for every $s \in S$. But a finitely σ -generated k_s - σ -subalgebra of $\pi_0^\sigma(R \otimes_k k_s|k_s)$ is strongly σ -étale, so $k_s\{s\} = k\{s\} \otimes_k k_s$ is strongly σ -étale and it follows from Lemma 4.2.8 that $k\{s\}$ is strongly σ -étale.

Step 2: Assume that $k = k_s$ is separably algebraically closed and that $K = \bar{k}$ is the algebraic closure of k . If the characteristic of k is zero, $k_s = \bar{k}$ and there is nothing to prove. So we may assume that the characteristic of k is $p > 0$. Then $\bar{k}$ is purely inseparable over k . By Lemma 4.2.19 it suffices to show that every periodic idempotent element $e = \sum r_i \otimes \lambda_i \in R \otimes_k \bar{k}$ belongs to R . As $\bar{k}$ is purely inseparable over k , there exists an integer $n \geq 1$ such that $\lambda_i^{p^n} \in k$ for all i . So $e = e^{p^n} = \sum r_i^{p^n} \otimes \lambda_i^{p^n}$ lies in R .

Step 3: Assume that $K = \bar{k}$ is the algebraic closure of k . Then the separable algebraic closure k_s of k is naturally a σ -subfield of $\bar{k}$ (Lemma 1.1.5) and it follows from steps 2 and 1 that

$$\begin{aligned} \pi_0^\sigma(R \otimes_k \bar{k} | \bar{k}) &= \pi_0^\sigma((R \otimes_k k_s) \otimes_{k_s} \bar{k} | \bar{k}) = \pi_0^\sigma(R \otimes_k k_s | k_s) \otimes_{k_s} \bar{k} = \pi_0^\sigma(R | k) \otimes_k k_s \otimes_{k_s} \bar{k} = \\ &= \pi_0^\sigma(R | k) \otimes_k \bar{k}. \end{aligned}$$

Step 4: Assume that k and K are algebraically closed. We know from Proposition 4.2.11 that $\pi_0^\sigma(R \otimes_k K | K)$ is generated as a K -vector space by periodic idempotent elements. By Lemma 4.2.20 every idempotent element e of $R \otimes_k K$ is of the form $e = f \otimes 1$ for some idempotent element $f \in R$. If e is periodic, then also f is periodic. Therefore $\pi_0^\sigma(R \otimes_k K | K)$ is generated as a K -vector space by $\pi_0^\sigma(R | k)$ and so $\pi_0^\sigma(R \otimes_k K | K) = \pi_0^\sigma(R | k) \otimes_k K$.

Step 5: Finally we treat the general case, i.e., K is an arbitrary σ -field extension of k . Let $\bar{K}$ denote the algebraic closure of K and choose an extension of $\sigma: k \rightarrow k$ to $\bar{K}$. Then the algebraic closure $\bar{k}$ of k is naturally a σ -subfield of $\bar{K}$. As $R \otimes_k \bar{K} = (R \otimes_k \bar{k}) \otimes_{\bar{k}} \bar{K}$ it follows from steps 4 and 3 that

$$\pi_0^\sigma(R \otimes_k \bar{K} | \bar{K}) = \pi_0^\sigma(R \otimes_k \bar{k} | \bar{k}) \otimes_{\bar{k}} \bar{K} = \pi_0^\sigma(R | k) \otimes_k \bar{k} \otimes_{\bar{k}} \bar{K} = \pi_0^\sigma(R | k) \otimes_k K \otimes_K \bar{K}.$$

Moreover,

$$\begin{aligned} \pi_0^\sigma(R | k) \otimes_k K \otimes_K \bar{K} &\subset \pi_0^\sigma(R \otimes_k K | K) \otimes_K \bar{K} \subset \pi_0^\sigma(R \otimes_k K \otimes_K \bar{K} | \bar{K}) = \\ &= \pi_0^\sigma(R \otimes_k \bar{K} | \bar{K}) = \pi_0^\sigma(R | k) \otimes_k K \otimes_K \bar{K}. \end{aligned}$$

Therefore $(\pi_0^\sigma(R) \otimes_k K) \otimes_K \bar{K} = \pi_0^\sigma(R \otimes_k K) \otimes_K \bar{K}$ and consequently $\pi_0^\sigma(R | k) \otimes_k K = \pi_0^\sigma(R \otimes_k K | K)$ as desired. $\square$

Lemma 4.2.23. *Let R and S be k - σ -algebras. Then*

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

Proof. The inclusion “ $\supset$ ” follows from the fact that the tensor product of two strongly σ -étale k - σ -algebras is strongly σ -étale (Lemma 4.2.12).

To prove the inclusion “ $\subset$ ” we may assume that k is algebraically closed and inversive (Lemmas 4.2.22 and 1.1.6). We know from Lemma 4.2.19 that $\pi_0^\sigma(R \otimes_k S)$ is generated as a k -vector space by periodic idempotent elements. So let $e \in R \otimes_k S$ be a periodic idempotent element. It suffices to show that $e \in \pi_0^\sigma(R) \otimes_k \pi_0^\sigma(S)$.

We have $e \in \pi_0(R \otimes_k S) = \pi_0(R) \otimes_k \pi_0(S)$ by Lemma 4.1.11. So there exist étale k -subalgebras R_1 and S_1 of R and S respectively such that $e \in R_1 \otimes_k S_1$.

If V_i is a k -subspace of R such that $e \in V_i \otimes_k S$, then $e \in \cap_i (V_i \otimes_k S) = (\cap_i V_i) \otimes_k S$. Thus there exists a smallest k -subspace V of R such that $e \in V \otimes_k S$. Let $v_1, \dots, v_n$ be

a k -basis of V and write $e = \sum v_i \otimes s_i \in V \otimes_k S$. The idempotent element e is periodic, say $\sigma^m(e) = e$. So $e = \sum \sigma^m(v_i) \otimes \sigma^m(s_i)$. By construction of V , the k -subspace of R generated by $\sigma^m(v_1), \dots, \sigma^m(v_n)$ contains V . Since V has dimension n , this shows that the $\sigma^m(v_i)$ are a k -basis of V . As k is inversive, we see that $\sigma^m(V) = V$. Let $W = V + \sigma(V) + \dots + \sigma^{m-1}(V)$. Then W is a k -subspace of R and $\sigma(W) = W$. Indeed, for dimension reasons, σ induces a bijection on W .

As V is contained in R_1 , every element v of V satisfies a separable polynomial over k . Thus also $\sigma(v)$ satisfies a separable polynomial over k (Lemma 1.1.4). It follows that all the elements of W satisfy separable polynomials over k . Therefore $k\{W\} = k[W] \subset R$ is an étale k -algebra. Because k is inversive and σ induces a bijection of W , we see that σ is a bijection on $k\{W\} = k[W]$. Thus $k\{W\}$ is a strongly σ -étale k - σ -algebra. Therefore $e \in k\{W\} \otimes_k S \subset \pi_0^\sigma(R) \otimes_k S$.

A similar argument shows that $e \in R \otimes_k \pi_0^\sigma(S)$ and it follows (using [Bou72, Prop. 7, Chapter I, §2.6, p. 18]) that

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

□

Lemma 4.2.24. *Let R be a strongly σ -étale k - σ -algebra and let $d_1, \dots, d_m \in R$ denote the primitive idempotent elements of R . Let $A_1 \uplus \dots \uplus A_n = \{1, \dots, m\}$ be the partition of $\{1, \dots, m\}$ corresponding to the cycle decomposition of the permutation τ of the d_i 's induced by σ (cf. Lemma 4.2.9). For $i = 1, \dots, n$ let $e_i = \sum_{j \in A_i} d_j$.*

Then $e_1, \dots, e_n$ are constant orthogonal idempotent elements with $e_1 + \dots + e_n = 1$ 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 $e_1 + \dots + e_n = d_1 + \dots + d_m = 1$. Any constant idempotent elements 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. □

Theorem 4.2.25. *Let R be a k - σ -algebra such that $\pi_0^\sigma(R)$ is strongly σ -étale. Let $e_1, \dots, e_n \in \pi_0^\sigma(R)$ be as in Lemma 4.2.24. Then the σ -connected components of $\text{Spec}(R)$ are $\mathcal{V}(1-e_1), \dots, \mathcal{V}(1-e_n)$. Moreover $\mathcal{V}(1-e_i)$ is isomorphic to $\text{Spec}(e_i R)$ as a σ -topological space.*

Proof. By Lemma 4.2.10 all the constant idempotent elements of R belong to $\pi_0^\sigma(R)$. So by Lemma 4.2.24 the constant idempotent elements $e_1, \dots, e_n$ satisfy the condition of Proposition 4.2.4. □

4.2.3 The group of difference connected components and the difference identity component

In this subsection we use the results proved about π_0^σ in the previous subsection to define the group of σ -connected components and the σ -identity component of a σ -algebraic group.

Let $\psi: R \rightarrow S$ be a morphism of k - σ -algebras. Because $\psi(R')$ is a strongly σ -étale k - σ -subalgebra of S for every strongly σ -étale k - σ -subalgebra R' of R (Lemma 4.2.12), we see that ψ maps $\pi_0^\sigma(R)$ into $\pi_0^\sigma(S)$. Thus π_0^σ defines a functor from the category of k - σ -algebras to the category of strongly σ -étale k - σ -algebras. Since π_0^σ is compatible with the tensor product (Lemma 4.2.23) we have:

Theorem 4.2.26. *Let R be a k - σ -Hopf algebra. Then $\pi_0^\sigma(R)$ is a k - σ -Hopf subalgebra of R . $\square$*

Let G be a σ -algebraic group. By Theorem 3.3.6 we can use Theorem 4.2.26 to define a quotient group $\pi_0^\sigma(G)$ of G . In fact, we will next characterize $\pi_0^\sigma(G)$ by a universal property.

Definition 4.2.27. *A σ -algebraic group G is called strongly σ -étale if $k\{G\}$ is a strongly σ -étale k - σ -algebra.*

Example 4.2.28. Let $0 \leq \alpha < n$ and $m \geq 1$ be integers and let G be the σ -closed subgroup of $\mathbb{G}_m$ given by

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

for any k - σ -algebra R . Then $k\{G\} = k[x, \sigma(x), \dots, \sigma^{m-1}(x)]$ 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 $1 \leq a < n$ 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

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

So after base extension to the inversive closure of k , it follows that $\sigma: k\{G\} \rightarrow k\{G\}$ is surjective. Because $k\{G\}$ is a finite dimensional vector space it follows that σ is injective. Therefore $k\{G\}$ is σ -separable (Proposition 1.1.8) and consequently G is strongly σ -étale.

Example 4.2.29. Let $\mathbf{G}$ be a finite group with an endomorphism $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ and let G be the σ -algebraic group associated to these data as in Example 2.1.15. We claim that G is strongly σ -étale if and only if $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ is an automorphism. Clearly $k\{G\}$ is étale, so the question is about the σ -separability of $k\{G\}$.

If $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ is not an automorphism there exist a $g \in \mathbf{G}$ that does not lie in the image. Therefore $\sigma(e_d) = 0$. So $k\{G\}$ is not σ -reduced and therefore not σ -separable. If $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ is an automorphism, then $\sigma: k\{G\} \rightarrow k\{G\}$ becomes bijective after base extension to the inversive closure of k . Therefore $k\{G\}$ is σ -separable (Proposition 1.1.8).

Example 4.2.30. Assume that k has positive characteristic. Let G be the Frobenius algebraic group associated to the algebraic group $\mathcal{G}$ as in Example 2.1.14. Then it follows from Corollary 1.1.9 that G is strongly σ -étale if and only if $\mathcal{G}$ is étale.

Proposition 4.2.31. *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 of σ -algebraic groups $G \rightarrow \pi_0^\sigma(G)$ such that for every morphism $G \rightarrow H$ of

σ -algebraic groups with H strongly σ -étale, there exists a unique morphism $\pi_0^\sigma(G) \rightarrow H$ making

$$\begin{array}{ccc} G & \xrightarrow{\quad} & \pi_0^\sigma(G) \\ & \searrow & \swarrow \text{dotted} \\ & H & \end{array}$$

commutative.

Proof. By Theorem 4.2.26 the k - σ -subalgebra $\pi_0^\sigma(k\{G\})$ is a k - σ -Hopf subalgebra of $k\{G\}$. It follows from Theorem 2.3.5 that $\pi_0^\sigma(k\{G\})$ is finitely σ -generated. So let F be a finite σ -generating set of $\pi_0^\sigma(k\{G\})$ over k . Since $\pi_0^\sigma(k\{G\})$ is the directed union of the strongly σ -étale k - σ -subalgebras of $k\{G\}$, F is contained in some strongly σ -étale k - σ -subalgebra R of $k\{G\}$. So $\pi_0^\sigma(k\{G\}) = k\{F\} \subset R \subset \pi_0^\sigma(k\{G\})$. Thus $\pi_0^\sigma(k\{G\}) = R$ is strongly σ -étale. Let $\pi_0^\sigma(G)$ denote the strongly σ -étale σ -algebraic group represented by $\pi_0^\sigma(k\{G\})$. The inclusion $\pi_0^\sigma(k\{G\}) \subset k\{G\}$ corresponds to a morphism $G \rightarrow \pi_0^\sigma(G)$ of σ -algebraic groups.

Let $\phi: G \rightarrow H$ be a morphism of σ -algebraic groups with H strongly σ -étale. By Lemma 4.2.12 the image of $\phi^*: k\{H\} \rightarrow k\{G\}$ is strongly σ -étale and is therefore contained in $\pi_0^\sigma(k\{G\})$. In other words, ϕ^* factors uniquely through the inclusion $\pi_0^\sigma(k\{G\}) \subset k\{G\}$. Turning the arrows around we obtain the required universal property. $\square$

As a corollary to the first part of the proof we obtain:

Corollary 4.2.32. *Let G be a σ -algebraic group. Then $\pi_0^\sigma(k\{G\})$ is strongly σ -étale.* $\square$

Definition 4.2.33. *Let G be a σ -algebraic group. The σ -algebraic group $\pi_0^\sigma(G)$ from Proposition 4.2.31 is called the group of σ -connected components of G . The kernel*

$$G^{\sigma\sigma}$$

of $G \rightarrow \pi_0^\sigma(G)$ 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 $G/G^{\sigma\sigma} = \pi_0^\sigma(G)$.

Recall that the topological space of a σ -algebraic group G is $\text{Spec}(k\{G\})$. As in Subsection 4.2.1 this is naturally a σ -topological space. By a σ -connected component of G we mean a σ -connected component of $\text{Spec}(k\{G\})$.

Theorem 4.2.34. *Let G be a σ -algebraic group. Then G has only finitely many σ -connected components. Moreover, the topological space of $G^{\sigma\sigma}$ is isomorphic (as a σ -topological space) to the σ -connected component of the topological space of G that contains $\mathfrak{m}_G$.*

Proof. As $\pi_0^\sigma(k\{G\})$ is strongly σ -étale (Corollary 4.2.32) the first statement follows immediately from Theorem 4.2.25. Let $d_1, \dots, d_m \in \pi_0^\sigma(k\{G\})$ and $e_1, \dots, e_n \in \pi_0^\sigma(k\{G\})$ be as in Lemma 4.2.24. The counit $\varepsilon: \pi_0^\sigma(k\{G\}) \rightarrow k$ 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 4.2.9 we have $\sigma(d_1) \in \{d_1, \dots, d_m\}$. 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 $G^{\sigma\sigma}$ we have $\mathbb{I}(G^{\sigma\sigma}) = (1 - e_1) \subset k\{G\}$. Therefore $k\{G^{\sigma\sigma}\} = k\{G\}/(1 - e_1)$ and consequently $\text{Spec}(k\{G^{\sigma\sigma}\})$ is isomorphic to $\mathcal{V}(1 - e_1) \subset \text{Spec}(k\{G\})$. We know from Theorem 4.2.25 that $\mathcal{V}(1 - e_1)$ is a σ -connected component and clearly $\mathfrak{m}_G \in \mathcal{V}(1 - e_1)$. $\square$

Lemma 4.2.35. *For a σ -algebraic group G , the following statements are equivalent:*

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

Proof. The equivalence of (ii) and (iii) is tautological. The implication (ii) $\Rightarrow$ (i) follows from the fact that the topological space of $G^{\sigma\sigma}$ is σ -connected by Theorem 4.2.34. Finally, let us show that (i) implies (iii). Let $d_1, \dots, d_m \in \pi_0^\sigma(k\{G\})$ and $e_1, \dots, e_n \in \pi_0^\sigma(k\{G\})$ be as in Lemma 4.2.24. 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 4.2.34 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 $e_1 \pi_0^\sigma(k\{G\}) = e_1 k \simeq k$. We know from Theorem 4.2.25 that G has n σ -connected components. By assumption $n = 1$. So $\pi_0^\sigma(k\{G\}) = k$. $\square$

Definition 4.2.36. *A σ -algebraic group satisfying the equivalent conditions of Lemma 4.2.35 is called σ -connected.*

As an immediate corollary to Theorem 4.2.34 we obtain:

Corollary 4.2.37. *Let G be a σ -algebraic group. Then $G^{\sigma\sigma}$ is σ -connected.* $\square$

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

Proposition 4.2.38. *Let G be a σ -algebraic group and K a σ -field extension of k . Then*

$$\pi_0^\sigma(G_K) = \pi_0^\sigma(G)_K \quad \text{and} \quad (G^{\sigma\sigma})_K = (G_K)^{\sigma\sigma}.$$

Proof. This is clear from Lemma 4.2.22. $\square$

A connected algebraic group is absolutely connected ([Mil12, Prop. 3.8, Chapter XIII, p. 210]). A similar results holds in our setting:

Corollary 4.2.39. *Let G be a σ -connected σ -algebraic group. Then G is absolutely σ -connected, i.e., G_K is σ -connected for every σ -field extension $K|k$.* $\square$

Theorem 4.2.40. *Let G be a σ -algebraic group. Then $G^{\sigma\sigma}$ is a characteristic subgroup of G .*

Proof. By Lemma 4.1.26 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 $\psi(\pi_0^\sigma(k\{G\} \otimes_k R)) \subset \pi_0^\sigma(k\{G\} \otimes_k R)$. Using Lemma 4.2.23, we obtain

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

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

The following proposition is useful for determining the σ -identity component.

Proposition 4.2.41. *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 4.2.31 a commutative diagram

$$\begin{array}{ccc} G & \xrightarrow{\quad} & \pi_0^\sigma(G) \\ & \searrow & \swarrow \text{dotted} \\ & G/N & \end{array}$$

So $G^{\sigma o} \leq N$ and the kernel of $N \rightarrow \pi_0^\sigma(G)$ is $G^{\sigma o}$. But by Proposition 4.2.31 again, $N \rightarrow \pi_0^\sigma(G)$ factors through $\pi_0^\sigma(N) = 1$. So the kernel of $N \rightarrow \pi_0^\sigma(G)$ is N . So $N = G^{\sigma o}$. $\square$

Alternatively, Proposition 4.2.41 can be restated as: For any σ -algebraic group G , there exists a unique exact sequence

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

with $G^{\sigma o}$ σ -connected and $\pi_0^\sigma(G)$ strongly σ -étale.

Proposition 4.2.42. *If $1 \rightarrow N \rightarrow G \rightarrow H \rightarrow 1$ is an exact sequence of σ -algebraic groups such that N and H are σ -connected, then G is σ -connected.*

Proof. By Proposition 4.2.31, the morphism $N \rightarrow G \rightarrow \pi_0^\sigma(G)$ factors through the morphism $N \rightarrow \pi_0^\sigma(N) = 1$. So N is contained in $G^{\sigma o}$, i.e., in the kernel of $G \rightarrow \pi_0^\sigma(G)$. We therefore have an induced surjective morphism $G/N \rightarrow \pi_0^\sigma(G)$. But $G/N \simeq H$ is σ -connected, so $G/N \rightarrow \pi_0^\sigma(G)$ factors through $\pi_0^\sigma(G/N) = 1$. Thus $\pi_0^\sigma(G) = 1$. $\square$

An algebraic group, when considered as a σ -algebraic group is σ -connected:

Proposition 4.2.43. *Let $\mathcal{G}$ be an algebraic group. Then $[\sigma]_k \mathcal{G}$ is a σ -connected σ -algebraic group.*

Proof. This is clear from Corollary 4.2.6. $\square$

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

Proposition 4.2.44. *Let G be a σ -algebraic group. Then $\sigma\text{-dim}(G^{\sigma o}) = \sigma\text{-dim}(G)$, $\text{ord}(G^{\sigma o}) = \text{ord}(G)$ and $\text{ld}(G^{\sigma o}) = \text{ld}(G)$.*

Proof. By Corollaries 3.2.12 and 3.2.14 it suffices to note that $\sigma\text{-dim}(\pi_0^\sigma(G)) = 0$, $\text{ord}(\pi_0^\sigma(G)) = 0$ and $\text{ld}(\pi_0^\sigma(G)) = 1$. $\square$

For later use we record a simple lemma:

Lemma 4.2.45. *Let $G \twoheadrightarrow H$ be a surjective morphism of σ -algebraic groups. If G is σ -connected then H is σ -connected.*

Proof. The dual morphism $k\{H\} \hookrightarrow k\{G\}$ is injective. So if $\pi_0^\sigma(k\{G\}) = k$, then also $\pi_0^\sigma(k\{H\}) = k$. $\square$

Example 4.2.46. Let $n \geq 2$ be an integer and let G be the σ -algebraic group given by

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

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 $\text{Spec}(k\{G\})$ is a discrete topological space. Suppose X_1 and X_2 are non-empty disjoint σ -stable subsets of $\text{Spec}(k\{G\})$. 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. Note that G is an example of a σ -infinitesimal σ -algebraic group (see Definition 6.3.1). In Theorem 6.3.20 we will show that any σ -infinitesimal σ -algebraic group is σ -connected.

Example 4.2.47. Let $n \geq 2$ be an integer and let G be the σ -algebraic group given by

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

for any k - σ -algebra R . We claim that G is not σ -connected. Indeed, for simplicity let us assume that the characteristic of k is zero or does not divide n . Then it follows from Example 4.2.28 that $k\{G\}$ is strongly σ -étale. So $G = \pi_0^\sigma(G)$ and $G^{\sigma\sigma} = 1$.

The number of σ -connected components of the σ -algebraic group in Example 4.2.47 cannot be easily read off. Indeed, the following example shows that the number of σ -connected components does not only depend on the underlying field of the base difference field, but it explicitly depends on the endomorphism $\sigma: k \rightarrow k$.

Example 4.2.48. 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 $\text{Spec}(k\{G\})$ consists of two elements and σ is the identity map on $\text{Spec}(k\{G\})$. 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 $\text{Spec}(k\{G\})$ 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 $\text{Spec}(k\{G\})$ 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 $\pi_0^\sigma(k\{G\}) = k\{G\}$.

The following example shows how we can use Proposition 4.2.42 to show that a σ -algebraic group is σ -connected.

Example 4.2.49. Let G be the σ -closed subgroup of $\mathbb{G}_m$ given by

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

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 $\phi: G \rightarrow H$ be the morphism given by

$$\phi_R: G(R) \rightarrow H(R), g \mapsto \sigma(g).$$

Then the dual map $\phi^*: k\{H\} \rightarrow k\{G\}$ is injective and so ϕ is surjective. 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 $1 \rightarrow N \rightarrow G \rightarrow H \rightarrow 1$. 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 Proposition 4.2.43 that H is σ -connected. Because N is σ -connected by Example 4.2.46, Proposition 4.2.42 shows that G is σ -connected.

The following example shows how Proposition 4.2.41 can be used to determine the σ -identity component.

Example 4.2.50. Let G be the σ -algebraic group given by

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

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 $G^{\sigma\sigma}$ is given by $G^{\sigma\sigma}(R) = \{g \in R^\times \mid g^2 = 1\}$.

Let H be the σ -algebraic group given by $H(R) = \{g \in R^\times \mid g^2 = 1, \sigma(g) = g\} \leq \mathbb{G}_m(R)$ for any k - σ -algebra R . It follows from $g^4 = 1$ and $g^2 \sigma(g)^2 = 1$ that $\sigma(g^2) = g^2$. Therefore we can define a morphism of σ -algebraic groups

$$\phi: G \rightarrow H, g \mapsto g^2.$$

The dual morphism $\phi^*: k\{H\} \rightarrow k\{G\}$ is injective, so ϕ is surjective. The kernel N of ϕ is given by $N(R) = \{g \in R^\times \mid g^2 = 1\}$. It follows from Proposition 4.2.43 that N is σ -connected. Moreover, by Example 4.2.28 the σ -algebraic group H is strongly σ -étale. Therefore it follows from Proposition 4.2.41 that $G^{\sigma\sigma} = N$ 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 Theorem 4.2.25 that G has two σ -connected components.

Example 4.2.51. Let $\mathbf{G}$ be a finite group with an endomorphism $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ and let G be the σ -algebraic group associated to these data as in Example 2.1.15. We will show that G is σ -connected if and only if some power of $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ is the trivial endomorphism ($g \mapsto 1$) of $\mathbf{G}$.

Let us start by determining the topological space of $G^{\sigma\sigma}$. Note that $\text{Spec}(k\{G\})$ is naturally in bijection with $\mathbf{G}$: An element $g \in \mathbf{G}$ corresponds to the prime ideal generated by $1 - e_g$. We have a commutative diagram

$$\begin{array}{ccc} \text{Spec}(k\{G\}) & \xrightarrow{\simeq} & \mathbf{G} \\ \sigma \downarrow & & \downarrow \sigma \\ \text{Spec}(k\{G\}) & \xrightarrow{\simeq} & \mathbf{G} \end{array}$$

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

The cosets $g\mathbf{N}$ of $\mathbf{N}$ in $\mathbf{G}$ need not correspond to σ -connected components of G because they may not be stable under σ . Note that the induced map $\sigma: \mathbf{G}/\mathbf{N} \rightarrow \mathbf{G}/\mathbf{N}$ 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 $\mathbf{G}/\mathbf{N}$.

Example 4.2.52. Let G be a Frobenius algebraic group as in Example 2.1.14. We claim that the σ -connected components of G coincide with the connected components of G . Indeed, as $\sigma: k\{G\} \rightarrow k\{G\}$, $f \mapsto f^q$ we have $\sigma^{-1}(\mathfrak{p}) = \{f \in k\{G\} \mid f^q \in \mathfrak{p}\} = \mathfrak{p}$ for any prime ideal $\mathfrak{p}$ of $k\{G\}$. Thus σ is the identity map on $\text{Spec}(k\{G\})$. So the σ -topology on $\text{Spec}(k\{G\})$ agrees with the usual (Zariski) topology.

Let R be a σ -ring. The reflexive closure of the nilradical $\sqrt{0}^*$ agrees with the radical of the reflexive closure $\sqrt{(0)^*}$ and both are equal to

$$\{f \in R \mid \exists m \geq 1, n \geq 0 : \sigma^n(f)^m = 0\}.$$

This implies that for a σ -algebraic group G we have $(G_{\text{red}})_{\sigma\text{-red}} = (G_{\sigma\text{-red}})_{\text{red}}$. For simplicity we will write

$$G_{\sigma\text{-red,red}}$$

for this. Note that $G_{\sigma\text{-red,red}}$ is a σ -closed subgroup of G if k is perfect and inversive (Corollary 2.5.7).

Our next goal is to show that $\pi_0^\sigma(G_{\sigma\text{-red,red}})$ and $\pi_0^\sigma(G)$ are isomorphic. This will be needed to prove a structure theorem for finite σ -algebraic groups later (Theorem 6.3.9). To prove $\pi_0^\sigma(G_{\sigma\text{-red,red}}) \simeq \pi_0^\sigma(G)$ we need several preparatory results.

Lemma 4.2.53. *Let k be a perfect and inversive σ -field, R a k - σ -algebra and K a σ -field extension of k . Then*

$$\sqrt{0}^* \otimes_k K = \sqrt{0}^* \subset R \otimes_k K.$$

Proof. The inclusion “ $\subset$ ” is obvious. To prove “ $\supset$ ” it suffices to note that $(R/\sqrt{0}^*) \otimes_k K$ is reduced and σ -reduced by Lemma 2.5.5, i.e., $\sqrt{0}^* \otimes_k K$ is reflexive and radical. $\square$

Similarly to Lemma 4.2.53 one shows that:

Lemma 4.2.54. *Let k be an inversive σ -field, R a k - σ -algebra and K a σ -field extension of k . Then $(0)^* \otimes_k K = (0)^* \subset R \otimes_k K$* $\square$

As seen in Example 4.2.48, the vector space dimension of $\pi_0^\sigma(k\{G\})$ may be strictly larger than the number of σ -connected components of G , even if k is algebraically closed. To obtain an equality in this respect we also have to take into account the higher powers of σ . Note that if (R, σ) is a difference ring, then (R, σ^d) is also a difference ring for any integer $d \geq 1$.

Let G be a σ -algebraic group. Then for every integer $d \geq 1$, $(k\{G\}, \sigma^d)$ is a difference Hopf algebra over the difference field (k, σ^d) .

Lemma 4.2.55. *Let G be a σ -algebraic group and $d \geq 1$ an integer. Then*

$$\pi_0^\sigma(k\{G\}) = \pi_0^{\sigma^d}(k\{G\}).$$

Proof. The inclusion $\pi_0^\sigma(k\{G\}) = \pi_0^{\sigma^d}(k\{G\})$ follows from the fact that a σ -separable k - σ -algebra is a σ^d -separable k - σ^d -algebra. To prove the equality we may assume that k is algebraically closed (Lemma 4.2.22). Then the claim follows from Lemma 4.2.19 because an idempotent element is periodic with respect to σ if and only if it is periodic with respect to σ^d . $\square$

Proposition 4.2.56. *Let G be a σ -algebraic group. Then the dimension of $\pi_0^\sigma(k\{G\})$ as a k -vector space is greater than or equal to the number of σ -connected components of G . Indeed,*

$$\dim_k(\pi_0^\sigma(k\{G\})) = \max_{d,K} |\{\sigma^d\text{-connected components of } G_K\}|, \quad (4.3)$$

where d ranges over all positive integers and K over all σ -field extensions of k . Moreover, if k is separably algebraically closed, then

$$\dim_k(\pi_0^\sigma(k\{G\})) = \max_d |\{\sigma^d\text{-connected components of } G\}|. \quad (4.4)$$

Proof. By Theorem 4.2.25 the number of σ -connected components of G is less than or equal to the number of primitive idempotent elements of $\pi_0^\sigma(k\{G\})$, and this number is clearly less than or equal to $\dim_k(\pi_0^\sigma(k\{G\}))$. Because $\dim_k(\pi_0^\sigma(k\{G\}))$ is invariant under extension of the base σ -field, this, together with Lemma 4.2.55 proves the “ $\leq$ ” in Equations (4.3) and (4.4).

To obtain equality we may assume that k is separably closed. Then $\dim_k(\pi_0^\sigma(k\{G\}))$ equals the number of primitive idempotent elements of $\pi_0^\sigma(k\{G\})$. In the notation of Lemma 4.2.24, it suffices to find a d such that $\sigma^d(d_i) = d_i$ for $i = 1, \dots, m$ (Theorem 4.2.25). It thus suffices to choose d such that τ^d is the identity. $\square$

Proposition 4.2.57. *Let G be a σ -algebraic group and assume that k is perfect and inversive. Then there is a natural bijection between the σ -connected components of G and the σ -connected components of $G_{\sigma\text{-red,red}}$.*

Proof. Let $Z_1, \dots, Z_n$ denote the σ -connected components of G . Let $\mathfrak{a} = \mathbb{I}(G_{\sigma\text{-red,red}}) = \sqrt{0}^* \subset k\{G\}$ denote the defining ideal of $G_{\sigma\text{-red,red}}$. We identify the topological space of $G_{\sigma\text{-red,red}}$ with $\mathcal{V}(\mathfrak{a}) \subset \text{Spec}(k\{G\})$. We will show that $Z_i \mapsto Z_i \cap \mathcal{V}(\mathfrak{a})$ defines a bijection between the σ -connected components of G and the σ -connected components of $\mathcal{V}(\mathfrak{a})$. For $i = 1, \dots, n$ let $\mathfrak{a}_i \subset k\{G\}$ denote the radical σ -ideal such that $\mathcal{V}(\mathfrak{a}_i) = Z_i$. As $\text{Spec}(k\{G\}) = Z_1 \cup \dots \cup Z_n$ we see that $\sqrt{0} = \mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_n$. Therefore $\mathfrak{a} = \sqrt{0}^* = \mathfrak{a}_1^* \cap \dots \cap \mathfrak{a}_n^*$.

We have $Z_i \cap \mathcal{V}(\mathfrak{a}) = \mathcal{V}(\mathfrak{a}_i + \mathfrak{a})$. Since $\mathfrak{a} \subset \mathfrak{a}_i^*$ we see that $\mathfrak{a}_i + \mathfrak{a} \subset \mathfrak{a}_i^* \neq k\{G\}$. Hence $Z_i \cap \mathcal{V}(\mathfrak{a}) \neq \emptyset$.

To prove the proposition it suffices to show that $Z_i \cap \mathcal{V}(\mathfrak{a})$ is σ -connected for every i . Suppose there exist non-empty σ -closed sets X_1, X_2 such that $Z_i \cap \mathcal{V}(\mathfrak{a}) = X_1 \uplus X_2$. Let $\mathfrak{b}_1, \mathfrak{b}_2 \subset k\{G\}$ denote the radical σ -ideals such that $X_1 = \mathcal{V}(\mathfrak{b}_1)$ and $X_2 = \mathcal{V}(\mathfrak{b}_2)$. Then $\sqrt{\mathfrak{a}_i + \mathfrak{a}} = \mathfrak{b}_1 \cap \mathfrak{b}_2$.

For every $f \in \mathfrak{a}$ there exist integers $\alpha \geq 0$ and $\beta \geq 1$ such that $\sigma^\alpha(f)^\beta = 0$. Because k is perfect and inversive $\mathfrak{a}$ is a Hopf ideal (Corollary 2.5.7) and it follows from Theorem 2.3.1 that $\mathfrak{a}$ is finitely σ -generated. Thus there exists $\alpha \geq 0$ such that $\sigma^\alpha(\mathfrak{a}) \subset \sqrt{0}$. For $j = 1, 2$ set

$$Y_j = \{z \in Z_i \mid \sigma^\alpha(z) \in X_j\} = \{\mathfrak{p} \in \mathcal{V}(\mathfrak{a}_i) \mid \mathfrak{b}_j \subset \sigma^{-\alpha}(\mathfrak{p})\} = \mathcal{V}(\mathfrak{a}_i) \cap \mathcal{V}(\sigma^\alpha(\mathfrak{b}_j)).$$

For every prime ideal $\mathfrak{p} \in \mathcal{V}(\mathfrak{a}_i) = Z_i$ we have $\mathfrak{a}_i \subset \sigma^{-\alpha}(\mathfrak{a}_i) \subset \sigma^{-\alpha}(\mathfrak{p})$. As $\sigma^\alpha(\mathfrak{a}) \subset \sqrt{0} \subset \mathfrak{p}$ we see that also $\mathfrak{a} \subset \sigma^{-\alpha}(\mathfrak{p})$. Hence $\mathfrak{b}_1 \cap \mathfrak{b}_2 = \sqrt{\mathfrak{a}_i + \mathfrak{a}} \subset \sigma^{-\alpha}(\mathfrak{p})$. So $\mathfrak{p} \in Y_1$ or $\mathfrak{p} \in Y_2$. This shows that $Z_i = Y_1 \cup Y_2$. As Y_1 and Y_2 are σ -closed and $Y_1 \cap Y_2 = \emptyset$, this contradicts the σ -connectedness of Z_i . $\square$

Theorem 4.2.58. *Let G be a σ -algebraic group and assume that k is perfect and inversive. Then*

$$\pi_0^\sigma(G_{\sigma\text{-red,red}}) \simeq \pi_0^\sigma(G).$$

Proof. We will show that the morphism $\pi_0^\sigma(G_{\sigma\text{-red,red}}) \rightarrow \pi_0^\sigma(G)$ induced by the inclusion $G_{\sigma\text{-red,red}} \hookrightarrow G$ is an isomorphism. Let $\mathfrak{a} = \mathbb{I}(G_{\sigma\text{-red,red}}) = \sqrt{0}^* \subset k\{G\}$ denote the defining ideal of $G_{\sigma\text{-red,red}}$. In terms of the coordinate rings we have to show that the morphism $k\{G\} \rightarrow k\{G\}/\mathfrak{a}$ induces an isomorphism $\psi: \pi_0^\sigma(k\{G\}) \rightarrow \pi_0^\sigma(k\{G\}/\mathfrak{a})$. The k - σ -algebra $\pi_0^\sigma(k\{G\})$ is reduced and σ -reduced. Because for every $f \in \mathfrak{a}$ there exist integers $n \geq 0$ and $m \geq 1$ such that $\sigma^n(f)^m = 0$, it follows that $\mathfrak{a} \cap \pi_0^\sigma(k\{G\}) = 0$, i.e., ψ is injective.

Let $\bar{k}$ denote the algebraic closure of k equipped with an extension of $\sigma: k \rightarrow k$. It follows from Lemma 4.2.53 that $(G_{\bar{k}})_{\sigma\text{-red,red}} = (G_{\sigma\text{-red,red}})_{\bar{k}}$. Together with Lemma 4.2.22 this shows that to prove the surjectivity of ψ , we may assume that k is algebraically closed. Indeed, it suffices to show that $\pi_0^\sigma(k\{G\})$ and $\pi_0^\sigma(k\{G\}/\mathfrak{a})$ have the same dimension as k -vector spaces. But by Proposition 4.2.56, the dimension of $\pi_0^\sigma(k\{G\})$ equals the maximal number of the σ^d -connected components of G , where d ranges over the positive integers. The reflexive closures of the radical of the zero ideal of $k\{G\}$ with respect to σ and σ^d are equal. So it follows from Proposition 4.2.57 that G and $G_{\sigma\text{-red,red}}$ have the same number of σ^d -connected components. In summary, this shows that $\dim_k(\pi_0^\sigma(k\{G\})) = \dim_k(\pi_0^\sigma(k\{G\}/\mathfrak{a}))$. $\square$

Chapter 5

Group theory

In this chapter we study group theoretic properties of σ -algebraic groups. The main result is an analog of the Jordan-Hölder theorem for σ -algebraic groups. It shows that, at least under rather mild assumptions, a σ -algebraic group can be decomposed into certain simpler pieces, namely almost-simple σ -algebraic groups. This decomposition also satisfies a uniqueness property. The proof of the uniqueness part of the Jordan-Hölder theorem for σ -algebraic groups follows along the lines of the standard proof of the usual Jordan-Hölder theorem for finite groups. We therefore need to transfer statements well-known for finite groups, such as the Butterfly lemma, to difference algebraic groups. This requires some flexibility when working with quotients. In particular, we need the analogs of the (Noether) isomorphism theorems for groups.

The task of proving the analogs of the isomorphism theorems is complicated by the fact that for a normal σ -closed subgroup N of a σ -algebraic group G , the quotient G/N is, at least initially, not easy accessible. As for algebraic groups, the functor $R \rightsquigarrow G(R)/N(R)$ need not be representable, in particular, it is distinct from G/N .

If we could identify G with $G(k)$, and $(G/N)(k)$ with $G(k)/N(k)$, where k is some “sufficiently large” difference field, we could apply the isomorphism theorems directly. This approach is not possible for us for several reasons. Firstly, we want to avoid restrictions on the base field. Secondly, the identification of G with $G(k)$ is only feasible for perfectly σ -reduced σ -algebraic groups. Thirdly, identifying G with $G(k)$ does introduce some blemishes. For example, the morphism of σ -algebraic groups $\phi: \mathrm{GL}_n \rightarrow \mathrm{GL}_n$, $g \mapsto \sigma(g)$ is such that $\phi_k: \mathrm{GL}_n(k) \rightarrow \mathrm{GL}_n(k)$ has trivial kernel, but ϕ is not a σ -closed embedding. Indeed, the kernel of ϕ is non-trivial.

For algebraic groups, the theory of sheaves (see [DG70, Chapter III]) provides an elegant and powerful tool to deal with quotients. In the first section of this chapter we adapt the theory of sheaves to difference algebra. The main result (Theorem 5.1.8) provides a canonical way to associate a sheaf to any functor from $k\text{-}\sigma\text{-Alg}$ to **Sets**. The relevance of Theorem 5.1.8 for quotients stems from the fact that the sheaf associated to the functor $R \rightsquigarrow G(R)/N(R)$ equals G/N . In the second section we then show how this result can be used to deduce the isomorphism theorems for difference algebraic groups from the isomorphism theorems for (abstract) groups. In the third section we prove the Jordan-Hölder theorem. While it may be possible to prove the isomorphism theorems for difference algebraic groups without explicitly introducing sheaves, we expect that Theorem 5.1.8 will also be useful in other situations, for example, when considering actions of difference algebraic groups on difference varieties, where the existence of a quotient in the category of difference varieties is problematic.

5.1 Sheaves

Our proof of Theorem 5.1.8 follows the proof of Theorem 1.8, Chapter III, §1 [DG70] rather closely.

Let k be a σ -field. If $(R_i)_{i \in I}$ is a finite family of k - σ -algebras, then the product $\prod_{i \in I} R_i$ is naturally a k - σ -algebra by $\sigma((r_i)_{i \in I}) = (\sigma(r_i))_{i \in I}$. The projections $\prod_{i \in I} R_i \rightarrow R_i$ are morphisms of k - σ -algebras. Recall that a morphism $\psi: R \rightarrow S$ of k - σ -algebras is called faithfully flat if the corresponding morphism $\psi^\sharp: R^\sharp \rightarrow S^\sharp$ of k -algebras is faithfully flat.

Definition 5.1.1. *Let R be a k - σ -algebra. A finite family $(R_i)_{i \in I}$ of R - σ -algebras is called R -covering if the canonical map $R \rightarrow \prod_{i \in I} R_i$ is faithfully flat.*

Note that if $(R_i)_{i \in I}$ and $(S_j)_{j \in J}$ are two R -covering families, then $(R_i \otimes_R S_j)_{(i,j) \in I \times J}$ is an R -covering family. If $R \rightarrow S$ is a morphism of k - σ -algebras and $(R_i)_{i \in I}$ is an R -covering family, then $(R_i \otimes_R S)_{i \in I}$ is an S -covering family.

Recall that a sequence of sets $A \xrightarrow{\alpha} B \xrightleftharpoons[\beta_2]{\beta_1} C$ is called exact if α is the equalizer of β_1 and β_2 , i.e., $\beta_1 \alpha = \beta_2 \alpha$ and for $b \in B$ with $\beta_1(b) = \beta_2(b)$ there exists a unique $a \in A$ with $\alpha(a) = b$.

Definition 5.1.2. *Let F be a functor from k - σ -Alg to Sets. Then F is called a sheaf, if for every k - σ -algebra R and every R -covering family $(R_i)_{i \in I}$ the sequence*

$$F(R) \xrightarrow{\alpha} \prod_i F(R_i) \xrightleftharpoons[\beta_2]{\beta_1} \prod_{i,j} F(R_i \otimes_R R_j) \quad (5.1)$$

is exact.

The maps in the above sequence are the obvious ones: The i -th component of α is induced from $R \rightarrow R_i$. The (i, j) -component of β_1 (respectively β_2) is the projection onto $F(R_i)$ (respectively $F(R_j)$) followed by the map induced from $R_i \rightarrow R_i \otimes_R R_j$, $f \mapsto f \otimes 1$ (respectively $R_j \rightarrow R_i \otimes_R R_j$, $f \mapsto 1 \otimes f$).

A morphism of sheaves is a morphism of functors.

Lemma 5.1.3. *A functor F from k - σ -Alg to Sets is a sheaf if and only if*

- (i) *for every finite family of k - σ -algebras $(R_i)_{i \in I}$, the map $F(\prod_{i \in I} R_i) \rightarrow \prod_{i \in I} F(R_i)$ is bijective;*
- (ii) *for every faithfully flat morphism of k - σ -algebras $R \rightarrow S$ the sequence*

$$F(R) \rightarrow F(S) \rightrightarrows F(S \otimes_R S)$$

is exact.

Proof. Let us first assume that F is a sheaf. If we take R as the zero ring and the R -covering family as the empty family, then the exactness of (5.1) signifies that $F(R)$ consists of one element.

Let $(R_i)_{i \in I}$ be a finite family of k - σ -algebras. If we set $R = \prod_i R_i$ and consider R_i as a R - σ -algebra via the projection $R \rightarrow R_i$, then the canonical map $R \rightarrow \prod_i R_i$ is the identity and $R_i \otimes_R R_j = 0$ for $i \neq j$, whereas $R_i \otimes_R R_j = R_i$ for $i = j$. Thus the exactness of (5.1) in this case yields condition (i) since β_1 and β_2 are reduced to the identity map. Clearly a sheaf satisfies condition (ii).

Conversely, assume that F satisfies (i) and (ii). Let $(R_i)_{i \in I}$ be an R -covering family. Taking $S = \prod_i R_i$ and applying (i) to (ii) yields the exactness of (5.1). $\square$

Corollary 5.1.4. *Every representable functor from $k\text{-}\sigma\text{-Alg}$ to **Sets** is a sheaf. In particular, every σ -variety and every σ -algebraic group is a sheaf.*

Proof. Let A be a $k\text{-}\sigma$ -algebra and $F = \text{Hom}(A, -)$. Clearly,

$$\text{Hom}(A, \prod_i R_i) \simeq \prod_i \text{Hom}(A, R_i),$$

for every finite family $(R_i)_{i \in I}$ of $k\text{-}\sigma$ -algebras. So F satisfies condition (i) of Lemma 5.1.3.

To verify (ii), let $R \rightarrow S$ be a faithfully flat morphism of $k\text{-}\sigma$ -algebras. Then

$$R \rightarrow S \rightrightarrows S \otimes_R S$$

is exact. (See e.g. [Wat79, Section 13.1, p. 104].) Therefore

$$\text{Hom}(A, R) \rightarrow \text{Hom}(A, S) \rightrightarrows \text{Hom}(A, S \otimes_R S)$$

is exact. □

Thus the category of σ -varieties is a full subcategory of the category of sheaves.

Definition 5.1.5. *A subfunctor D of a functor $F: k\text{-}\sigma\text{-Alg} \rightarrow \mathbf{Sets}$ is called fat if for every $k\text{-}\sigma$ -algebra R and every $a \in F(R)$ there exists an R -covering family $(R_i)_{i \in I}$ such that the image of a in $F(R_i)$ belongs to $D(R_i)$ for every $i \in I$.*

Some of the constructions with σ -varieties explained in Section 1.2 carry over to arbitrary functors from $k\text{-}\sigma\text{-Alg}$ to **Sets** without difficulty: If $\phi: E \rightarrow F$ is a morphism of functors and $D \subset F$ a subfunctor, then $\text{Im}(\phi)$ and $\phi^{-1}(D)$ may be defined as in Section 1.2; similarly for the intersection of subfunctors.

Note that if $\phi: E \rightarrow F$ is a morphism of functors and $D \subset F$ is fat, then $\phi^{-1}(D) \subset E$ is fat. As in [DG70, p. 285] one verifies: If D is a fat subfunctor of F and D_1 is a fat subfunctor of D , then D_1 is a fat subfunctor of F . If D_1 and D_2 are fat subfunctors of E , then $D_1 \cap D_2$ is a fat subfunctor of E .

Let R be a $k\text{-}\sigma$ -algebra. To simplify the notation we will write

$$\text{Sp}^\sigma(R)$$

for the functor $\text{Hom}(R, -): k\text{-}\sigma\text{-Alg} \rightarrow \mathbf{Sets}$. If $\psi: R \rightarrow S$ is a morphism of $k\text{-}\sigma$ -algebras, there is an induced morphism of functors $\text{Sp}^\sigma(\psi): \text{Sp}^\sigma(S) \rightarrow \text{Sp}^\sigma(R)$. Recall (See e.g. [EH00, Lemma VI-1 (a)].) that for any functor $F: k\text{-}\sigma\text{-Alg} \rightarrow \mathbf{Sets}$ and any $k\text{-}\sigma$ -algebra R there is a canonical bijection

$$F(R) \simeq \text{Hom}(\text{Sp}^\sigma(R), F)$$

Indeed, F and $\text{Hom}(\text{Sp}^\sigma(-), F)$ are isomorphic as functors. An element $a \in F(R)$ gives rise to a morphism $\text{Sp}^\sigma(R) \rightarrow F$ as follows: For a $k\text{-}\sigma$ -algebra S and $\psi \in \text{Hom}(R, S)$ let $\text{Sp}^\sigma(R)(S) \rightarrow F(S)$ be defined by sending ψ to $F(\psi)(a)$. Conversely, from a morphism $\text{Sp}^\sigma(R) \rightarrow F$ we obtain an element in $F(R)$ by considering the image of the identity under $\text{Sp}^\sigma(R)(R) \rightarrow F(R)$.

Lemma 5.1.6. *Let R be a $k\text{-}\sigma$ -algebra. Then a subfunctor D of $\text{Sp}^\sigma(R)$ is fat if and only if there exists an R -covering family $(R_i)_{i \in I}$ such that $\text{Im}(\text{Sp}^\sigma(R_i) \rightarrow \text{Sp}^\sigma(R)) \subset D$ for all $i \in I$.*

Proof. If $D \subset \mathrm{Sp}^\sigma(R)$ is fat, we can apply Definition 5.1.5 to the element

$$a = \mathrm{id}_R \in \mathrm{Hom}(R, R) = \mathrm{Sp}^\sigma(R)(R)$$

to find an R -covering family $(R_i)_{i \in I}$ such that the maps $R \rightarrow R_i$ lie in $D(R_i) \subset \mathrm{Sp}^\sigma(R)(R_i)$ for every $i \in I$. Let $\psi: R_i \rightarrow S$ be a morphism of k - σ -algebras. Since

$$\mathrm{Sp}^\sigma(R)(\psi): \mathrm{Sp}^\sigma(R)(R_i) \rightarrow \mathrm{Sp}^\sigma(R)(S)$$

maps $D(R_i)$ into $D(S)$ we see that the composition $R \rightarrow R_i \rightarrow S$ lies in $D(S) \subset \mathrm{Sp}^\sigma(R)(S)$. Therefore the image of $\mathrm{Sp}^\sigma(R)(S) \rightarrow \mathrm{Sp}^\sigma(R)(S)$ lies in $D(S)$. This shows that

$$\mathrm{Im}(\mathrm{Sp}^\sigma(R_i) \rightarrow \mathrm{Sp}^\sigma(R)) \subset D.$$

Conversely, if $(R_i)_{i \in I}$ verifies the condition of the lemma and $a: R \rightarrow S$ is a morphism of k - σ -algebras, then $(R_i \otimes_R S)_{i \in I}$ is an S -covering family. By assumption, $R \rightarrow R_i \rightarrow R_i \otimes_R S$ lies in $D(R_i \otimes_R S) \subset \mathrm{Sp}^\sigma(R)(R_i \otimes_R S)$. But $R \rightarrow R_i \rightarrow R_i \otimes_R S$ equals $R \rightarrow S \rightarrow R_i \otimes_R S$. Therefore $\mathrm{Sp}^\sigma(R)(S) \rightarrow \mathrm{Sp}^\sigma(R)(R_i \otimes_R S)$ maps a into $D(R_i \otimes_R S)$. $\square$

Proposition 5.1.7. *For a functor $F: k\text{-}\sigma\text{-Alg} \rightarrow \mathbf{Sets}$ the following properties are equivalent:*

- (i) *The functor F is a sheaf.*
- (ii) *If D is a fat subfunctor of a functor $E: k\text{-}\sigma\text{-Alg} \rightarrow \mathbf{Sets}$ and $\phi: D \rightarrow F$ a morphism, then there exists a unique extension of ϕ to E .*
- (iii) *If R is a k - σ -algebra, D a fat subfunctor of $\mathrm{Sp}^\sigma(R)$ and $\phi: D \rightarrow F$ a morphism, then there exists a unique extension of ϕ to $\mathrm{Sp}^\sigma(R)$.*

Proof. Let us start with (i) $\Rightarrow$ (ii). Let R be a k - σ -algebra and $a \in E(R)$. We have to construct $\phi(a) \in F(R)$. Since D is fat, there exists an R -covering family $(R_i)_{i \in I}$ such that the image a_i of a in $E(R_i)$ belongs to $D(R_i)$. Since $a \in E(R)$ we see that $(a_i)_{i \in I} \in \prod_i D(R_i) \subset \prod_i E(R_i)$ lies in the equalizer of the top row of

$$\begin{array}{ccc} \prod_i D(R_i) & \rightrightarrows & \prod_{i,j} D(R_i \otimes_R R_j) \\ \downarrow & & \downarrow \\ \prod_i F(R_i) & \rightrightarrows & \prod_{i,j} F(R_i \otimes_R R_j). \end{array}$$

Therefore $(\phi(a_i))_{i \in I} \in \prod_i F(R_i)$ lies in the equalizer of the bottom row. Since F is a sheaf there exists a unique $b \in F(R)$ mapping to $(\phi(a_i))_{i \in I}$. Set $\phi(a) = b$. We have to show that this definition does not depend on the choice of the R -covering family $(R_i)_{i \in I}$. So let $(S_j)_{j \in J}$ be another R -covering family such that the image of $a \in E(R)$ lies in $D(S_j) \subset E(S_j)$ for every $j \in J$. Then the R -covering family $(R_i \otimes_R S_j)_{(i,j) \in I \times J}$ also has the property that the image of a in $E(R_i \otimes_R S_j)$ lies in $D(R_i \otimes_R S_j)$ for $(i,j) \in I \times J$. Performing the above construction of $\phi(a)$ with the R -covering family $(R_i \otimes_R S_j)_{(i,j) \in I \times J}$

and considering the commutativity of

$$\begin{array}{ccc}
 & \prod_i R_i & \\
 & \downarrow & \\
 R & \xrightarrow{\quad} \prod_{i,j} R_i \otimes_R S_j & \\
 & \uparrow & \\
 & \prod_j S_j &
 \end{array}$$

we see that $\phi(a)$ is well-defined. To show that the definition of ϕ is functorial in R we can consider a morphism $R \rightarrow S$ of k - σ -algebras and the S -covering family $(R_i \otimes_R S)_{i \in I}$. The fact that $\phi: E \rightarrow F$ is the unique extension of $\phi: D \rightarrow F$ is immediate from the construction of ϕ .

The implication (ii) $\Rightarrow$ (iii) is obvious. Thus it only remains to show that (iii) $\Rightarrow$ (i). Let $(R_i)_{i \in I}$ be an R -covering family. Let D be the subfunctor of $\mathrm{Sp}^\sigma(R)$ equal to the union $\cup_{i \in I} \mathrm{Im}(\mathrm{Sp}^\sigma(R_i) \rightarrow \mathrm{Sp}^\sigma(R))$, i.e., a morphism of k - σ -algebras $R \rightarrow S$ lies in $D(S)$ if and only if it factors through $R \rightarrow R_i$ for some $i \in I$. Then D is a fat subfunctor of $\mathrm{Sp}^\sigma(R)$ by Lemma 5.1.6. We claim that the sequence

$$\mathrm{Hom}(D, F) \xrightarrow{\alpha} \prod_i \mathrm{Hom}(\mathrm{Sp}^\sigma(R_i), F) \xrightleftharpoons[\beta_2]{\beta_1} \prod_{i,j} \mathrm{Hom}(\mathrm{Sp}^\sigma(R_i \otimes_R R_j), F) \quad (5.2)$$

is exact. The injectivity of α is clear from the definition of D . Let $f = (f_i)_{i \in I} \in \prod_i \mathrm{Hom}(\mathrm{Sp}^\sigma(R_i), F)$ be such that $\beta_1(f) = \beta_2(f)$. Then for every pair $(i, j) \in I \times I$

$$\begin{array}{ccc}
 \mathrm{Sp}^\sigma(R_i) \times_{\mathrm{Sp}^\sigma(R)} \mathrm{Sp}^\sigma(R_j) & & \\
 \downarrow \simeq & & \\
 \mathrm{Sp}^\sigma(R_i \otimes_R R_j) & & \\
 \swarrow & & \searrow \\
 \mathrm{Sp}^\sigma(R_i) & & \mathrm{Sp}^\sigma(R_j) \\
 \searrow f_i & & \swarrow f_j \\
 & F(R) &
 \end{array} \quad (5.3)$$

commutes. Let us define a morphism $h: D \rightarrow F$ as follows: If S is a k - σ -algebra and $a \in D(S) \subset \mathrm{Sp}^\sigma(R)(S) = \mathrm{Hom}(R, S)$ then a factors as $a: R \rightarrow R_i \xrightarrow{b} S$ for some $i \in I$ and we can define $h(a) = f_i(b) \in F(S)$. It follows from the commutativity of (5.3) that $h(a)$ does not depend on the choice of i and b . Clearly, $\alpha(h) = f$. Therefore (5.2) is exact.

By assumption, every morphism $D \rightarrow F$ uniquely extends to $\mathrm{Sp}^\sigma(R) \rightarrow F$, i.e., $\mathrm{Hom}(\mathrm{Sp}^\sigma(R), F) \rightarrow \mathrm{Hom}(D, F)$ is bijective. Thus, applying the canonical bijections $\mathrm{Hom}(\mathrm{Sp}^\sigma(S), F) \simeq F(S)$ to (5.2), yields the exactness of (5.1). So F is a sheaf. $\square$

Theorem 5.1.8. *Let F be a functor from k - σ -Alg to Sets. Then there exists a sheaf $\tilde{F}$ and a morphism $\iota: F \rightarrow \tilde{F}$ that is universal among morphisms from F to sheaves, i.e., for*

every morphism ϕ from F to a sheaf E there exists a unique morphism $\tilde{\phi}: \tilde{F} \rightarrow E$ making

$$\begin{array}{ccc} F & \xrightarrow{\iota} & \tilde{F} \\ & \searrow \phi & \swarrow \tilde{\phi} \\ & E & \end{array}$$

commutative.

Proof. For any k - σ -algebra R we set $(\mathcal{L}F)(R) = \varinjlim \text{Hom}(D, F)$, where the limit is taken over all fat subfunctors D of $\text{Sp}^\sigma(R)$. An element of $(\mathcal{L}F)(R)$ is thus an equivalence class (D, α) , where D is a fat subfunctor of $\text{Sp}^\sigma(R)$ and $\alpha: D \rightarrow F$ a morphism of functors. We have $(D, \alpha) = (D', \alpha')$ if and only if there exists a fat subfunctor D'' of $\text{Sp}^\sigma(R)$ contained in D and D' such that the restrictions of α and α' to D'' are equal.

Let $\psi: R \rightarrow S$ be a morphism of k - σ -algebras. For every fat subfunctor D of $\text{Sp}^\sigma(R)$ the map $\text{Sp}^\sigma(\psi): \text{Sp}^\sigma(\psi)^{-1}(D) \rightarrow D$ induces a map $\text{Hom}(D, F) \rightarrow \text{Hom}(\text{Sp}^\sigma(\psi)^{-1}(D), F)$. By passing to the limit we obtain a map $\mathcal{L}(\psi): (\mathcal{L}F)(R) \rightarrow (\mathcal{L}F)(S)$. Thus $\mathcal{L}F$ is a functor from k - σ -Alg to Sets. We have a morphism of functors $\iota_F: F \rightarrow \mathcal{L}F$ determined by sending, for each k - σ -algebra R , an element of $F(R) \simeq \text{Hom}(\text{Sp}^\sigma(R), F)$ to its canonical image in $\varinjlim \text{Hom}(D, F)$.

Now set $\tilde{F} = \mathcal{L}(\mathcal{L}F)$ and $\iota = \iota_{\mathcal{L}F} \circ \iota_F$. With the notation of the theorem, we will next show the existence and uniqueness of $\tilde{\phi}$. Since $\iota = \iota_{\mathcal{L}F} \circ \iota_F$, it suffices to show that for every morphism ϕ from F to a sheaf E , there exists a unique morphism $\phi': \mathcal{L}F \rightarrow E$ making

$$\begin{array}{ccc} F & \xrightarrow{\iota_F} & \mathcal{L}F \\ & \searrow \phi & \swarrow \phi' \\ & E & \end{array} \quad (5.4)$$

commutative.

Let us first prove the uniqueness of ϕ' . Let R be a k - σ -algebra and let $\mu: \text{Sp}^\sigma(R) \rightarrow \mathcal{L}F$ correspond to $(D, \alpha) \in (\mathcal{L}F)(R)$ under the bijection $(\mathcal{L}F)(R) \simeq \text{Hom}(\text{Sp}^\sigma(R), \mathcal{L}F)$. It follows from the definitions that

$$\begin{array}{ccc} D & \hookrightarrow & \text{Sp}^\sigma(R) \\ \alpha \downarrow & & \downarrow \mu \\ F & \xrightarrow{\iota_F} & \mathcal{L}F \end{array} \quad (5.5)$$

commutes. Let $\eta: \text{Sp}^\sigma(R) \rightarrow E$ correspond to $\phi'((D, \alpha)) \in E(R)$ under the bijection $E(R) \simeq \text{Hom}(\text{Sp}^\sigma(R), E)$. Then $\eta = \phi'\mu$. Combining this with (5.5) and (5.4), we see that the restriction of η to D equals $\phi\alpha$. By Proposition 5.1.7, this shows that η is uniquely determined by (D, α) and ϕ . Therefore $\phi'((D, \alpha))$ is uniquely determined by ϕ .

Let us now establish the existence of ϕ' . Let R be a k - σ -algebra and $(D, \alpha) \in (\mathcal{L}F)(R)$. By Proposition 5.1.7, the composition $D \xrightarrow{\alpha} F \xrightarrow{\phi} E$ has a unique extension $\eta: \text{Sp}^\sigma(R) \rightarrow E$. Note that η only depends on the equivalence class (D, α) . Now define $\phi'((D, \alpha)) \in E(R)$ as the image of η under the canonical bijection $\text{Hom}(\text{Sp}^\sigma(R), E) \simeq E(R)$. This defines a morphism $\phi': \mathcal{L}F \rightarrow E$ such that $\phi = \phi'\iota_F$.

It remains to show that $\tilde{F}$ is a sheaf. But let us first show that

$$\iota_{\mathcal{L}F}: (\mathcal{L}F)(R) \rightarrow (\mathcal{L}(\mathcal{L}F))(R)$$

is injective for every k - σ -algebra R . So we have to show that if $\mu, \eta: \mathrm{Sp}^\sigma(R) \rightarrow \mathcal{L}F$ are two morphisms having the same restriction to a fat subfunctor $D \subset \mathrm{Sp}^\sigma(R)$, then $\mu = \eta$. Let $\hat{\mu}, \hat{\eta} \in (\mathcal{L}F)(R)$ correspond to μ and η under the bijection $(\mathcal{L}F)(R) \simeq \mathrm{Hom}(\mathrm{Sp}^\sigma(R), \mathcal{L}F)$. Replacing D by a smaller fat subfunctor of $\mathrm{Sp}^\sigma(R)$ if necessary, we can assume that $\hat{\mu} = (D, \mu')$ and $\hat{\eta} = (D, \eta')$. As in (5.5), we have $\iota_F \mu' = \mu|_D$ and $\iota_F \eta' = \eta|_D$. By Lemma 5.1.6, there exists an R -covering family $(R_i)_{i \in I}$ such that $\mathrm{Im}(\mathrm{Sp}^\sigma(R_i) \rightarrow \mathrm{Sp}^\sigma(R)) \subset D$ for all $i \in I$. For $i \in I$ let $\mu_i: \mathrm{Sp}^\sigma(R_i) \rightarrow D \xrightarrow{\mu'} F$ and $\eta_i: \mathrm{Sp}^\sigma(R_i) \rightarrow D \xrightarrow{\eta'} F$ be the induced morphisms. Then $\iota_F \mu_i = \iota_F \eta_i$. Considering the image of $\mathrm{id}_{R_i} \in \mathrm{Sp}^\sigma(R_i)(R_i)$ in $(\mathcal{L}F)(R_i)$ under $\iota_F \mu_i = \iota_F \eta_i$, shows that there exists a fat subfunctor D_i of $\mathrm{Sp}^\sigma(R_i)$ such that $\mu_i|_{D_i} = \eta_i|_{D_i}$. By Lemma 5.1.6, there exists for every $i \in I$ an R_i -covering family $(S_{ij})_{j \in J_i}$ such that $\mathrm{Im}(\mathrm{Sp}^\sigma(S_{ij}) \rightarrow \mathrm{Sp}^\sigma(R_i)) \subset D_i$ for all $j \in J_i$. The family $(S_{ij})_{i \in I, j \in J_i}$ is R -covering and therefore the union D' of all $\mathrm{Im}(\mathrm{Sp}^\sigma(S_{ij}) \rightarrow R)$ is a fat subfunctor of $\mathrm{Sp}^\sigma(R)$ by Lemma 5.1.6.

$$\begin{array}{ccccccc}
 \mathrm{Sp}^\sigma(S_{ij}) & \longrightarrow & D_i & \hookrightarrow & \mathrm{Sp}^\sigma(R_i) & \longrightarrow & D \hookrightarrow \mathrm{Sp}^\sigma(R) \\
 & & & & \searrow \eta_i & \downarrow \eta' & \downarrow \mu \\
 & & & & \mu_i & \downarrow \mu' & \downarrow \mu \\
 & & & & & F & \xrightarrow{\iota_F} \mathcal{L}F
 \end{array}$$

Since μ_i and η_i agree on D_i we see that μ' and η' agree on D' . Therefore $\hat{\mu} = \hat{\eta}$ and consequently $\mu = \eta$ as claimed.

To show that $\tilde{F}$ is a sheaf, it thus suffices to show that $\mathcal{L}F$ is a sheaf whenever $\iota_F: F(R) \rightarrow (\mathcal{L}F)(R)$ is injective for every k - σ -algebra R . Let us identify F with a subfunctor of $\mathcal{L}F$ via ι_F and let $(D, \alpha) \in (\mathcal{L}F)(R)$. Since D is fat in $\mathrm{Sp}^\sigma(R)$, by Lemma 5.1.6, there exists an R -covering family $(R_i)_{i \in I}$ such that $\mathrm{Im}(\mathrm{Sp}^\sigma(R_i) \rightarrow \mathrm{Sp}^\sigma(R)) \subset D$. Let $\phi_i: \mathrm{Sp}^\sigma(R_i) \rightarrow \mathrm{Sp}^\sigma(R)$ denote the canonical map. The commutativity of

$$\begin{array}{ccc}
 \phi_i^{-1}(D) & \hookrightarrow & \mathrm{Sp}^\sigma(R_i) \\
 \downarrow & \swarrow & \downarrow \phi_i \\
 D & \hookrightarrow & \mathrm{Sp}^\sigma(R) \\
 \downarrow \alpha & & \\
 F & &
 \end{array}$$

shows that $(\mathcal{L}F)(R) \rightarrow (\mathcal{L}F)(R_i)$ maps (D, α) into $F(R_i) \subset (\mathcal{L}F)(R_i)$. Thus F is fat in $\mathcal{L}F$.

To show that $\mathcal{L}F$ is a sheaf, it suffices to show (Proposition 5.1.7) that for every k - σ -algebra R , every morphism $\mu: D \rightarrow \mathcal{L}F$ from a fat subfunctor $D \subset \mathrm{Sp}^\sigma(R)$ to $\mathcal{L}F$ has a unique extension $\mu': \mathrm{Sp}^\sigma(R) \rightarrow \mathcal{L}F$. The uniqueness of μ' follows from the assumed injectivity of $\iota_F: F(R) \rightarrow (\mathcal{L}F)(R)$. So it remains to prove the existence of μ' . Since $F \subset \mathcal{L}F$ is fat, $\mu^{-1}(F) \subset D$ is fat. Since D is fat in $\mathrm{Sp}^\sigma(R)$ it follows that $\mu^{-1}(F)$ is fat in $\mathrm{Sp}^\sigma(R)$. Let $\mu': \mathrm{Sp}^\sigma(R) \rightarrow \mathcal{L}F$ correspond to the image of $\mu: \mu^{-1}(F) \rightarrow F$ in $(\mathcal{L}F)(R)$ under the bijection $(\mathcal{L}F)(R) \simeq \mathrm{Hom}(\mathrm{Sp}^\sigma(R), \mathcal{L}F)$. Then μ' is an extension of $\mu: \mu^{-1}(F) \rightarrow F \subset \mathcal{L}F$. It remains to show that μ' also extends $\mu: D \rightarrow \mathcal{L}F$. So we have to show that $\mu(a) = \mu'(a)$ for any k - σ -algebra S and $a \in D(S)$. Let $\hat{a}: \mathrm{Sp}^\sigma(S) \rightarrow D$ correspond to a under the bijection $D(S) \simeq \mathrm{Hom}(\mathrm{Sp}^\sigma(S), D)$. Since $\mu \hat{a}$ and $\mu' \hat{a}$ have the same restriction to $\hat{a}^{-1}(\mu^{-1}(F)) \subset \mathrm{Sp}^\sigma(S)$, it follows from the injectivity of $\iota_{\mathcal{L}F}: (\mathcal{L}F)(S) \rightarrow (\mathcal{L}(\mathcal{L}F))(S)$ that $\mu \hat{a} = \mu' \hat{a}$. As $\mu(a)$ and $\mu'(a) \in (\mathcal{L}F)(S)$ corresponds to $\mathrm{Sp}^\sigma(S) \xrightarrow{\hat{a}} D \xrightarrow{\mu} \mathcal{L}F$ and

$\mathrm{Sp}^\sigma(S) \xrightarrow{\hat{a}} D \xrightarrow{\mu'} \mathcal{L}F$ respectively under the bijection $(\mathcal{L}F)(S) \simeq \mathrm{Hom}(\mathrm{Sp}^\sigma(S), \mathcal{L}F)$ we find that $\mu(a) = \mu'(a)$ as desired. $\square$

The sheaf

$$\tilde{F}$$

from Theorem 5.1.8 is called the *sheaf associated with F* , or the *sheafification of F* . If $\phi: F \rightarrow E$ is a morphism of functors from $k\text{-}\sigma\text{-Alg}$ to **Sets**, then $F \xrightarrow{\phi} E \rightarrow \tilde{E}$ induces a morphism $\tilde{\phi}: \tilde{F} \rightarrow \tilde{E}$. So sheafification is a functor. Indeed, as

$$\mathrm{Hom}(\tilde{F}, E) \simeq \mathrm{Hom}(F, E),$$

we see that sheafification is left adjoint to the inclusion of functors into sheaves.

Corollary 5.1.9. *Let D be a fat subfunctor of a sheaf $F: k\text{-}\sigma\text{-Alg} \rightarrow \mathbf{Sets}$, then $\tilde{D} = F$.*

Proof. This is clear from Proposition 5.1.7. $\square$

Lemma 5.1.10. *Let $\phi: F \rightarrow E$ be a morphism of functors from $k\text{-}\sigma\text{-Alg}$ to **Sets** such that $\phi_R: F(R) \rightarrow E(R)$ is injective for any $k\text{-}\sigma\text{-algebra}$ R . Then $\tilde{\phi}_R: \tilde{F}(R) \rightarrow \tilde{E}(R)$ is injective for any $k\text{-}\sigma\text{-algebra}$ R .*

Proof. It suffices to show that $(\mathcal{L}F)(R) \rightarrow (\mathcal{L}E)(R)$ is injective for any $k\text{-}\sigma\text{-algebra}$ R . So let $\alpha_1: D_1 \rightarrow F$ and $\alpha_2: D_2 \rightarrow F$ be morphism with D_1, D_2 fat subfunctors of $\mathrm{Sp}^\sigma(R)$ such that $\alpha_1\phi$ and $\alpha_2\phi$ have the same image in $(\mathcal{L}E)(R) = \varinjlim \mathrm{Hom}(D, E)$. Then there exists a fat subfunctor D of $\mathrm{Sp}^\sigma(R)$ with $D \subset D_1 \cap D_2$ such that the restriction of $\alpha_1\phi$ and $\alpha_2\phi$ to D are equal. It follows from the injectivity of ϕ that α_1 and α_2 have the same restriction to D . $\square$

For simplicity, let us call a functor $G: k\text{-}\sigma\text{-Alg} \rightarrow \mathbf{Groups}$ a *group functor*. Equivalently, a group functor is a group object in the category of functors from $k\text{-}\sigma\text{-Alg}$ to **Sets**. If G is a group functor, then the associated sheaf $\tilde{G}$ is naturally a group functor such that the associated morphism of functors $\iota: G \rightarrow \tilde{G}$ is a morphism of group functors, i.e., is compatible with the group structure. Indeed, if G is a group functor, then $\mathrm{Hom}(D, G)$ has naturally the structure of a group for any functor $D: k\text{-}\sigma\text{-Alg} \rightarrow \mathbf{Sets}$. If R is a $k\text{-}\sigma\text{-algebra}$ and $D_1 \subset D_2$ are fat subfunctors of $\mathrm{Sp}^\sigma(R)$ then $\mathrm{Hom}(D_2, G) \rightarrow \mathrm{Hom}(D_1, G)$ is a morphism of groups and we have an induced group structure on the limit $(\mathcal{L}G)(R) = \varinjlim \mathrm{Hom}(D, G)$. This group structure is functorial in R and $\iota_G: G \rightarrow \mathcal{L}G$ is a morphism of group functors. Applying this construction twice, yields the required group structure on $\tilde{G} = \mathcal{L}(\mathcal{L}G)$. Alternatively, the group structure on $\tilde{G}$, can be obtained by applying $(\)$ to the multiplication $G \times G \rightarrow G$ and using the canonical isomorphism $\widetilde{G \times G} \simeq \tilde{G} \times \tilde{G}$.

If G is a group functor and N a normal subgroup functor, i.e., $N(R)$ is a normal subgroup of $G(R)$ for any $k\text{-}\sigma\text{-algebra}$ R , we can define a group functor

$$G//N$$

by $R \rightsquigarrow G(R)/N(R)$. The crux with this functor is that it may not be a sheaf (or $\sigma\text{-variety}$) if G and N are sheaves (or $\sigma\text{-varieties}$). We therefore need to sheafify $G//N$. Sheafification is compatible with quotients in the following sense:

Lemma 5.1.11. *Let G be a group functor and N a normal subgroup functor. Then $\widetilde{N}$ is a normal subgroup functor of $\widetilde{G}$ and*

$$\widetilde{\widetilde{G//N}} \simeq \widetilde{G//N}.$$

Proof. By Lemma 5.1.10 the map $\widetilde{N}(R) \rightarrow \widetilde{G}(R)$ is injective for any k - σ -algebra R . Since N is normal in G , $\text{Hom}(D, N)$ is normal in $\text{Hom}(D, G)$ for every fat subfunctor D of $\text{Sp}^\sigma(R)$. It follows that $(\mathcal{L}N)(R)$ is normal in $(\mathcal{L}G)(R)$ and therefore $\widetilde{N}$ is normal in $\widetilde{G}$.

The morphism $N \rightarrow G \rightarrow G//N$ factors through the sheaf E that maps every k - σ -algebra to a set with one element. Hence $\widetilde{N} \rightarrow \widetilde{G} \rightarrow \widetilde{G//N}$ factors through E . So $\widetilde{N}$ maps into the kernel of $\widetilde{G} \rightarrow \widetilde{G//N}$ and we obtain a morphism $\mu: \widetilde{G//N} \rightarrow \widetilde{G//N}$. Since N lies in the kernel of $G \rightarrow \widetilde{G} \rightarrow \widetilde{G//N}$ we obtain a morphism $\eta: G//N \rightarrow \widetilde{G//N}$.

All the subdiagrams of

$$\begin{array}{ccc} & G & \xrightarrow{\pi_G} G//N \\ & \downarrow i_G & \downarrow i_{G//N} \\ & \widetilde{G} & \xrightarrow{\pi_{\widetilde{G}}} \widetilde{G//N} \\ & \downarrow \pi_{\widetilde{G}} & \downarrow \mu \\ \widetilde{G//N} & \xrightarrow{i_{\widetilde{G//N}}} & \widetilde{G//N} \end{array}$$

η (curved arrow from G to $\widetilde{G//N}$)
 α (dashed arrow from $\widetilde{G//N}$ to $\widetilde{G//N}$)
 β (dashed arrow from $\widetilde{G//N}$ to $\widetilde{G//N}$)

consisting only of solid arrows commute. By the universal property of $i_{\widetilde{G//N}}$ there exists a morphism $\alpha: \widetilde{G//N} \rightarrow \widetilde{G//N}$ such that $\alpha i_{\widetilde{G//N}} = \mu$. By the universal property of $i_{G//N}$ there exists a morphism $\beta: \widetilde{G//N} \rightarrow \widetilde{G//N}$ such that $\beta i_{G//N} = i_{\widetilde{G//N}} \eta$. We will show that α and β are inverse to each other. We have

$$\beta \pi_{\widetilde{G}} i_G = \beta i_{G//N} \pi_G = i_{\widetilde{G//N}} \eta \pi_G = i_{\widetilde{G//N}} \pi_{\widetilde{G}} i_G.$$

Therefore $\beta \pi_{\widetilde{G}} = i_{\widetilde{G//N}} \pi_{\widetilde{G}}$. Since, for any k - σ -algebra R and element from $(\widetilde{G//N})(R)$ lifts to an element of $\widetilde{G}(R)$, this implies that $\beta \mu = i_{\widetilde{G//N}}$. From $\alpha i_{\widetilde{G//N}} = \mu$ and $\beta \mu = i_{\widetilde{G//N}}$ we deduce that $\beta \alpha i_{\widetilde{G//N}} = i_{\widetilde{G//N}}$. Thus $\beta \alpha$ is the identity on $\widetilde{G//N}$.

We have $\alpha i_{\widetilde{G//N}} \eta = \mu \eta = i_{G//N}$. Together with $i_{\widetilde{G//N}} \eta = \beta i_{G//N}$, this implies $\alpha \beta i_{G//N} = i_{G//N}$. Therefore $\alpha \beta$ is the identity on $\widetilde{G//N}$. □

Theorem 5.1.12. *Let G be a σ -algebraic group and $N \trianglelefteq G$ a σ -closed subgroup. Then $G//N$ is a fat subfunctor of G/N . In particular,*

$$\widetilde{G//N} = G/N.$$

Proof. By Theorem 3.2.3 the kernel of $G \rightarrow G/N$ equals N , i.e., for every k - σ -algebra R the kernel of $G(R) \rightarrow (G/N)(R)$ is $N(R)$. Thus the canonical map $G(R)/N(R) \rightarrow (G/N)(R)$ is injective. Therefore we can identify $G//N$ with a subfunctor of G/N . It follows from Lemma 3.2.8 that $G//N$ is fat in G/N . □

5.2 The isomorphism theorems

In this section we prove the isomorphism theorems for σ -algebraic groups.

The following theorem is the analog of the first isomorphism theorem for groups.

Theorem 5.2.1. *Let $\phi: G \rightarrow H$ be a morphism of σ -algebraic groups. Then $\phi(G)$ is a σ -closed subgroup of H and the induced morphism $G/\ker(\phi) \rightarrow \phi(G)$ is an isomorphism.*

Proof. We already observed in Lemma 3.3.5 that $\phi(G)$ is a σ -closed subgroup. Since $\ker(\phi)$ is the kernel of $G \rightarrow \phi(G)$, the induced morphism $G/\ker(\phi) \rightarrow \phi(G)$ is a σ -closed embedding by Corollary 3.2.4 and so we can identify $G/\ker(\phi)$ with a σ -closed σ -subvariety of $\phi(G)$. Since ϕ factors through $G/\ker(\phi)$ it follows from the definition of $\phi(G)$ that $G/\ker(\phi) = \phi(G)$. $\square$

Corollary 5.2.2. *Let $\phi: G \rightarrow H$ be a morphism of σ -algebraic groups. Then*

$$\phi(G) = \widetilde{\text{Im}(\phi)}.$$

Proof. The isomorphism $G/\ker(\phi) \simeq \phi(G)$ identifies $G/\ker(\phi)$ with $\text{Im}(\phi)$. Therefore the claim follows from Theorem 5.1.12. $\square$

Let N and H be σ -closed subgroups of a σ -algebraic group G such that H normalizes N , i.e., $H(R)$ normalizes $N(R)$ for any k - σ -algebra R . Then we can form the semidirect product $N \rtimes H$: This is a σ -algebraic group with underlying σ -variety $N \times H$ and multiplication given by $((n_1, h_1), (n_2, h_2)) \mapsto (n_1 h_1 n_2 h_1^{-1}, h_1 h_2)$ for any k - σ -algebra R and $n_1, n_2 \in N(R)$, $h_1, h_2 \in H(R)$. Cf. the end of Section 3.3. The map

$$m: N \rtimes H \rightarrow G, (n, h) \mapsto nh$$

for any k - σ -algebra R and $n \in N(R)$, $h \in H(R)$ is a morphism of σ -algebraic groups. We define

$$HN := NH := m(N \rtimes H).$$

By construction HN is a σ -closed subgroup of G (Lemma 3.3.5). In fact, HN is the smallest σ -closed subgroup of G which contains N and H . It follows from Corollary 5.2.2 that HN is the sheaf associated to the functor $R \mapsto N(R)H(R)$. Moreover, by Lemma 3.3.14 we have

$$(NH)(R) = \{g \in G(R) \mid \exists \text{ faithfully flat } R\text{-}\sigma\text{-algebra } S \text{ such that } g \in N(S)H(S)\}$$

for any k - σ -algebra R . It follows from Lemma 3.3.15 that $N = m(N)$ is normal in HN .

The following theorem is the analog of the second isomorphism theorem for groups.

Theorem 5.2.3. *Let H and N be σ -closed subgroups of a σ -algebraic group G such that H normalizes N . Then the canonical morphism*

$$H/(H \cap N) \rightarrow HN/N$$

is an isomorphism.

Proof. For every k - σ -algebra R we have an isomorphism

$$H(R)/(H(R) \cap N(R)) \rightarrow H(R)N(R)/N(R)$$

which is functorial in R . Passing to the associated sheaves and using Lemma 5.1.11 we find the required isomorphism. $\square$

The following theorem is the analog of the third isomorphism theorem for groups.

Theorem 5.2.4. *Let G be a σ -algebraic group, $N \trianglelefteq G$ a normal σ -closed subgroup and $\pi: G \rightarrow G/N$ the quotient. 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 H' of G/N . The inverse map 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 which case the canonical morphism*

$$G/H \rightarrow (G/N)/(H/N)$$

is an isomorphism.

Proof. By Theorem 5.2.1 and Theorem 3.2.3 we have $\pi(H) = H/N$. Let us show that $\pi^{-1}(\pi(H)) = H$ for every σ -closed subgroup H of G containing N . Let R be a k - σ -algebra and $g \in \pi^{-1}(\pi(H))(R)$, i.e., $\pi(g) \in \pi(H)(R)$. By Lemma 3.3.14 there exists a faithfully flat R - σ -algebra S and $h \in H(S)$ with $\pi(h) = \pi(g) \in (G/N)(S)$. As $\ker(\pi) = N$ by Theorem 3.2.3, this implies that $gh^{-1} \in N(S) \leq H(S)$. Therefore $g \in H(S)$ and $g \in H(S) \cap G(R) = H(R)$ by Lemma 3.3.13. Thus $\pi^{-1}(\pi(H)) \subset H$. The reverse inclusion is obvious.

Let us next show that $\pi(\pi^{-1}(H')) = H'$ for a σ -closed subgroup H' of G/N . As π maps $\pi^{-1}(H')$ into H' , it is clear from the definition of $\pi(\pi^{-1}(H'))$ (Lemma 1.2.6) that $\pi(\pi^{-1}(H')) \subset H'$.

Let R be a k - σ -algebra and $h' \in H'(R)$. There exists a faithfully flat R - σ -algebra S and $g \in G(S)$ such that $\pi(g) = h'$. So $g \in \pi^{-1}(H')(S)$ and $h' = \pi(g) \in \pi(\pi^{-1}(H')(S)) \subset \pi(\pi^{-1}(H'))(S)$. Thus $h' \in \pi(\pi^{-1}(H'))(S) \cap H'(R) = \pi(\pi^{-1}(H'))(R)$. Hence $\pi(\pi^{-1}(H')) = H'$.

If H is normal in G , then $\pi(H)$ is normal in G/N by Lemma 3.3.15. Clearly $\pi^{-1}(H')$ is normal if H' is normal.

For every k - σ -algebra R we have an isomorphism

$$G(R)/H(R) \rightarrow (G(R)/N(R))/(H(R)/N(R)).$$

Passing to the associated sheaves and using Lemma 5.1.11 we obtain the required isomorphism. $\square$

5.3 Jordan-Hölder theorem

In this section we apply the results from the previous sections to prove a Jordan-Hölder type theorem for σ -algebraic groups. A Jordan-Hölder type theorem for algebraic groups can be found in [Ros56], while a Jordan-Hölder type theorem for differential algebraic groups has been proved in [CS11]. As we will show, the Schreier refinement theorem also holds for σ -algebraic groups (Theorem 5.3.5). So any two decomposition series of a σ -algebraic group have equivalent refinements. However, a σ -algebraic group rarely has a decomposition series. It is therefore useful to consider more general subnormal series. The basic idea is to consider σ -algebraic groups up to quotients by zero σ -dimensional normal subgroups. Formally this is realized by replacing in the uniqueness statement of the classical Jordan-Hölder theorem the notion of isomorphism by the notion of isogeny.

Our first aim is to prove the analog of the Schreier refinement theorem. We follow along the lines of the well-known proof via the Butterfly lemma. (Cf. [Lan02, Section 1.3] and [Mil12, Chapter IX, Section 6].) We will need two analogs of elementary statements about groups.

Lemma 5.3.1. *Let N , G and H be σ -closed subgroups of a σ -algebraic group G' such that $N \trianglelefteq G$ and N normalizes H . Then $G \cap NH = N(G \cap H)$.*

Proof. As $N \leq G \cap NH$ and $G \cap H \leq G \cap NH$ it is clear that $N(G \cap H) \subset G \cap NH$.

Conversely, let R be a k - σ -algebra and $g \in (G \cap NH)(R)$. There exists a faithfully flat R - σ -algebra S and $n \in N(S)$, $h \in H(S)$ such that $g = nh$ in $G'(S)$. But then $h = n^{-1}g \in G(S)$ and therefore $g = nh \in N(S)(G(S) \cap H(S)) \subset (N(G \cap H))(S)$. It follows from Lemma 3.3.13 that $g \in (N(G \cap H))(R)$. $\square$

Lemma 5.3.2. *Let $H_1 \trianglelefteq H_2$ be σ -closed subgroups of a σ -algebraic group G . Assume that H_2 normalizes $N \leq G$. Then $NH_1 \trianglelefteq NH_2$.*

Proof. Clearly $N \rtimes H_1$ is a normal σ -closed subgroup of $N \rtimes H_2$. Therefore $NH_1 = m(N \rtimes H_1)$ is a normal σ -closed subgroup of $NH_2 = m(N \rtimes H_2)$ by Lemma 3.3.15. $\square$

The following lemma is the analog of the Butterfly (or Zassenhaus) lemma.

Lemma 5.3.3. *Let $N_1 \trianglelefteq H_1$ and $N_2 \trianglelefteq H_2$ be σ -closed subgroups of a σ -algebraic group G . Then $N_1(H_1 \cap H_2) \trianglelefteq N_1(H_1 \cap H_2)$, $N_2(N_1 \cap H_2) \trianglelefteq N_2(H_1 \cap H_2)$ and*

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

Proof. Since $H_1 \cap N_2$ is normal in $H_1 \cap H_2$ it follows from Lemma 5.3.2 that $N_1(H_1 \cap N_2)$ is normal in $N_1(H_1 \cap H_2)$. Similarly, $N_2(N_1 \cap H_2) \trianglelefteq N_2(H_1 \cap H_2)$. As $H_1 \cap H_2$ normalizes $N_1(H_1 \cap N_2)$ it follows from Theorem 5.2.3 that

$$\frac{H_1 \cap H_2}{(H_1 \cap H_2) \cap N_1(H_1 \cap N_2)} \simeq \frac{(H_1 \cap H_2)N_1(H_1 \cap N_2)}{N_1(H_1 \cap N_2)}. \quad (5.6)$$

Lemma 5.3.1 with $N = H_1 \cap N_2$, $G = H_1 \cap H_2$ and $H = N_1$ shows that

$$(H_1 \cap H_2) \cap N_1(H_1 \cap N_2) = (H_1 \cap N_2)(H_1 \cap H_2 \cap N_1) = (H_1 \cap N_2)(N_1 \cap H_2).$$

Because $H_1 \cap N_2 \subset H_1 \cap H_2$ we find $(H_1 \cap H_2)N_1(H_1 \cap N_2) = N_1(H_1 \cap H_2)$. Therefore (5.6) becomes

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

By symmetry

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

$\square$

Definition 5.3.4. *Let G be a σ -algebraic group. A subnormal series of G is a sequence*

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_n = 1 \quad (5.7)$$

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

$$G = H_0 \supsetneq H_1 \supsetneq \cdots \supsetneq H_m = 1 \quad (5.8)$$

of G is called a refinement of (5.7) if $\{G_0, \dots, G_n\} \subset \{H_1, \dots, H_m\}$. We say that (5.7) and (5.8) are equivalent if $n = m$ and there exists a permutation π such that the quotient groups G_i/G_{i+1} and $H_{\pi(i)}/H_{\pi(i)+1}$ are isomorphic for $i = 0, \dots, n-1$. A subnormal series is called a decomposition series if no quotient group has a proper non-trivial normal σ -closed subgroup.

The following theorem is the analog of the Schreier refinement theorem.

Theorem 5.3.5. *Any two subnormal series of a σ -algebraic group have equivalent refinements.*

Proof. Let

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$$

and

$$G = H_0 \supset H_1 \supset \cdots \supset H_m = 1$$

be subnormal series of a σ -algebraic group G . Set $G_{i,j} = G_{i+1}(H_j \cap G_i)$ for $i = 0, \dots, n-1$ and $j = 0, \dots, m$. Then

$$G = G_0 = G_{0,0} \supset G_{0,1} \supset G_{0,2} \supset \cdots \supset G_{0,m} = G_1 = G_{1,0} \supset G_{1,1} \supset \cdots \supset G_{n-1,m} = 1$$

is a subnormal series for G . Similarly, setting $H_{j,i} = H_{j+1}(G_i \cap H_j)$ for $j = 0, \dots, m-1$ and $i = 0, \dots, n$, defines a subnormal series for G . By Lemma 5.3.3

$$G_{i,j}/G_{i,j+1} \simeq H_{j,i}/H_{j,i+1}.$$

□

Corollary 5.3.6. *Any two decomposition series of a σ -algebraic group are equivalent.*

Proof. By Theorem 5.3.5 there exist equivalent refinements. But a refinement of a decomposition series is necessarily trivial. □

The above corollary is not that useful as it may seem at first sight, because a σ -algebraic group need not possess a decomposition series. Let us illustrate this with an example.

Example 5.3.7. Let k be a σ -field of characteristic zero. The σ -algebraic group $G = \mathbb{G}_a$ does not have a decomposition series. Indeed, by [DVHW, Corollary A.3], every proper σ -closed subgroup G of $\mathbb{G}_a$ is of the form $G(R) = \{g \in R \mid f(g) = 0\}$ for some non-zero homogeneous linear difference equation $f = \sigma^n(y) + \lambda_{n-1}\sigma^{n-1}(y) + \cdots + \lambda_0 y$. If h is another non-trivial linear homogeneous difference equation, then the product $h * f$ in the sense of linear difference operators (see [Lev08, Section 3.1]) defines a σ -closed subgroup H of $\mathbb{G}_a$ with $G \subsetneq H \subsetneq \mathbb{G}_a$. For example, for $h = \sigma(y)$ we have

$$H(R) = \{g \in R \mid \sigma^{n+1}(g) + \sigma(\lambda_{n-1})\sigma^n(y) + \cdots + \sigma(\lambda_0)\sigma(g) = 0\}.$$

To remedy this shortcoming we need to relax the condition that the quotient groups of a decomposition series are simple.

Definition 5.3.8. *A σ -algebraic group G with $\sigma\text{-dim}(G) > 0$ is called almost-simple if every normal proper σ -closed subgroup of G has σ -dimension zero.*

In the differential world, the almost-simple differential algebraic groups are fairly well understood. See [CS11], [Min], [Fre]. We hope to elucidate the structure of almost-simple σ -algebraic groups in the future. Considerable understanding of the Zariski dense σ -algebraic subgroups of almost-simple algebraic groups has already been obtained in [CHP02, Proposition 7.10]. See also [DVHW, Section A4].

Example 5.3.9. The σ -algebraic group $G = \mathbb{G}_a$ is almost-simple. (Cf. Example 5.3.7).

Lemma 5.3.10. *Let G be a σ -algebraic group with $\sigma\text{-dim}(G) > 0$. Among the σ -closed subgroups H of G with $\sigma\text{-dim}(H) = \sigma\text{-dim}(G)$ there exists a unique smallest one.*

Proof. Let H_1 and H_2 be σ -closed subgroups of G with $\sigma\text{-dim}(H_1) = \sigma\text{-dim}(H_2) = \sigma\text{-dim}(G)$. By Theorem 2.3.6 we have $\sigma\text{-dim}(H_1 \cap H_2) = \sigma\text{-dim}(G)$. Thus the claim follows from Corollary 2.3.3. $\square$

Definition 5.3.11. *Let G be a σ -algebraic group with $\sigma\text{-dim}(G) > 0$. The smallest σ -closed subgroup of G with σ -dimension equal to the σ -dimension of G is called the strong identity component of G . It is denoted by*

$$G^{so}.$$

A σ -algebraic group of positive σ -dimension is called strongly connected if it is equal to its strong identity component.

Thus a σ -algebraic group G is strongly connected if and only if it has no proper σ -closed subgroup with σ -dimension equal to the σ -dimension of G . It is clear from Lemma 4.1.21 that a strongly connected σ -algebraic group is connected. The strong identity component of a σ -algebraic group is strongly connected.

Example 5.3.12. If $\mathcal{G}$ is a smooth connected algebraic group with $\dim(\mathcal{G}) > 0$, then $G = [\sigma]_k \mathcal{G}$ is strongly connected. Indeed, as $\mathcal{G}$ is smooth and connected $k[\mathcal{G}[i]]$ is an integral domain for every $i \geq 0$. So if H is a proper σ -closed subgroup of G , then $\dim(H[i]) < \dim(G[i])$ for $i \gg 0$. But $\dim(G[i]) = \dim(\mathcal{G})(i+1)$ and so it follows from Theorem 2.2.7 that $\sigma\text{-dim}(H) < \sigma\text{-dim}(G)$.

The following example shows that a σ -integral σ -algebraic group need not be strongly connected.

Example 5.3.13. Let G be the σ -closed subgroup of $\mathbb{G}_a^2$ given by

$$G(R) = \{(g_1, g_2) \in R^2 \mid \sigma(g_1) = g_1\} \leq \mathbb{G}_a^2(R)$$

for any k - σ -algebra R . As $k\{G\} = k[y_1]\{y_2\}$ with $\sigma(y_1) = y_1$ we see that G is σ -integral. We have $\sigma\text{-dim}(G) = 1$ (for example by Proposition 2.2.17). The σ -closed subgroup H of G given by $H(R) = \{(0, g) \in R^2\}$ is isomorphic to $\mathbb{G}_a$ and therefore also has σ -dimension one. It is clear from Example 5.3.12 that $G^{so} = H$.

It is clear that G^{so} is a characteristic subgroup of G in the weak sense that every automorphism τ of G induces an automorphism of G^{so} . However, the following example illustrates the somewhat disturbing fact that G^{so} need not be normal in G . In particular, G^{so} need not be a characteristic subgroup of G (in the sense of Definition 2.1.5).

Example 5.3.14. Let $G = N \rtimes H$ be the σ -algebraic group from Example 2.5.11. Then $\sigma\text{-dim}(G) = 1$. The σ -closed subgroup $H = \mathbb{G}_m$ of G has σ -dimension one. Since H is strongly connected (Example 5.3.12) we see that $H = G^{so}$. We already noted in Example 2.5.11 that H is not normal in G .

Lemma 5.3.15. *Assume that k is perfect and inversive. Then a strongly connected σ -algebraic group is σ -integral.*

Proof. Let G be a strongly connected σ -algebraic group. Then G is connected and because $\sigma\text{-dim}(G) = \sigma\text{-dim}(G_{\text{red}})$ by Lemma 4.1.22, we must have $G = G_{\text{red}}$. So G is reduced and hence integral by Proposition 4.1.15. Similarly, $G = G_{\sigma\text{-red}}$ by Lemma 4.1.22. Thus G is σ -integral. $\square$

The following example shows that Lemma 5.3.15 fails over an arbitrary base σ -field. There exists a strongly connected σ -algebraic group which is not σ -reduced.

Example 5.3.16. Let k be a non-inversive σ -field of characteristic zero. So there exists $\lambda \in k$ with $\lambda \notin \sigma(k)$. Let G be the σ -closed subgroup of $\mathbb{G}_a^2$ given by

$$G(R) = \{(g_1, g_2) \in R^2 \mid \sigma(g_1) = \lambda \sigma(g_2)\}$$

for any k - σ -algebra R . Then $k\{G\} = k[y_1, y_2, \sigma(y_2), \dots]$ with $\sigma(y_1) = \lambda \sigma(y_2)$. For $i \geq 0$ let $G[i]$ denote the i -th order Zariski closure of G in $\mathbb{G}_a^2$. Then $k[G[i]] = k[y_1, y_2, \dots, \sigma^i(y_2)]$ and therefore $\dim(G[i]) = 1 \cdot (i + 1) + 1$, in particular $\sigma\text{-dim}(G) = 1$.

We claim that G is strongly connected. Suppose that $H \leq G$ is a proper σ -closed subgroup with $\sigma\text{-dim}(H) = \sigma\text{-dim}(G)$. Let a_1 and a_2 denote the image of y_1 and y_2 in $k\{H\}$ respectively. By [DVHW, Corollary A.3] the σ -ideal $\mathbb{I}(H) \subset k\{\mathbb{G}_a^2\}$ is σ -generated by homogenous linear σ -polynomials. Thus there exists a non-trivial k -linear relation between $a_1, a_2, \sigma(a_2), \dots$. If that relation would properly involve $\sigma^i(a_2)$ for $i \geq 1$, then $\sigma\text{-dim}(H) = 0$. Thus there exists a non-trivial k -linear relation between a_1 and a_2 . We have $a_1 \neq 0$ and $a_2 \neq 0$ because otherwise $\sigma\text{-dim}(H) = 0$. So there exists $\mu \in k$ with $a_1 - \mu a_2 = 0$. Consequently

$$0 = \sigma(a_1) - \sigma(\mu)\sigma(a_2) = \lambda\sigma(a_2) - \sigma(\mu)\sigma(a_2) = (\lambda - \sigma(\mu))\sigma(a_2).$$

Since $\lambda \notin \sigma(k)$ this implies $\sigma(a_2) = 0$. But then $\sigma\text{-dim}(H) = 0$; a contradiction.

Now assume that $\lambda^2 \in \sigma(k)$. (For example, we can choose $k = \mathbb{C}(\sqrt{x}, \sqrt{x+1}, \dots)$ with action of σ determined by $\sigma(x) = x + 1$ and $\lambda = \sqrt{x}$.) If $\mu \in k$ with $\sigma(\mu) = \lambda^2$ then $\sigma(y_1^2 - \mu y_2^2) = 0$. Thus G is not σ -reduced.

We have seen in Example 5.3.14 that the strong identity component need not be normal. Our next goal is to reconcile this difficulty:

Proposition 5.3.17. *Assume that k is algebraically closed and inversive. Let G be a strongly connected σ -algebraic group and H a normal σ -closed subgroup of G with $\sigma\text{-dim}(H) > 0$. Then H^{so} is normal in G . (In particular, H^{so} is normal in H .)*

For the proof of Proposition 5.3.17 we need several preparatory results.

Lemma 5.3.18. *Assume that k is algebraically closed and inversive. Let K be a σ -field extension of k . Then there exists a σ -field extension L of K such that only the elements of k are fixed by all σ -field automorphisms of $L|k$, i.e., $L^{\text{Aut}(L|k)} = k$.*

Proof. Let us start with proving the following claim: There exists a σ -field extension L of K such that for all $a \in K \setminus k$ there exists a σ -field automorphism τ of $L|k$ with $\tau(a) \neq a$ and such that every σ -field automorphism of $K|k$ extends to a σ -field automorphism of $L|k$.

Since k is algebraically closed $K \otimes_k K$ is an integral domain. Since k is inversive $K \otimes_k K$ is σ -reduced (Lemma 2.5.5 (ii)). Therefore the quotient field L of $K \otimes_k K$ is naturally a σ -field. Consider L as a σ -field extension of K via the embedding $a \mapsto a \otimes 1$.

The σ -field automorphism τ of $L|k$ determined by $\tau(a \otimes b) = b \otimes a$ moves every element of $K \setminus k$. Moreover, every σ -field automorphism τ' of $K|k$ extends to $L|k$, for example by $\tau'(a \otimes b) = \tau'(a) \otimes b$.

Now let us prove the lemma. By the above claim, there exists a σ -field extension $L_1|K$ such that every element of $K \setminus k$ can be moved by a σ -field automorphism of $L_1|K$ and every σ -field automorphism of $K|k$ extends to a σ -field automorphism of $L_1|k$. Now apply the claim again to $L_1|k$ to find a σ -field extension $L_2|L_1$ such that every element of $L_1 \setminus k$ can be moved by a σ -field automorphism of $L_2|k$ and every σ -field automorphism of $L_1|k$ extends to a σ -field automorphism of $L_2|k$. Continuing like this we obtain a chain of σ -field extensions $k \subset K \subset L_1 \subset L_2 \subset \dots$. The union $L = \cup L_i$ has the required property. $\square$

We need to know if the strong identity component is compatible with base extension.

Lemma 5.3.19. *Assume that k is algebraically closed and inversive. Let G be a σ -algebraic group with $\sigma\text{-dim}(G) > 0$ and K a σ -field extension of k . Then*

$$(G_K)^{so} = (G^{so})_K.$$

Proof. As the σ -dimension is invariant under base extension (Lemma 2.2.19),

$$\sigma\text{-dim}((G^{so})_K) = \sigma\text{-dim}(G^{so}) = \sigma\text{-dim}(G) = \sigma\text{-dim}(G_K).$$

Therefore $(G_K)^{so} \leq (G^{so})_K$.

Let us now show that $(G_K)^{so}$ descends to k , i.e., there exists a σ -closed subgroup H of G with $(G_K)^{so} = H_K$. By Lemma 5.3.18 there exists a σ -field extension L of K such that $L^{\text{Aut}(L|k)} = k$, where $\text{Aut}(L|k)$ is the group of all σ -field automorphisms of $L|k$. The group $\text{Aut}(L|k)$ acts on $L\{G_L\} = k\{G\} \otimes_k L$ by k - σ -algebra automorphisms via the right factor. Let H' be a σ -closed subgroup of G_L . Since the Hopf algebra structure maps commute with the $\text{Aut}(L|k)$ -action, $\tau(\mathbb{I}(H'))$ is a σ -Hopf ideal of $k\{G\} \otimes_k L$ for every $\tau \in \text{Aut}(L|k)$. Moreover, the σ -dimension of the σ -closed subgroup of G_L defined by $\tau(\mathbb{I}(H'))$ is equal to the σ -dimension of H' (cf. Lemma 2.2.19). Since $\mathbb{I}((G_L)^{so})$ is the unique maximal σ -Hopf ideal of $k\{G\} \otimes_k L$ such that $\sigma\text{-dim}((G_L)^{so}) = \sigma\text{-dim}(G_L)$, we see that $\tau(\mathbb{I}((G_L)^{so})) = \mathbb{I}((G_L)^{so})$ for every $\tau \in \text{Aut}(L|k)$. Let

$$\mathfrak{a} = \{f \in \mathbb{I}((G_L)^{so}) \mid \tau(f) = f \ \forall \ \tau \in \text{Aut}(L|k)\} = \mathbb{I}((G_L)^{so}) \cap k\{G\}.$$

Since the action of $\text{Aut}(L|k)$ commutes with the Hopf algebra structure maps, $\mathfrak{a}$ is σ -Hopf ideal of $k\{G\}$ and therefore corresponds to a σ -closed subgroup H of $k\{G\}$. We have $\mathfrak{a} \otimes_k L = \mathbb{I}((G_L)^{so})$. (See [Bou90, Corollary to Proposition 6, Chapter V, §10.4, A.V.63].) So $H_L = (G_L)^{so}$. As $\sigma\text{-dim}(H) = \sigma\text{-dim}((G_L)^{so}) = \sigma\text{-dim}(G_L) = \sigma\text{-dim}(G)$ we see that $G^{so} \leq H$, therefore $(G^{so})_L \leq H_L = (G_L)^{so}$. Hence also

$$((G^{so})_K)_L = (G^{so})_L \leq (G_L)^{so} \leq ((G_K)^{so})_L.$$

Thus $(G^{so})_K \leq (G_K)^{so}$. $\square$

The following example shows that the formation of the strongly connected component is in general not compatible with base extension.

Example 5.3.20. Let G be the strongly connected σ -algebraic group from Example 5.3.16. Let $K = k^*$ be the inversive closure of k (see ([Lev08, Definition 2.1.6])) and

let $\mu \in K$ with $\sigma(\mu) = \lambda$. Then G_K is not strongly connected since it has the σ -closed subgroup H of $\sigma\text{-dim}(H) = 1 = \sigma\text{-dim}(G)$ given by

$$H(R) = \{(g_1, g_2) \in R^2 \mid g_1 = \mu g_2\}$$

for any k - σ -algebra R . So $(G_K)^{so}$ is properly contained in $(G^{so})_K = G_K$.

Now we are prepared to prove Proposition 5.3.17.

Proof of Proposition 5.3.17. We have to show that the morphism of σ -varieties

$$\phi: G \times H^{so} \rightarrow G, (g, h) \mapsto ghg^{-1}$$

maps into H^{so} . We know from Lemma 5.3.15 that H^{so} and G are σ -integral. A fortiori H^{so} and G are perfectly σ -reduced. Because of Lemma 2.5.5 (iv) also the product $G \times H^{so}$ is perfectly σ -reduced. So by Lemma 2.5.4, it suffices to show that $\phi_K((G \times H^{so})(K)) \subset H^{so}(K)$ for every σ -field extension K of k . Let $g \in G(K)$. Then g induces an automorphism of G_K by conjugation. Since H is normal in G we have an induced automorphism on H_K . This automorphism maps $(H_K)^{so}$ into $(H_K)^{so}$. But $(H_K)^{so} = (H^{so})_K$ by Lemma 5.3.19. This shows that conjugation by g maps $H^{so}(K)$ into $H^{so}(K)$. Thus $\phi_K((G \times H^{so})(K)) \subset H^{so}(K)$ as required. $\square$

Definition 5.3.21. Let G and H be strongly connected σ -algebraic groups of positive σ -dimension. A morphism $\phi: G \rightarrow H$ is called an isogeny if $\sigma\text{-dim}(\ker(\phi)) = 0$ and ϕ is surjective. Two strongly connected σ -algebraic groups H_1, H_2 of positive σ -dimension are called isogenous if there exists a strongly connected σ -algebraic group G and isogenies $G \twoheadrightarrow H_1, G \twoheadrightarrow H_2$.

By Theorem 5.2.1 and Corollary 3.2.12 a surjective morphism $\phi: G \twoheadrightarrow H$ is an isogeny, if and only if $\sigma\text{-dim}(G) = \sigma\text{-dim}(H)$. In particular, isogenous σ -algebraic groups have the same σ -dimension.

Lemma 5.3.22. The composition of two isogenies is an isogeny.

Proof. Clearly the composition of surjective morphisms is surjective. If $G_1 \twoheadrightarrow G_2$ and $G_2 \twoheadrightarrow G_3$ are isogenies, then $\sigma\text{-dim}(G_1) = \sigma\text{-dim}(G_2)$ and $\sigma\text{-dim}(G_2) = \sigma\text{-dim}(G_3)$. Therefore $\sigma\text{-dim}(G_1) = \sigma\text{-dim}(G_3)$. $\square$

Lemma 5.3.23. Isogeny is an equivalence relation on the set of strongly connected difference algebraic groups of positive σ -dimension.

Proof. Reflexivity and symmetry are obvious. Let us prove the transitivity. So let $\phi_1: G \twoheadrightarrow H_1$, $\phi_2: G \twoheadrightarrow H_2$ and $\phi'_2: G' \twoheadrightarrow H_2$, $\phi'_3: G' \twoheadrightarrow H_3$ be isogenies. The morphism $\phi_2 \times \phi'_2: G \times G' \rightarrow H_2 \times H_2$ is surjective with kernel $\ker(\phi_2) \times \ker(\phi'_2)$, which has σ -dimension zero by Lemma 2.2.20. The diagonal $D \leq H_2 \times H_2$ given by $D(R) = \{(h_2, h_2) \mid h_2 \in H_2(R)\}$ for any k - σ -algebra R is a σ -closed subgroup of $H_2 \times H_2$ isomorphic to H_2 . Therefore $G'' = ((\phi_2 \times \phi'_2)^{-1}(D))^{so}$ is a σ -closed subgroup of $G \times G'$ with $\sigma\text{-dim}(G'') = \sigma\text{-dim}(H_2)$. Let $\pi: G'' \rightarrow G$ and $\pi': G'' \rightarrow G'$ denote the projections onto the first and second factor

respectively. We have the following diagram

$$\begin{array}{ccccc}
 & & G'' & & \\
 & \swarrow \pi & & \searrow \pi' & \\
 & G & & G' & \\
 \swarrow \phi_1 & & \searrow \phi_2 & \swarrow \phi'_2 & \searrow \phi'_3 \\
 H_1 & & H_2 & & H_3
 \end{array}$$

We claim that π and π' are isogenies. We have $\ker(\pi) \leq 1 \times \ker(\phi'_2)$. Therefore $\sigma\text{-dim}(\ker(\pi)) = 0$ and consequently

$$\sigma\text{-dim}(\pi(G'')) = \sigma\text{-dim}(G'') = \sigma\text{-dim}(H_2) = \sigma\text{-dim}(G).$$

Since G is strongly connected, this shows that $\pi(G'') = G$, so π is surjective. Hence π is an isogeny. Similarly, it follows that π' is an isogeny. The isogenies $\phi_1\pi$ and $\phi'_3\pi'$ (Lemma 5.3.22) now show that H_1 and H_3 are isogenous. $\square$

Theorem 5.3.24. *Assume that k is algebraically closed and inversive. Let G be a strongly connected σ -algebraic group with $\sigma\text{-dim}(G) > 0$. Then there exists a subnormal series*

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = 1 \quad (5.9)$$

such that $\sigma\text{-dim}(G_i) > 0$, G_i is strongly connected, $\sigma\text{-dim}(G_i/G_{i+1}) > 0$ and G_i/G_{i+1} is almost-simple for $i = 0, \dots, n-1$. If

$$G = H_0 \supset H_1 \supset \cdots \supset H_m = 1 \quad (5.10)$$

is another such subnormal series, then $m = n$ and there exists a permutation π such that G_i/G_{i+1} and $H_{\pi(i)}/H_{\pi(i)+1}$ are isogenous for $i = 0, \dots, n-1$.

Proof. Let us first prove the existence statement. Among all normal proper σ -closed subgroups of G choose one, say H , with maximal σ -dimension. If $\sigma\text{-dim}(H) = 0$, G is almost-simple and we are done. So let us assume that $\sigma\text{-dim}(H) > 0$. Since G is strongly connected, $\sigma\text{-dim}(H) < \sigma\text{-dim}(G)$. By construction G/H is almost-simple (Theorem 5.2.4). Let $G_1 = H^{so}$. Then G_1 is normal in G by Proposition 5.3.17 and $\sigma\text{-dim}(G/G_1) > 0$. Let us show that G/G_1 is almost-simple. Let N be a proper normal σ -closed subgroup of G containing G_1 . By choice of H , $\sigma\text{-dim}(N) \leq \sigma\text{-dim}(H)$, but since $\sigma\text{-dim}(H) = \sigma\text{-dim}(G_1) \leq \sigma\text{-dim}(N)$ we have $\sigma\text{-dim}(N) = \sigma\text{-dim}(G_1)$. So G/G_1 is almost-simple (Theorem 5.2.4). As $\sigma\text{-dim}(G_1) < \sigma\text{-dim}(G)$ the claim follows by induction on $\sigma\text{-dim}(G)$.

Now let us prove the uniqueness statement. It follows from Theorem 5.3.5 that (5.9) and (5.10) have equivalent refinements. Let

$$G = G_0 \supsetneq G_{0,1} \supsetneq G_{0,2} \supsetneq \cdots \supsetneq G_{0,n_0} \supsetneq G_1 \supsetneq G_{1,1} \supsetneq \cdots \supsetneq G_{1,n_1} \supsetneq G_2 \supsetneq \cdots \supsetneq G_n = 1 \quad (5.11)$$

be such a refinement of (5.9). For $i = 0, \dots, n-1$, as G_i is strongly connected and G_i/G_{i+1} is almost-simple, $\sigma\text{-dim}(G_i/G_{i,1}) = \sigma\text{-dim}(G_i/G_{i+1}) > 0$ and $\sigma\text{-dim}(G_{i,j}/G_{i,j+1}) = 0$ for $j = 1, \dots, n_i - 1$, also $\sigma\text{-dim}(G_{i,n_i}/G_{i+1}) = 0$. The kernel of $G_i/G_{i+1} \twoheadrightarrow G_i/G_{i,1}$ has σ -dimension zero, so G_i/G_{i+1} and $G_i/G_{i,1}$ are isogenous. In summary, we find that

among the quotient groups of the subnormal series (5.11), there are precisely n of positive σ -dimension, (namely G_i/G_{i+1} , $i = 0, \dots, n-1$). A similar statement applies to the equivalent refinement of (5.10). Therefore $n = m$ and there is a permutation π such that G_i/G_{i+1} and $H_{\pi(i)}/H_{\pi(i)+1}$ are isogenous for $i = 0, \dots, n-1$. $\square$

Remark 5.3.25. *It is clear from the proof that the uniqueness statement in Theorem 5.3.24 is also valid without any restriction on the base σ -field k .*

Chapter 6

Étale difference algebraic groups

In this chapter we study σ -étale σ -algebraic groups in full detail. As explained in Section 4.1 every σ -algebraic group G fits into an exact sequence $1 \rightarrow G^\circ \rightarrow G \rightarrow \pi_0(G) \rightarrow 1$ with G° connected and $\pi_0(G)$ σ -étale. In this sense the study of arbitrary σ -algebraic groups reduces to the study of connected σ -algebraic groups and the study of σ -étale σ -algebraic groups.

Over a σ -field of characteristic zero the σ -étale σ -algebraic groups are precisely the σ -algebraic groups of order zero (Corollary 6.1.8). In this sense σ -étale σ -algebraic groups are the “smallest possible” σ -algebraic groups. However, a σ -algebraic group may have infinitely many components and so σ -étale σ -algebraic groups are in a certain sense “infinite”, e.g., the coordinate ring of a σ -étale σ -algebraic group may be infinite dimensional as a k -vector space. In particular, a σ -étale σ -algebraic group is a much richer structure than just a finite group.

The category of étale algebraic groups is equivalent to the category of finite groups with a continuous action of the absolute Galois group ([Wat79, Section 6.4]). One of the main results of this chapter is a difference analog of this result (Theorem 6.2.14). We show that σ -étale σ -algebraic groups are equivalent to certain profinite groups equipped with a σ -continuous action of the absolute Galois group.

An étale algebraic group, when interpreted as a σ -algebraic group is σ -étale. A σ -étale σ -algebraic group of this form will be called benign. The second main result of this chapter is a decomposition theorem for σ -étale σ -algebraic groups (Theorem 6.4.10). Roughly speaking, we show that, up to some finite interference, any σ -étale σ -algebraic group can be decomposed into benign σ -algebraic groups. This result is analogous to Babbitt’s decomposition theorem ([Lev08, Theorem 5.4.13, p. 336]), an important structure theorem for algebraic extensions of σ -fields.

We also study σ -infinitesimal σ -algebraic groups and prove two structure theorems (Theorems 6.3.9 and 6.3.14) for finite σ -algebraic groups.

6.1 Basic properties of σ -étale difference algebraic groups

Recall (Definition 4.1.10) that a σ -algebraic group G is called σ -étale if $k\{G\}$ is a union of étale k -algebras, i.e., every element of $k\{G\}$ satisfies a separable polynomial over k . Clearly a σ -étale σ -algebraic group has σ -dimension zero and order zero. However, the limit degree may be strictly larger than one.

Clearly a σ -algebraic group G is σ -étale if and only if $G = \pi_0(G)$. Thus a σ -algebraic

group is σ -étale if and only if its identity component is trivial. Let us see some examples of σ -étale σ -algebraic groups.

Example 6.1.1. Let $n \geq 2$ be an integer. If the characteristic of k does not divide n , the σ -algebraic group G given by

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

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

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 $k\{G\} = \cup k[\mathcal{G}[i]]$ is σ -étale. The statement that $\text{ld}(G) = |\mathcal{G}|$ is a special case of Example 2.4.6.

Note that Example 6.1.1 is a special case of Example 6.1.2 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 .

Definition 6.1.3. 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 $\mathcal{G}$.

Not every σ -étale σ -algebraic is benign. For example, a strongly σ -étale σ -algebraic group is σ -étale but not benign.

Example 6.1.4. Let $\mathbb{G}$ be a finite group and $\sigma: \mathbb{G} \rightarrow \mathbb{G}$ a group endomorphism. Then the σ -algebraic group G constructed from this data as in Example 2.1.15 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.

One of our main goals in this chapter is to show that in a certain sense Examples 6.1.2 and 6.1.4 are the “only” examples of σ -étale σ -algebraic groups. Indeed, Babbitt’s decomposition theorem for σ -étale σ -algebraic groups (Theorem 6.4.10) shows that any σ -étale σ -algebraic group can be decomposed into a strongly σ -étale σ -algebraic group, a σ -infinitesimal σ -étale σ -algebraic group and benign σ -algebraic groups.

Lemma 6.1.5. *Quotients and σ -closed subgroups of σ -étale σ -algebraic groups are σ -étale.*

Proof. Let G be a σ -étale σ -algebraic group. Since quotients of G correspond to k - σ -Hopf subalgebras of $k\{G\}$ (Theorem 3.3.6) it is clear that quotients of G are σ -étale.

If H is a σ -closed subgroup $k\{H\} = k\{G\}/\mathbb{I}(H)$. Since quotients of étale k -algebras are étale k -algebras it follows that H is σ -étale. $\square$

Lemma 6.1.6. *Let $\mathcal{G}$ be an algebraic group and $G \leq \mathcal{G}$ a σ -closed subgroup. For $i \geq 0$ 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 $i \geq 0$.

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 by Lemma 1.1.4. $\square$

A σ -closed subgroup of an étale algebraic group is σ -étale (Lemma 6.1.5). Conversely, if G is an étale algebraic group, we can embed G as σ -closed subgroup into an étale algebraic group. For example, we may first embed G into some algebraic group $\mathcal{G}$ (Theorem 2.1.17) and then consider the Zariski closure of G in $\mathcal{G}$. 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 6.1.7. *A σ -algebraic group is σ -étale if and only if it 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 ([Wat79, Ex. 8, p. 53]). It follows from Lemma 6.1.6 that G is σ -étale. $\square$

Corollary 6.1.8. *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 ([Wat79, Theorem 11.4, p. 86]). Thus the claim follows from Proposition 6.1.7. $\square$

6.2 Profinite σ -groups

Profinite σ -groups provide a combinatorial description of σ -étale σ -algebraic groups. The category of étale algebraic groups is equivalent to the category of finite groups with a continuous action of the absolute Galois group of the base field ([Wat79, Section 6.4]). The purpose of this section is to establish an analogous result for σ -étale σ -algebraic groups.

Definition 6.2.1. *A profinite σ -group is a profinite group $\mathbf{G}$ together with a continuous endomorphism $\sigma: \mathbf{G} \rightarrow \mathbf{G}$.*

A morphism of profinite σ -groups is a continuous morphism of groups that commutes with the action of σ .

Example 6.2.2. A finite group with an endomorphism can be regarded as a profinite σ -group in virtue of the discrete topology.

Example 6.2.3. Let $L|K$ be an extension of σ -fields such that the underlying field extension is Galois. Then the Galois group $\mathbf{G}$ of $L|K$ is naturally a profinite σ -group: Clearly $\mathbf{G}$ is a profinite group. To define $\sigma: \mathbf{G} \rightarrow \mathbf{G}$, note that for every $g \in \mathbf{G}$ the maps σ and $g\sigma$ are extensions of $\sigma: K \rightarrow K$ to L . Thus, by Lemma 4.2.21, there exists a unique $g^\sigma \in \mathbf{G}$ such that

$$\begin{array}{ccc} L & \xrightarrow{g^\sigma} & L \\ \sigma \downarrow & & \downarrow \sigma \\ L & \xrightarrow{g} & L \end{array}$$

commutes. Then $\sigma: \mathbf{G} \rightarrow \mathbf{G}$, $g \mapsto g^\sigma$ is a group endomorphism. To see that σ is continuous, note that for an open subgroup $\mathbf{H}$ of $\mathbf{G}$ and $M = L^\mathbf{H}$ we have

$$\sigma^{-1}(\mathbf{H}) = \{g \in \mathbf{G} \mid g^\sigma(a) = a \ \forall a \in M\} = \{g \in \mathbf{G} \mid g(\sigma(a)) = \sigma(a) \ \forall a \in M\}.$$

Thus $\sigma^{-1}(\mathbf{H})$ is the Galois group of $L|K(\sigma(M))$.

By a σ -projective system we mean a family $(\mathbf{G}_i)_{i \in \mathbb{N}}$ of finite groups together with morphisms of groups $\pi_i, \sigma_i: \mathbf{G}_i \rightarrow \mathbf{G}_{i-1}$ for $i \geq 1$ such that $\ker(\pi_i) \cap \ker(\sigma_i) = 1$ and

$$\begin{array}{ccc} \mathbf{G}_i & \xrightarrow{\pi_i} & \mathbf{G}_{i-1} \\ \sigma_i \downarrow & & \downarrow \sigma_{i-1} \\ \mathbf{G}_{i-1} & \xrightarrow{\pi_{i-1}} & \mathbf{G}_{i-2} \end{array} \quad (6.1)$$

commutes for $i \geq 2$. The projective limit

$$\mathbf{G} = \varprojlim_{i \in \mathbb{N}} \mathbf{G}_i = \{(g_0, g_1, \dots) \mid g_i \in \mathbf{G}_i, \pi_i(g_i) = g_{i-1}\}$$

is a profinite σ -group with

$$\sigma: \mathbf{G} \rightarrow \mathbf{G}, (g_0, g_1, \dots) \mapsto (\sigma_1(g_1), \sigma_2(g_2), \dots).$$

Example 6.2.4. A finite group $\mathbf{H}$ gives rise to a particularly simple σ -projective system by setting $\mathbf{G}_i = \mathbf{H}^{i+1}$,

$$\pi_i: \mathbf{G}_i \rightarrow \mathbf{G}_{i-1}, (h_0, \dots, h_i) \mapsto (h_0, \dots, h_{i-1}) \text{ and } \sigma_i: \mathbf{G}_i \rightarrow \mathbf{G}_{i-1}, (h_0, \dots, h_i) \mapsto (h_1, \dots, h_i).$$

Then $\mathbf{G} = \mathbf{H}^\mathbb{N}$ with $\sigma((h_0, h_1, h_2, \dots)) = (h_1, h_2, \dots)$.

Lemma 6.2.5. *The following conditions on a profinite σ -group $\mathbf{G}$ are equivalent.*

- (i) $\mathbf{G}$ is the projective limit of a σ -projective system.
- (ii) There exists a normal open subgroup $\mathbf{N}$ of $\mathbf{G}$ such that $\bigcap_{i \geq 0} \sigma^{-i}(\mathbf{N}) = 1$.

Proof. Assume that $\mathbf{G} = \varprojlim \mathbf{G}_i$ is the limit of a σ -projective system. Let $\mathbf{N}$ be the kernel of the projection $\mathbf{G} \rightarrow \mathbf{G}_0$. Then $\mathbf{N}$ is normal and open in $\mathbf{G}$. We will show by induction on $j \geq 1$ that every element of $\mathbf{H} = \bigcap_{i \geq 0} \sigma^{-i}(\mathbf{N})$ has its first j entries equal to 1. The case $j = 1$ is clear as $\mathbf{H} \subset \mathbf{N}$. So let $g = (\bar{1}, \dots, 1, g_j, g_{j+1}, \dots) \in \mathbf{H}$. Then $\pi_j(g_j) = 1$ and since $\sigma(g) = (1, \dots, 1, \sigma_j(g_j), \dots) \in \mathbf{H}$, it follows from the induction hypothesis that $\sigma_j(g_j) = 1$. As $\ker(\pi_j) \cap \ker(\sigma_j) = 1$ we find $g_j = 1$. This shows that $\mathbf{H} = 1$. So (i) implies (ii).

Now assume that $\mathbf{N}$ is a normal open subgroup of $\mathbf{G}$ such that $\bigcap_{i \geq 0} \sigma^{-i}(\mathbf{N}) = 1$. For $i \geq 0$ set $\mathbf{N}_i = \mathbf{N} \cap \sigma^{-1}(\mathbf{N}) \cap \dots \cap \sigma^{-i}(\mathbf{N})$ and $\mathbf{G}_i = \mathbf{G}/\mathbf{N}_i$. Then the $\mathbf{G}_i$'s are finite groups and we have morphisms $\pi_i: \mathbf{G}_i \rightarrow \mathbf{G}_{i-1}$ deduced from the inclusion $\mathbf{N}_i \subset \mathbf{N}_{i-1}$ and morphisms $\sigma_i: \mathbf{G}_i \rightarrow \mathbf{G}_{i-1}$ induced by $\sigma: \mathbf{G} \rightarrow \mathbf{G}$. By construction, these maps form a σ -projective system.

In general, if $\mathbf{G}$ is a profinite group and $(\mathbf{N}_i)$ a directed family of normal open subgroups of $\mathbf{G}$ with $\bigcap_i \mathbf{N}_i = 1$, then the canonical map $\mathbf{G} \rightarrow \varprojlim_i \mathbf{G}/\mathbf{N}_i$ is an isomorphism of topological groups ([FJ08, Lemma 1.2.4, p. 7]).

Thus, as a topological group, $\mathbf{G}$ is canonically isomorphic to the limit of the above σ -projective system. By construction, the isomorphism is also compatible with σ . $\square$

Definition 6.2.6. A profinite σ -group is called of finite σ -type if it satisfies the equivalent conditions of Lemma 6.2.5.

Definition 6.2.6 is motivated by the following fact (cf. [Lev08, Section 8.1]):

Lemma 6.2.7. Let $L|K$ be an extension of σ -fields such that the underlying field extension is Galois. Let $\mathbf{G}$ denote the Galois group of $L|K$, considered as a profinite σ -group as in Example 6.2.3. Then $\mathbf{G}$ is of finite σ -type if and only if L is a finitely σ -generated σ -field extension of K .

Proof. Let $\mathbf{N}$ be a normal open subgroup of $\mathbf{G}$ with $\bigcap_{i \geq 0} \sigma^{-i}(\mathbf{N}) = 1$. Then $M = L^{\mathbf{N}}$ is a finite Galois extension of K . We claim that $L = K\langle M \rangle$. It suffices to show that the Galois group of $L|K\langle M \rangle$ is trivial. But the Galois group of $L|K\langle M \rangle$ consists of all $g \in \mathbf{G}$ which fix every element of $K(\sigma^i(M))$ for $i \geq 0$. Since the Galois group of $L|K(\sigma^i(M))$ is $\sigma^{-i}(\mathbf{N})$ (cf. Example 6.2.3) it follows that the Galois group of $L|K\langle M \rangle$ equals $\bigcap_{i \geq 0} \sigma^{-i}(\mathbf{N}) = 1$.

Conversely, if $L|K$ is finitely σ -generated, then $L = K\langle M \rangle$ for a finite Galois extension M of K . Let $\mathbf{N}$ be the kernel of the restriction map from $\mathbf{G}$ to the Galois group of $M|K$. Then $\mathbf{N}$ is normal and open in $\mathbf{G}$. Since $\bigcap_{i \geq 0} \sigma^{-i}(\mathbf{N})$ is the Galois group of L over $K\langle M \rangle = L$, we find $\bigcap_{i \geq 0} \sigma^{-i}(\mathbf{N}) = 1$. $\square$

In the proof of the main theorem of this section we will use the following fact about field extensions.

Lemma 6.2.8. Let $k_s|k$ be an extension of σ -fields such that k_s is the separable algebraic closure of k . Let k' be a separable algebraic field extension of k and $\sigma': k' \rightarrow k_s$ a morphism of rings such that

$$\begin{array}{ccc} k' & \xrightarrow{\sigma'} & k_s \\ \uparrow & & \uparrow \\ k & \xrightarrow{\sigma} & k \end{array}$$

commutes. Then there exists a unique k -embedding $\alpha: k' \rightarrow k_s$ such that $\sigma' = \sigma\alpha$.

Proof. The uniqueness of α is clear from the injectivity of σ . Let $\beta: k' \rightarrow k_s$ be some k -embedding. Using Zorn's Lemma, we may extend $\sigma'\beta^{-1}: \beta(k') \rightarrow k_s$ to an extension $\sigma_1: k_s \rightarrow k_s$ of $\sigma: k \rightarrow k$. By Lemma 4.2.21 there exists an automorphism τ of $k_s|k$ such that $\sigma_1 = \sigma\tau$ on k_s . Now $\alpha = \tau\beta: k' \rightarrow k_s$ has the required property. $\square$

Before proceeding to the main theorem of this section, let us recall the algebraic facts that lead to the statement that the category of étale algebraic groups is equivalent to the category of finite groups with a continuous action of the absolute Galois group. (See Sections 6.3 and 6.4 in [Wat79] or Section 2 in Chapter XII in [Mil12].)

Let k be a field, k_s the separable algebraic closure of k and $\mathcal{G}$ the Galois group of k_s over k . If $\mathcal{G}$ is acting on a group, we always assume that every $\tau \in \mathcal{G}$ is acting as a group automorphism. An action of $\mathcal{G}$ on a finite set X is called continuous if $\mathcal{G} \times X \rightarrow X$ is a continuous map, where X is considered as a discrete topological space. This is the case if and only if the action factors through a finite quotient of $\mathcal{G}$.

Let R be a k -algebra. For the sake of brevity, let us write

$$F(R)$$

for the set of all k -algebra morphisms from R to k_s . There is a natural action of $\mathcal{G}$ on $F(R)$ via the action on k_s : For $\tau \in \mathcal{G}$ and $g \in F(R)$ we have $\tau(g): R \xrightarrow{g} k_s \xrightarrow{\tau} k_s$. If R is an étale k -algebra, $F(R)$ is a finite set and the action of $\mathcal{G}$ on $F(R)$ is continuous. A morphism of finite sets with $\mathcal{G}$ -action is simply a map of sets that commutes with the $\mathcal{G}$ -action.

Theorem 6.2.9. *The functor $R \rightsquigarrow F(R)$ defines an anti-equivalence between the category of étale k -algebras and the category of finite sets with a continuous $\mathcal{G}$ -action. In this connection an injective map of sets corresponds to a surjective morphism of k -algebras. Moreover, the product of sets corresponds to the tensor product of k -algebras.*

Proof. The statement about the equivalence is Theorem 6.3 in [Wat79], while the statement about products is obvious. So let us prove the statement about injective maps. Let $\psi: R \rightarrow S$ be a morphism of étale k -algebras such that $F(S) \rightarrow F(R)$ is injective. Suppose ψ is not surjective. Then $\psi(R)$ is an étale algebra properly contained in S .

In general, for an étale algebra R , the number of k -algebra morphisms from R to k_s equals the dimension of R as a k -vector space (cf. [Bou90, Prop. 4, Chapter V, §6, No. 5, A.V.32]). Because $\psi(R)$ is properly contained in S , it follows that there must exist two distinct morphisms g_1, g_2 from S to k_s with the same restriction to $\psi(R)$. But then g_1 and g_2 have the same image under $F(S) \rightarrow F(R)$; a contradiction. $\square$

Lemma 6.2.10. *Let R be a k -algebra that is integral and separable over k . If f_1 and f_2 are two distinct elements of R , then there exists a morphism $g: R \rightarrow k_s$ of k -algebras such that $g(f_1) \neq g(f_2)$.*

Proof. Because R is reduced there exists a prime ideal $\mathfrak{p}$ of R such that $f_1 - f_2 \notin \mathfrak{p}$. Then $R/\mathfrak{p}$ is a separable algebraic field extension of k and therefore embeds into k_s . The precomposition with the canonical map $R \rightarrow R/\mathfrak{p}$ yields a morphism g with the required property. $\square$

Let R be a k -Hopf algebra that is integral and separable over k , i.e., R is the directed union of its étale Hopf subalgebras. There is a natural bijection between $F(R)$ and $\text{Spec}(R \otimes_k k_s)$: Every $g \in F(R)$ extends k_s -linearly to a map $R \otimes_k k_s \rightarrow k_s$ whose kernel is a prime ideal $\mathfrak{p}$ of $R \otimes_k k_s$. Conversely, for a prime ideal $\mathfrak{p}$ of $R \otimes_k k_s$ we have $R \otimes_k k_s/\mathfrak{p} = k_s$. So we can define an element $g \in F(R)$ by sending $f \in R$ to the image of $f \otimes 1$ in k_s . Now we use the bijection $F(R) \simeq \text{Spec}(R \otimes_k k_s)$ to define a topology on $F(R)$.

As a corollary to Theorem 6.2.9 we obtain:

Corollary 6.2.11. *Let R and S be k -Hopf algebras that are integral and separable over k . Then there is a natural bijection between the morphisms of k -Hopf algebras from R to S and the continuous group morphisms from $F(S)$ to $F(R)$ that commute with the $\mathcal{G}$ -action.*

Proof. Let $\mathcal{G}$ be the affine group scheme over k represented by S . So $k[\mathcal{G}] = S$ and $\mathcal{G}(k_s) = F(S)$. Similarly, let $\mathcal{H}$ be the affine group scheme represented by R . Let $\psi: k[\mathcal{H}] \rightarrow k[\mathcal{G}]$ be a morphism of k -Hopf algebras. Then the induced map $\tilde{\psi}: \mathcal{G}(k_s) \rightarrow \mathcal{H}(k_s)$ is a morphism of groups. We have a commutative diagram

$$\begin{array}{ccc} \mathcal{G}(k_s) & \xrightarrow{\quad} & \mathcal{H}(k_s) \\ \simeq \downarrow & & \downarrow \simeq \\ \text{Spec}(k[\mathcal{G}] \otimes_k k_s) & \longrightarrow & \text{Spec}(k[\mathcal{H}] \otimes_k k_s) \end{array}$$

where the lower horizontal arrow is continuous, because it is induced by the morphism of rings $k[\mathcal{H}] \otimes_k k_s \rightarrow k[\mathcal{G}] \otimes_k k_s$. Therefore $\tilde{\psi}$ is continuous. Clearly $\tilde{\psi}$ commutes with the $\mathcal{G}$ -action.

Let $\psi_1, \psi_2: k[\mathcal{H}] \rightarrow k[\mathcal{G}]$ be morphisms of k -Hopf algebras with $\psi_1 \neq \psi_2$. Then there exists $f \in k[\mathcal{H}]$ such that $\psi_1(f) \neq \psi_2(f)$. By Lemma 6.2.10 there exists a morphism $g: k[\mathcal{G}] \rightarrow k_s$ with $g(\psi_1(f)) \neq g(\psi_2(f))$. So $\tilde{\psi}_1(g) \neq \tilde{\psi}_2(g)$. This shows that $\psi \mapsto \tilde{\psi}$ is injective.

To prove the surjectivity, let $\varphi: \mathcal{G}(k_s) \rightarrow \mathcal{H}(k_s)$ be a continuous morphism of groups that commutes with the $\mathcal{G}$ -action. Let I denote the directed set of all étale k -Hopf subalgebras of $k[\mathcal{G}]$. For $i \in I$ let $\mathcal{G}_i$ denote the corresponding étale algebraic group. So $k[\mathcal{G}]$ is the directed union of the $k[\mathcal{G}_i]$'s and $\mathcal{G}(k_s) = \varprojlim \mathcal{G}_i(k_s)$, where the projective limit is taken in the category of groups equipped with a $\mathcal{G}$ -action.

If R_i is a directed system of rings, then the projective limit of the $\text{Spec}(R_i)$'s in the category of topological spaces agrees with the spectrum of the direct limit of the R_i 's. (See [Sta14, Tag 01YY].) As $\text{Spec}(k[\mathcal{G}_i] \otimes_k k_s)$ is a discrete topological space, it follows that $\mathcal{G}(k_s) = \varprojlim \mathcal{G}_i(k_s)$ also as topological spaces, where each $\mathcal{G}_i(k_s)$ is given the discrete topology. Similarly to $\mathcal{G}$, we write $k[\mathcal{H}]$ as a directed union of its étale Hopf subalgebras $k[\mathcal{H}_j]$. Because φ is continuous and $\mathcal{G}$ -equivariant, also the composition $\varphi_j: \mathcal{G}(k_s) \rightarrow \mathcal{H}(k_s) \rightarrow \mathcal{H}_j(k_s)$ is continuous and $\mathcal{G}$ -equivariant. So the kernel of φ_j is an open subgroup of $\mathcal{G}(k_s)$. By the definition of the (profinite) topology on $\mathcal{G}(k_s) = \varprojlim \mathcal{G}_i(k_s)$ there exists an $i \in I$ such that $\ker(\varphi_j)$ contains the kernel of $\mathcal{G}(k_s) \rightarrow \mathcal{G}_i(k_s)$. Thus there is an induced $\mathcal{G}$ -equivariant morphism of finite groups $\mathcal{G}_i(k_s) \rightarrow \mathcal{H}_j(k_s)$, which, by Theorem 6.2.9, corresponds to a morphism of k -Hopf algebras $k[\mathcal{H}_j] \rightarrow k[\mathcal{G}_i] \subset k[\mathcal{G}]$. These morphisms are compatible and therefore yield a morphism of k -Hopf algebras $\psi: k[\mathcal{H}] \rightarrow k[\mathcal{G}]$. Clearly $\tilde{\psi} = \varphi$. $\square$

Let k be a σ -field and let k_s denote the separable algebraic closure of k . By Lemma 1.1.5 we can extend $\sigma: k \rightarrow k$ to an endomorphism of k_s . Let us fix such an extension and let $\mathcal{G}$ denote the Galois group of $k_s|k$. As explained in Example 6.2.3 the group $\mathcal{G}$ is naturally a profinite σ -group.

Let $\mathbf{G}$ be a finite group equipped with a continuous $\mathcal{G}$ -action. Then we can define a new action $(\tau, g) \mapsto \tau.g$ of $\mathcal{G}$ on $\mathbf{G}$ by precomposition with $\sigma: \mathcal{G} \rightarrow \mathcal{G}$, i.e., $\tau.g = \sigma(\tau)(g)$. Because $\sigma: \mathcal{G} \rightarrow \mathcal{G}$ is continuous this new action is also continuous. We denote the finite group $\mathbf{G}$ equipped with this new action by

$${}^\sigma \mathbf{G}.$$

Lemma 6.2.12. *If $\mathbf{G}$ corresponds to the étale algebraic group $\mathcal{G}$. Then ${}^\sigma \mathbf{G}$ corresponds to the étale algebraic group ${}^\sigma \mathcal{G}$.*

Proof. Let $\mathcal{G}$ be an étale algebraic group. Applying σ yields a bijection $\mathcal{G}(k_s) \rightarrow ({}^\sigma \mathcal{G})(k_s)$: More formally, let

$$\psi: \mathcal{G}(k_s) = \text{Hom}(k[\mathcal{G}], k_s) \longrightarrow \text{Hom}({}^\sigma(k[\mathcal{G}]), k_s) = ({}^\sigma \mathcal{G})(k_s)$$

be the map that associates to $g \in \text{Hom}(k[\mathcal{G}], k_s)$ the morphism $\psi(g) \in \text{Hom}({}^\sigma(k[\mathcal{G}]), k_s)$ defined by $\psi(g)(f \otimes \lambda) = \sigma(g(f))\lambda$ for $f \in k[\mathcal{G}]$ and $\lambda \in k$. As σ is injective on k_s it is clear that ψ is injective. Because ψ is a map of finite sets, it follows that ψ is an isomorphism of groups. We have

$$\psi(\sigma(\tau)(g))(f \otimes \lambda) = \sigma(\sigma(\tau)(g(f)))\lambda = \tau(\sigma(g(f)))\lambda = \tau(\psi(g)(f \otimes \lambda)).$$

Thus $\psi(\sigma(\tau)(g)) = \tau(\psi(g))$. In other words, ψ is an isomorphism between ${}^\sigma(\mathcal{G}(k_s))$ and $({}^\sigma\mathcal{G})(k_s)$. $\square$

Let $(\mathbf{G}_i)_{i \in \mathbb{N}}$ be a σ -projective system and let each $\mathbf{G}_i$ be equipped with a continuous $\mathcal{G}$ -action such that

$$\pi_i(\tau(g)) = \tau(\pi_i(g))$$

and

$$\sigma_i(\tau(g)) = \sigma(\tau)(\sigma_i(g))$$

for $\tau \in \mathcal{G}$, $g \in \mathbf{G}_i$ and $i \geq 1$. Then the projective limit $\mathbf{G} = \varprojlim \mathbf{G}_i$ is naturally equipped with a $\mathcal{G}$ -action by $\tau(g_0, g_1, \dots) = (\tau(g_0), \tau(g_1), \dots)$ and we have

$$\sigma(\tau(g)) = \sigma(\tau)(\sigma(g))$$

for $\tau \in \mathcal{G}$ and $g \in \mathbf{G}$.

Definition 6.2.13. *An action of $\mathcal{G}$ on a profinite σ -group $\mathbf{G}$ is called σ -continuous if $\mathbf{G}$ is the projective limit of a σ -projective system such that the $\mathcal{G}$ -action on $\mathbf{G}$ is induced from an action of $\mathcal{G}$ on the σ -projective system as above.*

A morphism of profinite σ -groups with a σ -continuous $\mathcal{G}$ -action is a morphism of profinite σ -groups that commutes with the $\mathcal{G}$ -action. Now we are prepared to prove the main theorem of this section.

Theorem 6.2.14. *The category of σ -étale σ -algebraic groups is equivalent to the category of profinite σ -groups of finite σ -type with a σ -continuous $\mathcal{G}$ -action.*

Proof. The equivalence is given by the functor $G \rightsquigarrow G^\#(k_s)$. So let us explain how $\mathbf{G} = G^\#(k_s) = \text{Hom}(k\{G\}^\#, k_s^\#)$ is a profinite σ -group of finite σ -type with a σ -continuous $\mathcal{G}$ -action. Clearly $\mathbf{G}$ is a group. Note that $\mathbf{G}$ is in bijection with $\text{Spec}(k\{G\} \otimes_k k_s)$: Every $g \in \mathbf{G}$ extends k_s -linearly to a map $g: k\{G\} \otimes_k k_s \rightarrow k_s$, whose kernel is a prime ideal $\mathfrak{p}$ in $k\{G\} \otimes_k k_s$. Conversely, a prime ideal $\mathfrak{p}$ of $k\{G\} \otimes_k k_s$ satisfies $(k\{G\} \otimes_k k_s)/\mathfrak{p} = k_s$ and therefore gives rise to a morphism $g: k\{G\} \rightarrow k_s$ by sending $f \in k\{G\}$ to the image of $f \otimes 1$ in k_s . On $\text{Spec}(k\{G\} \otimes_k k_s)$ we have a continuous map σ given by $\mathfrak{p} \mapsto \sigma^{-1}(\mathfrak{p})$. By transport of structure, we can use the bijection

$$\mathbf{G} \simeq \text{Spec}(k\{G\} \otimes_k k_s)$$

to define a topology and a continuous map σ on $\mathbf{G}$. We will next give a more explicit description of $\sigma: \mathbf{G} \rightarrow \mathbf{G}$. We claim that for $g \in \mathbf{G}$ there exists a $g^\sigma \in \mathbf{G}$ such that

$$\begin{array}{ccc} k\{G\} & \xrightarrow{g^\sigma} & k_s \\ \sigma \downarrow & & \downarrow \sigma \\ k\{G\} & \xrightarrow{g} & k_s \end{array} \quad (6.2)$$

commutes. The uniqueness of g^σ follows from the injectivity of $\sigma: k_s \rightarrow k_s$. To prove the existence of g^σ , let $\mathfrak{p}$ denote the kernel of g and set

$$\sigma': k\{G\}/\sigma^{-1}(\mathfrak{p}) \xrightarrow{\sigma} k\{G\}/\mathfrak{p} \hookrightarrow k_s.$$

By Lemma 6.2.8 there exists a k -embedding $\alpha: k\{G\}/\sigma^{-1}(\mathfrak{p}) \rightarrow k_s$ such that $\sigma' = \sigma\alpha$. Thus $g^\sigma: k\{G\} \rightarrow k\{G\}/\sigma^{-1}(\mathfrak{p}) \xrightarrow{\alpha} k_s$ has the required property.

Since diagram (6.2) extends to

$$\begin{array}{ccc} k\{G\} \otimes_k k_s & \xrightarrow{g^\sigma} & k_s \\ \sigma \downarrow & & \downarrow \sigma \\ k\{G\} \otimes_k k_s & \xrightarrow{g} & k_s \end{array}$$

we find that $\sigma(g) = g^\sigma$. Using this description it is easy to see that $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ is a morphism of groups. Indeed, for $g_1, g_2 \in \mathbf{G}$, the commutativity of

$$\begin{array}{ccccc} k\{G\} & \xrightarrow{\Delta} & k\{G\} \otimes_k k\{G\} & \xrightarrow{\sigma(g_1) \cdot \sigma(g_2)} & k_s \\ \sigma \downarrow & & \sigma \downarrow & & \downarrow \sigma \\ k\{G\} & \xrightarrow{\Delta} & k\{G\} \otimes_k k\{G\} & \xrightarrow{g_1 \cdot g_2} & k_s \end{array} \quad (6.3)$$

shows that $\sigma(g_1 g_2) = \sigma(g_1) \sigma(g_2)$.

To see that $\mathbf{G}$ is profinite and of finite σ -type we may choose a σ -closed embedding of G into some algebraic group $\mathcal{G}$. For $i \geq 0$ let $G[i]$ denote the i -th order Zariski closure of G in $\mathcal{G}$. By Lemma 6.1.6 the algebraic groups $G[i]$ are étale. So $\mathbf{G}_i = G[i](k_s) = \text{Hom}(k[G[i]], k_s)$ is a finite group. Since $k\{G\} = \bigcup_{i \geq 0} k[G[i]]$, it is clear that $\mathbf{G} = \varprojlim \mathbf{G}_i$ as groups, where the projective limit is formed by virtue of the group morphisms $\pi_i: \mathbf{G}_i \rightarrow \mathbf{G}_{i-1}$ deduced from the projections $G[i] \rightarrow G[i-1]$. The commutative diagram

$$\begin{array}{ccc} \mathbf{G} & \xrightarrow{\simeq} & \varprojlim \mathbf{G}_i \\ \simeq \downarrow & & \downarrow \simeq \\ \text{Spec}(k\{G\} \otimes_k k_s) & \xrightarrow{\simeq} & \varprojlim \text{Spec}(k[G[i]] \otimes_k k_s) \end{array}$$

shows that $\mathbf{G} = \varprojlim \mathbf{G}_i$ as topological groups, where each $\mathbf{G}_i$ is given the discrete topology. Thus $\mathbf{G}$ is profinite.

Let $i \geq 1$. As above, for diagram (6.2), one shows that for every $g \in \mathbf{G}_i$ there exists a unique $g^\sigma \in \mathbf{G}_{i-1}$ such that

$$\begin{array}{ccc} k[G[i-1]] & \xrightarrow{g^\sigma} & k_s \\ \sigma \downarrow & & \downarrow \sigma \\ k[G[i]] & \xrightarrow{g} & k_s \end{array}$$

commutes. Define $\sigma_i: \mathbf{G}_i \rightarrow \mathbf{G}_{i-1}$, $g \mapsto g^\sigma$. A diagram similar to (6.3), shows that σ_i is a morphism of groups. It follows from the commutativity of

$$\begin{array}{ccccc} k[G[i-2]] & \hookrightarrow & k[G[i-1]] & \xrightarrow{\sigma_i(g)} & k_s \\ \sigma \downarrow & & \downarrow \sigma & & \downarrow \sigma \\ k[G[i-1]] & \hookrightarrow & k[G[i]] & \xrightarrow{g} & k_s \end{array}$$

that

$$\begin{array}{ccc} \mathbf{G}_i & \xrightarrow{\pi_i} & \mathbf{G}_{i-1} \\ \sigma_i \downarrow & & \downarrow \sigma_{i-1} \\ \mathbf{G}_{i-1} & \xrightarrow{\pi_{i-1}} & \mathbf{G}_{i-2} \end{array}$$

commutes for $i \geq 2$. To show that $\ker(\pi_i) \cap \ker(\sigma_i) = 1$, note that $g \in \mathbf{G}_i$ is the identity if and only if g vanishes on the ideal $\mathfrak{m}_{k[G[i]]} \subset k[G[i]]$. If $g \in \ker(\pi_i) \cap \ker(\sigma_i)$, then g vanishes on $\mathfrak{m}_{k[G[i-1]]}$ and on $\sigma(\mathfrak{m}_{k[G[i-1]]})$. Since $\mathfrak{m}_{k[G[i-1]]}$ and $\sigma(\mathfrak{m}_{k[G[i-1]]})$ generate $\mathfrak{m}_{k[G[i]]}$, this shows that $g = 1$. In summary, we find that the $\mathbf{G}_i$'s form a σ -projective system. Since the limit of the σ_i 's agrees with the original σ on $\mathbf{G}$, we have thus shown that $\mathbf{G}$ is a profinite σ -group of finite σ -type.

We next describe the $\mathcal{G}$ -action. For $\tau \in \mathcal{G}$ and $g \in \mathbf{G}$ let $\tau(g)$ denote the composition $\tau(g): k\{G\} \xrightarrow{g} k_s \xrightarrow{\tau} k_s$. In this fashion every $\tau \in \mathcal{G}$ defines a group automorphism of $\mathbf{G}$ and we have defined an action of $\mathcal{G}$ on $\mathbf{G}$. It is easy to see that this action is σ -continuous: We have a continuous action of $\mathcal{G}$ on each $\mathbf{G}_i$ by $\tau(g): k[G[i]] \xrightarrow{g} k_s \xrightarrow{\tau} k_s$ for $\tau \in \mathcal{G}$ and $g \in \mathbf{G}_i$. Clearly $\pi_i(\tau(g)) = \tau(\pi_i(g))$ and it follows from the commutative diagram

$$\begin{array}{ccccc} k[G[i-1]] & \xrightarrow{\sigma_i(g)} & k_s & \xrightarrow{\sigma(\tau)} & k_s \\ \sigma \downarrow & & \sigma \downarrow & & \sigma \downarrow \\ k[G[i]] & \xrightarrow{g} & k_s & \xrightarrow{\tau} & k_s \end{array}$$

that $\sigma_i(\tau(g)) = \sigma(\tau)(\sigma_i(g))$ for $\tau \in \mathcal{G}$, $i \geq 1$ and $g \in \mathbf{G}_i$. Obviously the $\mathcal{G}$ -action on the $\mathbf{G}_i$'s induces the $\mathcal{G}$ -action on $\mathbf{G}$. This concludes the description of the functor $G \rightsquigarrow G^\#(k_s)$ on objects.

Let us next describe this functor on morphisms. If $\phi: G \rightarrow H$ is a morphism of σ -étale σ -algebraic groups, we have an induced morphism $\phi^\#: G^\#(k_s) \rightarrow H^\#(k_s)$ of groups. Moreover, there is a commutative diagram

$$\begin{array}{ccc} G^\#(k_s) & \xrightarrow{\phi^\#} & H^\#(k_s) \\ \simeq \downarrow & & \downarrow \simeq \\ \mathrm{Spec}(k\{G\} \otimes_k k_s) & \xrightarrow{\alpha} & \mathrm{Spec}(k\{H\} \otimes_k k_s) \end{array}$$

where α is induced from the morphism $k\{H\} \otimes_k k_s \rightarrow k\{G\} \otimes_k k_s$ of σ -rings. Because α is continuous and commutes with the action of σ , we see that $\phi^\#$ is a morphism of profinite σ -groups. Clearly $\phi^\#$ also commutes with the $\mathcal{G}$ -action.

We have to show that

$$\mathrm{Hom}(G, H) \longrightarrow \mathrm{Hom}(G^\#(k_s), H^\#(k_s)), \quad \phi \mapsto \phi^\#$$

is a bijection. The set $\mathrm{Hom}(G, H)$ is in bijection with the morphisms of k - σ -Hopf algebras from $k\{H\} \rightarrow k\{G\}$. By Corollary 6.2.11 the set of k -Hopf algebra morphisms from $k\{H\}$ to $k\{G\}$ is in bijection with the set of continuous group morphisms from $G^\#(k_s)$ to $H^\#(k_s)$ that commute with the $\mathcal{G}$ -action. It therefore suffices to show that if $\varphi: G^\#(k_s) \rightarrow H^\#(k_s)$ is a morphism of profinite σ -groups that commutes with the $\mathcal{G}$ -action, then the corresponding morphism of k -Hopf algebras is a morphism of σ -rings. So let $\psi: k\{H\} \rightarrow k\{G\}$ be a

morphism of k -Hopf algebras such that the induced morphism $G^\#(k_s) \rightarrow H^\#(k_s)$ commutes with σ . This means that for every $g: k\{G\} \rightarrow k_s$ the outer rectangle in the following diagram

$$\begin{array}{ccccc} k\{H\} & \xrightarrow{\psi} & k\{G\} & \xrightarrow{\sigma(g)} & k_s \\ \sigma \downarrow & & \sigma \downarrow & & \sigma \downarrow \\ k\{H\} & \xrightarrow{\psi} & k\{G\} & \xrightarrow{g} & k_s \end{array}$$

commutes. Because also the right square commutes it follows that $g\sigma\psi = g\psi\sigma$ for any morphism $g: k\{G\} \rightarrow k_s$. By Lemma 6.2.10 this implies that $\sigma\psi = \psi\sigma$.

It remains to show that any profinite σ -group $\mathbf{G}$ of finite σ -type with a σ -continuous $\mathcal{G}$ -action comes from a σ -étale σ -algebraic group. Let $(\mathbf{G}_i)_{i \in \mathbb{N}}$ be a σ -projective system for $\mathbf{G}$ with a $\mathcal{G}$ -action as described before Definition 6.2.13. By Theorem 6.2.9 each $\mathbf{G}_i$ corresponds to an étale algebraic group $\mathcal{G}_i$ and the morphisms $\pi_i: \mathbf{G}_i \rightarrow \mathbf{G}_{i-1}$ correspond to morphisms of k -Hopf algebras $k[\mathcal{G}_{i-1}] \rightarrow k[\mathcal{G}_i]$. Let $k\{G\}$ denote the k -Hopf algebra that is the direct limit of this system. By assumption we have $\sigma_i(\tau(g)) = \sigma(\tau)(\sigma_i(g))$ for $\tau \in \mathcal{G}$, $g \in \mathbf{G}_i$ and $i \geq 1$. So the maps $\sigma_i: \mathbf{G}_i \rightarrow \mathbf{G}_{i-1}$ are in fact morphisms $\sigma_i: \mathbf{G}_i \rightarrow {}^\sigma\mathbf{G}_{i-1}$ in the category of finite groups with a continuous $\mathcal{G}$ -action. By Lemma 6.2.12 they correspond to morphisms of k -Hopf algebras $\bar{\sigma}_i: {}^\sigma(k[\mathcal{G}_{i-1}]) \rightarrow k[\mathcal{G}_i]$. The commutative diagram

$$\begin{array}{ccc} \mathbf{G}_i & \xrightarrow{\pi_i} & \mathbf{G}_{i-1} \\ \sigma_i \downarrow & & \downarrow \sigma_{i-1} \\ {}^\sigma\mathbf{G}_{i-1} & \xrightarrow{\pi_{i-1}} & {}^\sigma\mathbf{G}_{i-2} \end{array}$$

yields a commutative diagram

$$\begin{array}{ccc} k[\mathcal{G}_i] & \longleftarrow & k[\mathcal{G}_{i-1}] \\ \bar{\sigma}_i \uparrow & & \uparrow \bar{\sigma}_{i-1} \\ {}^\sigma(k[\mathcal{G}_{i-1}]) & \longleftarrow & {}^\sigma(k[\mathcal{G}_{i-2}]) \end{array}$$

Thus the limit of the $\bar{\sigma}_i$'s yields a morphism of k -Hopf algebras $\bar{\sigma}: {}^\sigma(k\{G\}) \rightarrow k\{G\}$. As in the proof of Theorem 2.4.10 this map corresponds to a map $\sigma: k\{G\} \rightarrow k\{G\}$ that turns $k\{G\}$ into a k - σ -Hopf algebra.

We need to show that $k\{G\}$ is finitely σ -generated over k . Indeed, we will show that $k\{G\}$ is σ -generated by the image of $k[\mathcal{G}_0]$. To do this it suffices to show that the morphism of k -algebras $k[\mathcal{G}_{i-1}] \otimes_k {}^\sigma(k[\mathcal{G}_{i-1}]) \rightarrow k[\mathcal{G}_i]$ is surjective. But it corresponds to the morphism $\mathbf{G}_i \rightarrow \mathbf{G}_{i-1} \times {}^\sigma\mathbf{G}_{i-1}$, $g \mapsto (\pi_i(g), \sigma_i(g))$. By the definition a σ -projective system $\ker(\pi_i) \cap \ker(\sigma_i) = 1$. So the latter map is injective. By Theorem 6.2.9 this implies that $k[\mathcal{G}_{i-1}] \otimes_k {}^\sigma(k[\mathcal{G}_{i-1}]) \rightarrow k[\mathcal{G}_i]$ is surjective.

So $k\{G\}$ is a finitely σ -generated k - σ -Hopf algebra and we can define G as the σ -algebraic group represented by $k\{G\}$. Because the $k[\mathcal{G}_i]$'s are étale k -algebras, it is clear that G is σ -étale.

Finally, a morphism $k\{G\} \rightarrow k_s$ of k -algebras, is a consistent family of morphisms of k -algebras $k[\mathcal{G}_i] \rightarrow k_s$. So $G^\#(k_s) = \varprojlim \mathbf{G}_i = \mathbf{G}$. $\square$

As an immediate corollary to Theorem 6.2.14 we obtain:

Corollary 6.2.15. *Let k be a separably algebraically closed σ -field. Then the category of σ -étale σ -algebraic groups is equivalent to the category of profinite σ -groups of finite σ -type.* $\square$

Definition 6.2.16. *A σ -algebraic group G is called finite if $k\{G\}$ is a finite dimensional k -vector space.*

We will study finite σ -algebraic groups in more detail in Subsection 6.3.2. Clearly a σ -algebraic group G is finite and σ -étale if and only if $k\{G\}$ is an étale k -algebra.

Let $\mathbf{G}$ be a finite σ -group, i.e., a finite group equipped with a group endomorphism $\sigma: \mathbf{G} \rightarrow \mathbf{G}$. A continuous action of $\mathcal{G}$ on $\mathbf{G}$ is called a *continuous σ -action* if

$$\sigma(\tau(g)) = \sigma(\tau)(\sigma(g))$$

for all $\tau \in \mathcal{G}$ and $g \in \mathbf{G}$. A morphism of finite σ -groups with a continuous σ -action of $\mathcal{G}$ is a morphism of groups that commutes with σ and the action of $\mathcal{G}$.

Corollary 6.2.17. *The category of finite σ -étale σ -algebraic groups is equivalent to the category of finite σ -groups with a continuous σ -action of $\mathcal{G}$.*

Proof. A σ -étale σ -algebraic group G is finite if and only if $G^\sharp(k_s)$ is a finite group. A finite σ -group equipped with the discrete topology is a profinite σ -group of finite σ -type. According to Theorem 6.2.14 it suffices to show that a σ -continuous action of $\mathcal{G}$ on a finite σ -group is equivalent to a continuous σ -action.

Given a continuous σ -action we can form the σ -projective system $\mathbf{G}_i = \mathbf{G}$ with π_i the identity map and $\sigma_i = \sigma$ to see that the action is σ -continuous. Conversely a σ -continuous action is a continuous σ -action because $\mathbf{G}$ is finite. $\square$

Corollary 6.2.18. *The category of strongly σ -étale σ -algebraic groups is equivalent to the category of finite σ -groups with a continuous σ -action of $\mathcal{G}$ where σ is an automorphism.*

Proof. Following Corollary 6.2.17 it suffices to show that a finite σ -étale σ -algebraic group G is strongly σ -étale, i.e., $k\{G\}$ is σ -separable, if and only if $\sigma: G^\sharp(k_s) \rightarrow G^\sharp(k_s)$ is an isomorphism.

If $k\{G\}$ is σ -separable, then $\sigma: k\{G\} \otimes_k k_s \rightarrow k\{G\} \otimes_k k_s$ is injective. Therefore the induced map on spectra $\text{Spec}(k\{G\} \otimes_k k_s) \rightarrow \text{Spec}(k\{G\} \otimes_k k_s)$ is surjective (cf. [Bou72, Prop. 16, Chapter II, §2.6, p.74]). Since these are finite sets we see that $\sigma: G^\sharp(k_s) \rightarrow G^\sharp(k_s)$ is bijective. Conversely, let $\mathbf{G}$ be a finite σ -group with a continuous σ -action of $\mathcal{G}$ such that $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ is bijective. Then $\sigma: \mathbf{G} \rightarrow {}^\sigma\mathbf{G}$ is an isomorphism of groups with a continuous $\mathcal{G}$ -action. So, using Lemma 6.2.12, we see that the corresponding map of k -algebras ${}^\sigma(k\{G\}) \rightarrow k\{G\}$ is an isomorphism. Thus $k\{G\}$ is σ -separable over k (Proposition 1.1.8). $\square$

Example 6.2.19. Let $k = \mathbb{Q}$, considered as a constant σ -field and let $\mathcal{G}$ 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 $\mathcal{G}$ is trivial and therefore a continuous σ -action is a continuous action that commutes with σ .

Let $\mathbf{G}$ be the group with three elements and let $\sigma: \mathbf{G} \rightarrow \mathbf{G}$, $g \mapsto g^2$ be the non-trivial endomorphism of $\mathbf{G}$. We define a continuous σ -action of $\mathcal{G}$ on $\mathbf{G}$ as follows: The field $\mathbb{Q}(e^{\pm \frac{2\pi i}{3}}) = \mathbb{Q}(\frac{i\sqrt{3}}{2})$ is a quadratic field extension of $\mathbb{Q}$. Let the non-trivial element of its Galois group act on $\mathbf{G}$ as the non-trivial endomorphism of $\mathbf{G}$ and let $\mathcal{G}$ act on $\mathbf{G}$ via

its restriction to $\mathbb{Q}(e^{\pm \frac{2\pi i}{3}})$. Clearly, the action of $\mathcal{G}$ is continuous and commutes with σ . Therefore $\mathbf{G}$ is a finite σ -group with a continuous σ -action. The corresponding σ -algebraic group is given by

$$G(R) = \{g \in R^\times \mid g^3 = 1, \sigma(g) = g^2\} \leq \mathbb{G}_m(R)$$

for any k - σ -algebra R .

The following example shows that a σ -continuous action need not be continuous.

Example 6.2.20. Let $\mathbb{F}_3$ denote the field with three elements and let $k = \mathbb{F}_3\langle\lambda\rangle$, i.e., k is the quotient field of the σ -polynomial ring $k\{\lambda\}$. Let G be the σ -closed subgroup of $\mathbb{G}_a$ given by

$$G(R) = \{g \in R \mid g^3 - \lambda g = 0\} \leq \mathbb{G}_a(R)$$

for any k - σ -algebra R . Because the polynomial $y^3 - \lambda y$ is separable, G is a σ -étale σ -algebraic group. Let k_s denote the separable algebraic closure of k and choose a root $\sqrt{\lambda} \in k_s$ of λ . We can define a morphism of k - σ -algebras $g: k\{G\} = k\{y\}/[y^3 - \lambda y] \rightarrow k_s$ by sending y to $\sqrt{\lambda}$. The image of g is $\mathbb{F}_3\langle\sqrt{\lambda}\rangle$ and this is an infinite field extension of $k = \mathbb{F}_3\langle\lambda\rangle$. As in the proof of Theorem 6.2.14 let $\mathbf{G} = G^\#(k_s)$ be the profinite σ -group of finite σ -type with a σ -continuous action of the Galois group $\mathcal{G}$ of k_s over k . Because $g(k\{G\})$ is an infinite field extension of k , the orbit of g under the action of $\mathcal{G}$ is infinite. Thus the stabilizer of g is not an open subgroup of $\mathcal{G}$ and the action of $\mathcal{G}$ on $\mathbf{G}$ is not continuous.

6.3 Infinitesimal and finite difference algebraic groups

Infinitesimal algebraic groups play an important role in the theory of algebraic groups in positive characteristic. A possible analogy for difference algebraic groups in positive characteristic is to consider difference algebraic groups where the maximal ideal $\mathfrak{m}_G$ corresponding to the identity element is nilpotent. However, there also is another analogy which applies in any characteristic. Namely, we can think of the endomorphism σ as being analogous to the Frobenius endomorphism. So $\mathfrak{m}_G$ is σ -nilpotent in the sense that $\sigma^n(\mathfrak{m}_G) = 0$ for some $n \in \mathbb{N}$. Also a combination of the two ideas just outlined is possible.

Definition 6.3.1. A σ -algebraic group G is called

- infinitesimal if $G(R) = 1$ for every reduced k - σ -algebra R .
- σ -infinitesimal if $G(R) = 1$ for every σ -reduced k - σ -algebra R .
- semiinfinitesimal if $G(R) = 1$ for every reduced and σ -reduced k - σ -algebra R .

Clearly an infinitesimal σ -algebraic group is semiinfinitesimal. Also a σ -infinitesimal σ -algebraic group is semiinfinitesimal. Semiinfinitesimal σ -algebraic groups are important for us because they naturally appear in the structure theorem of finite σ -algebraic groups (Theorem 6.3.9). While σ -infinitesimal σ -algebraic groups naturally occur in Babbitt's decomposition for σ -étale σ -algebraic groups (Theorem 6.4.10).

6.3.1 Semiinfinitesimal difference algebraic groups

Lemma 6.3.2. *The following four conditions on a σ -algebraic group G are equivalent.*

- (i) G is semiinfinitesimal.
- (ii) $G_{\sigma\text{-red,red}} = 1$.
- (iii) The radical of the reflexive closure of the zero ideal of $k\{G\}$ equals $\mathfrak{m}_G$.
- (iv) For every element $f \in \mathfrak{m}_G$ there exist integers $n \geq 0$, $m \geq 1$ such that $\sigma^n(f)^m = 0$.

Proof. The equivalence of (ii), (iii) and (iv) follows immediately from the definitions. Let us show that (i) implies (iii). Let $\mathfrak{a}$ denote the reflexive closure of the radical of the zero ideal of $k\{G\}$. Then $R = k\{G\}/\mathfrak{a}$ is reduced and σ -reduced. As $G(R) = 1$, the canonical map $k\{G\} \rightarrow R$ factors through the counit $\varepsilon: k\{G\} \rightarrow k$. This means that $\mathfrak{a} = \mathfrak{m}_G$.

Finally, we show that (iv) implies (i). Let R be a reduced and σ -reduced k - σ -algebra. Let $g \in G(R) = \text{Hom}(k\{G\}, R)$ and let $f \in \mathfrak{m}_G$. By (iv) there exist integers $n \geq 0$, $m \geq 1$ such that $\sigma^n(f)^m = 0$. So $\sigma^n(g(f))^m = 0$. Because R is reduced and σ -reduced this implies $g(f) = 0$. Thus $g(\mathfrak{m}_G) = 0$ and g factors through the counit, i.e., $g = 1$. $\square$

Lemma 6.3.3. *A semiinfinitesimal σ -algebraic group is σ -connected and has σ -dimension zero.*

Proof. Let G be a semiinfinitesimal σ -algebraic group. To show that G is σ -connected it suffices to show that $k\{G\}$ contains no non-trivial constant idempotent element (Corollary 4.2.3). Suppose $e \in k\{G\}$ is a non-trivial constant idempotent. Then also $e' := 1 - e$ is a non-trivial constant idempotent. Because $ee' = 0$, the counit $\varepsilon: k\{G\} \rightarrow k$ must satisfy $\varepsilon(e) = 0$ or $\varepsilon(e') = 0$. Without loss of generality we may assume that $\varepsilon(e) = 0$. So $e \in \mathfrak{m}_G$, but then $\sigma^n(e)^m = 0$ for some $n \geq 0$ and $m \geq 1$ since G is semiinfinitesimal (Lemma 6.3.2). This contradicts the assumption that e is a constant idempotent.

To show that G has σ -dimension zero, we may assume that k is perfect and inverse (Lemma 2.2.19). Then $\sigma\text{-dim}(G) = \sigma\text{-dim}(G_{\sigma\text{-red,red}})$ by Lemma 4.1.22. Because $G_{\sigma\text{-red,red}} = 1$ by Lemma 6.3.2, we see that $\sigma\text{-dim}(G) = 0$. $\square$

The following example shows that a semiinfinitesimal σ -algebraic group need not be connected.

Example 6.3.4. Let G be the σ -algebraic group given by

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

for any k - σ -algebra R . Clearly G is σ -infinitesimal. If the characteristic of k is not equal to 2, then $k\{G\} = k \times k$. So G is not connected.

The following example shows that a semiinfinitesimal σ -algebraic group may have positive order.

Example 6.3.5. For $n \geq 1$ let G be the σ -algebraic group given by

$$G(R) = \{g \in R \mid \sigma^n(g) = 0\} \leq \mathbb{G}_a(R)$$

for any k - σ -algebra R . Then G is σ -infinitesimal and has order n .

The following example shows that a semiinfinitesimal σ -algebraic group may have limit degree greater than one.

Example 6.3.6. Let G be the σ -algebraic group given by

$$G(R) = \{g \in R^\times \mid g^2 = 1\} \leq \mathbb{G}_m(R)$$

for any k - σ -algebra R . Assume that the characteristic of k is equal to 2. Then $g^2 - 1 = (g - 1)^2$ for any $g \in R$. Thus G is infinitesimal. According to Example 2.4.6 we have $\text{ld}(G) = 2$.

6.3.2 Finite difference algebraic groups

Recall that a σ -algebraic group G is called finite if $k\{G\}$ is a finite dimensional k -vector space. In this subsection we prove a structure theorem for finite σ -algebraic groups. We show that over an inversive and perfect σ -field a finite σ -algebraic group is a semidirect product of a semiinfinitesimal σ -algebraic group and a strongly σ -étale σ -algebraic group. We also prove a similar result for finite σ -étale σ -algebraic groups. Over an inversive base σ -field every finite σ -étale σ -algebraic group is as a semidirect product of a σ -infinitesimal σ -algebraic group and a strongly σ -étale σ -algebraic group.

Clearly quotients and σ -closed subgroups of finite σ -algebraic groups are finite. A finite connected algebraic group is infinitesimal. The following result can be seen as a difference analog of this fact.

Lemma 6.3.7. *A finite σ -connected σ -algebraic group is semiinfinitesimal.*

Proof. Let G be a finite σ -connected σ -algebraic group. Then $\text{Spec}(k\{G\})$ is a finite discrete topological space. Set

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

Then Z and the complement of Z are σ -closed subsets of $\text{Spec}(k\{G\})$. Because $\text{Spec}(k\{G\})$ is σ -connected and $\mathfrak{m}_G \in Z$ we must have $Z = \text{Spec}(k\{G\})$. 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 $k\{G\}$. Since the nilradical is the intersection of all prime ideals, it follows that $\sigma^{-n}(\sqrt{0}) = \mathfrak{m}_G$. So $\sqrt{0}^* = \mathfrak{m}_G$. This shows that G is semiinfinitesimal (Lemma 6.3.2). $\square$

Corollary 6.3.8. *A finite σ -algebraic group is σ -connected if and only if it is semiinfinitesimal.*

Proof. Clear from Lemma 6.3.7 and Lemma 6.3.3. $\square$

Theorem 6.3.9. *Let G be a finite σ -algebraic group. If k is perfect and inversive, then G is the semidirect product of a semiinfinitesimal σ -algebraic group and a strongly σ -étale σ -algebraic group. More precisely,*

$$G \simeq G^{\sigma o} \rtimes \pi_0^\sigma(G)$$

with $G^{\sigma o}$ semiinfinitesimal and $\pi_0^\sigma(G)$ strongly σ -étale.

Proof. We know from Lemma 6.3.7 that $G^{\sigma\sigma}$ is semiinfinite and clearly $\pi_0^\sigma(G)$ is strongly σ -étale. Considering the exact sequence

$$1 \rightarrow G^{\sigma\sigma} \rightarrow G \rightarrow \pi_0^\sigma(G) \rightarrow 1$$

we see from Lemma 3.3.17, that it suffices to find a σ -closed subgroup H of G such that $G \rightarrow \pi_0^\sigma(G)$ induces an isomorphism $H \rightarrow \pi_0^\sigma(G)$. Because k is perfect and in-
versive $G_{\sigma\text{-red},\text{red}}$, is a subgroup of G (Corollary 2.5.7). The k - σ -algebra $k\{G_{\sigma\text{-red},\text{red}}\}$ is reduced and σ -reduced. Because k is perfect and $k\{G_{\sigma\text{-red},\text{red}}\}$ is reduced and of finite degree over k , we know from [Bou90, Theorem 4, Chapter V, §6, No. 7, A.V.34] that $k\{G_{\sigma\text{-red},\text{red}}\}$ is an étale k -algebra. Similarly, because $k\{G_{\sigma\text{-red},\text{red}}\}$ is σ -reduced and k is in-
versive, it follows from Proposition 1.1.8 that $k\{G_{\sigma\text{-red},\text{red}}\}$ is σ -separable. So $k\{G_{\sigma\text{-red},\text{red}}\}$ is strongly σ -étale and $\pi_0^\sigma(G_{\sigma\text{-red},\text{red}}) = G_{\sigma\text{-red},\text{red}}$. By Theorem 4.2.58 the inclusion $G_{\sigma\text{-red},\text{red}} \hookrightarrow G$ induces an isomorphism $G_{\sigma\text{-red},\text{red}} = \pi_0^\sigma(G_{\sigma\text{-red},\text{red}}) \rightarrow \pi_0^\sigma(G)$. Thus $G \rightarrow \pi_0^\sigma(G)$ restricts to an isomorphism $G_{\sigma\text{-red},\text{red}} \simeq \pi_0^\sigma(G)$. $\square$

Example 6.3.10. Assume that k has positive characteristic and let G be a Frobenius algebraic group as in Example 2.1.14, with corresponding algebraic group $\mathcal{G}$. Assume that $\mathcal{G}$ is finite and that k is perfect (and therefore in-
versive). Then the semidirect product decomposition $G \simeq G^{\sigma\sigma} \rtimes \pi_0^\sigma(G)$ of Theorem 6.3.9 corresponds to the semidirect product decomposition $\mathcal{G} \simeq \mathcal{G}^\sigma \rtimes \pi_0(\mathcal{G})$. (See [Wat79, Theorem 6.8, p. 52].)

The example in [Wat79, Exercise 10, Chapter 6, p. 53] shows that Theorem 6.3.9 is not valid without restrictions on the base σ -field k .

Our next goal is to prove a statement similar to Theorem 6.3.9 for finite σ -étale σ -algebraic groups. For this we need the following lemma:

Lemma 6.3.11. *A reduced finite σ -connected σ -algebraic group is σ -infinitesimal.*

Proof. Let G be a reduced finite σ -connected σ -étale σ -algebraic group. As in the proof of Lemma 6.3.7 we see that there exists $n \geq 1$ such that $\sigma^{-n}(\mathfrak{p}) = \mathfrak{m}_G$ for every prime ideal $\mathfrak{p}$ of $k\{G\}$. Because G is reduced, this implies $\sigma^{-n}(0) = \mathfrak{m}_G$. So G is σ -infinitesimal. $\square$

The following example shows that Lemma 6.3.11 does not hold without the assumption that G is reduced.

Example 6.3.12. Let k be a σ -field of characteristic 2 and let G be the σ -algebraic group given by

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

for any k - σ -algebra R . Then $k\{G\} = k[y]/(y^2 - 1) = k[y]/((y - 1)^2)$. So G is finite and connected (in particular, G is σ -connected). The image of $y - 1$ lies in $\mathfrak{m}_G$ and is fixed by σ . So G is not σ -infinitesimal.

Corollary 6.3.13. *A finite reduced σ -algebraic group is σ -connected if and only if it is σ -infinitesimal.*

Proof. Clear from Lemma 6.3.11 and Lemma 6.3.3. $\square$

Theorem 6.3.14. *Let G be a finite σ -étale σ -algebraic group. If k is in-
versive, then G is the semidirect product of a σ -infinitesimal σ -algebraic group and a strongly σ -étale σ -algebraic group. More precisely,*

$$G \simeq G^{\sigma\sigma} \rtimes \pi_0^\sigma(G)$$

with $G^{\sigma\sigma}$ σ -infinitesimal and $\pi_0^\sigma(G)$ strongly σ -étale.

Proof. As $G^{\sigma\sigma}$ is σ -étale it is reduced. Therefore $G^{\sigma\sigma}$ is σ -infinitesimal by Lemma 6.3.11. Because k is inductive, $G_{\sigma\text{-red}}$ is a subgroup of G (Corollary 2.5.7). As in the proof of Theorem 6.3.9 it suffices to show that $G \rightarrow \pi_0^\sigma(G)$ induces an isomorphism $G_{\sigma\text{-red}} \simeq \pi_0^\sigma(G)$.

Because k is inductive it follows from Lemma 4.2.54 that $(G_{\sigma\text{-red}})_K = (G_K)_{\sigma\text{-red}}$ for every σ -field extension K of k . Replacing k with a perfect and inductive σ -field extension of k (cf. Lemma 1.1.6) we may therefore assume that k is perfect.

Because k is inductive and $k\{G_{\sigma\text{-red}}\}$ σ -reduced, it follows from Proposition 1.1.8 that $k\{G_{\sigma\text{-red}}\}$ is σ -separable. Because $G_{\sigma\text{-red}}$ is σ -étale (Lemma 6.1.5) we see that $G_{\sigma\text{-red}}$ is strongly σ -étale. Moreover $G_{\sigma\text{-red}} = G_{\sigma\text{-red},\text{red}}$. So $G_{\sigma\text{-red}} = \pi_0^\sigma(G_{\sigma\text{-red}}) \simeq \pi_0^\sigma(G)$ by Theorem 4.2.58. $\square$

Let us illustrate Theorem 6.3.14 in the case that G comes from a finite group.

Example 6.3.15. Let $\mathbf{G}$ be a finite group and $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ an endomorphism. Let G be the σ -algebraic group associated to this data as in Example 2.1.15. We have seen in Example 2.5.9 that $G_{\sigma\text{-red}}$ corresponds to the subgroup $\mathbf{H} = \bigcap_{n \in \mathbb{N}} \sigma^n(\mathbf{G})$ of $\mathbf{G}$. And in Example 4.2.51 we have seen that $G^{\sigma\sigma}$ corresponds to the subgroup

$$\mathbf{N} = \{g \in \mathbf{G} \mid \exists n \in \mathbb{N} : \sigma^n(g) = 1\}$$

of $\mathbf{G}$. So the semidirect product composition of Theorem 6.3.14 corresponds to the semidirect product composition $\mathbf{G} = \mathbf{N} \rtimes \mathbf{H}$ of $\mathbf{G}$.

6.3.3 Difference infinitesimal difference algebraic groups

Proposition 6.3.16. *The following conditions on a σ -algebraic group G are equivalent:*

- (i) G is σ -infinitesimal.
- (ii) $G_{\sigma\text{-red}} = 1$.
- (iii) *The reflexive closure of the zero ideal of $k\{G\}$ equals $\mathfrak{m}_G$.*
- (iv) *For every $f \in \mathfrak{m}_G$ there exists an integer $n \geq 1$ such that $\sigma^n(f) = 0$.*
- (v) *There exists an integer $n \geq 1$ such that $\sigma^n(\mathfrak{m}_G) = 0$.*

Proof. The equivalence of (ii), (iii) and (iv) is tautological. Let us show that (i) implies (iii). Let $\mathfrak{a}$ denote the reflexive closure of the zero ideal of $k\{G\}$. Since $R = k\{G\}/\mathfrak{a}$ is σ -reduced, it follows from (i) that the canonical map $k\{G\} \rightarrow k\{G\}/\mathfrak{a}$ factors through the counit $k\{G\} \rightarrow k$ whose kernel is $\mathfrak{m}_G$. Thus $\mathfrak{a} = \mathfrak{m}_G$.

Let us next show that (iv) implies (i). Let $f \in k\{G\}$ with $\sigma^n(f) = 0$. If R is σ -reduced and $g \in G(R)$, i.e., $g: k\{G\} \rightarrow R$ is a morphism of k - σ -algebras, then $g(f) = 0$ since $\sigma^n(g(f)) = g(\sigma^n(f)) = 0$. By (iv), $g(\mathfrak{m}_G) = 0$ so that the morphism $g: k\{G\} \rightarrow R$ factors through the counit $k\{G\} \rightarrow k\{G\}/\mathfrak{m}_G = k$, i.e., $g = 1$.

Finally we show that (iv) implies (v). By Theorem 2.3.1, there exist $f_1, \dots, f_m \in \mathfrak{m}_G$ such that $\mathfrak{m}_G = [f_1, \dots, f_m]$. For every $i = 1, \dots, m$ there exists an integer $n_i \geq 1$ such that $\sigma^{n_i}(f_i) = 0$. For the maximum n of the n_i 's we have $\sigma^n(\mathfrak{m}_G) = 0$. $\square$

Example 6.3.17. Let $\mathbf{G}$ be a finite group and $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ an endomorphism. As in Example 2.1.15 let G be the σ -algebraic group associated to this data. Then it follows from Corollary 6.3.13 and Example 4.2.51 that G is σ -infinitesimal if and only if some power of $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ is the trivial endomorphism.

Example 6.3.18. Assume that k has positive characteristic. Let $\mathcal{G}$ be an algebraic group and let G be the associated Frobenius algebraic group as in Example 2.1.14. Then it follows from Proposition 6.3.16 that G is σ -infinitesimal if and only if $\mathcal{G}$ is an infinitesimal algebraic group.

Lemma 6.3.19. *Let G be a σ -algebraic group and K a σ -field extension of k . Then G is σ -infinitesimal if and only if G_K is σ -infinitesimal.*

Proof. This is clear from Proposition 6.3.16 since $\mathfrak{m}_{G_K} = \mathfrak{m}_G \otimes_k K$ and $\sigma^n(\mathfrak{m}_G) = 0$ if and only if $\sigma^n(\mathfrak{m}_G \otimes_k K) = 0$. $\square$

Theorem 6.3.20. *Let G be a σ -infinitesimal σ -algebraic group. Then $\sigma\text{-dim}(G) = 0$, $\text{ld}(G) = 1$ and G is σ -connected.*

Proof. We already know from Lemma 6.3.3 that G is σ -connected and that $\sigma\text{-dim}(G) = 0$. So we only have to show that $\text{ld}(G) = 1$. Assume that $f_1, \dots, f_n$ σ -generate $k\{G\}$ over k . For $i = 1, \dots, n$ let $\lambda_i \in k$ denote the image of f_i under the counit $k\{G\} \rightarrow k$. Then $\mathfrak{m}_G = [f_1 - \lambda_1, \dots, f_n - \lambda_n]$. Since G is σ -infinitesimal, there exists an integer $m \geq 1$ such that $\sigma^m(f_i - \lambda_i) = 0$ for $i = 1, \dots, n$. So $\sigma^j(f_i) \in k$ for $j \geq m$. It follows that the $\sigma^j(f_i)$, ($1 \leq i \leq n$, $0 \leq j \leq m$) generate $k\{G\}$ as a k -algebra. Thus G has limit degree one (Proposition 2.4.8). $\square$

In particular, a σ -infinitesimal σ -algebraic group has only finitely many components. We have already seen in Example 6.3.4 that a σ -infinitesimal σ -algebraic group need not be connected.

For later use we record:

Lemma 6.3.21. *Let $\phi: G \rightarrow H$ be a morphism of σ -algebraic groups and $H' \leq H$. If H' and $\ker(\phi)$ are σ -infinitesimal, then $\phi^{-1}(H')$ is σ -infinitesimal.*

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

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

$\square$

6.3.4 Difference Frobenius kernels

Difference Frobenius kernels are certain σ -infinitesimal σ -algebraic groups which are naturally associated to any σ -algebraic group. Frobenius kernels play an important role in the representation theory of algebraic groups in positive characteristic. (See e.g., [Jan87, Section 9, Part I].) In this subsection we introduce a σ -analog of Frobenius kernels by replacing the Frobenius endomorphism with an arbitrary endomorphism σ . We are mainly interested in σ -Frobenius kernels as a tool for the proof of Babbitt's decomposition for σ -étale σ -algebraic groups (Theorem 6.4.10).

Starting from Section 2.2 we have made it a general assumption that the base σ -ring k is a σ -field. However, in the beginning of this subsection until Definition 6.3.23 we allow k to be an arbitrary σ -ring¹.

¹This generality is needed for the proof of Proposition 6.3.32

Let R be a k - σ -algebra. For $r \in \mathbb{N}$ the map $\sigma^r: k \rightarrow k$, $\lambda \mapsto \sigma^r(\lambda)$ is a morphism of difference rings. We denote by

$$\sigma^r R$$

the k - σ -algebra obtained from R by restriction of scalars via $\sigma^r: k \rightarrow k$. That is, $\sigma^r R$ equals R as a difference ring, but the k -algebra structure map is $k \rightarrow \sigma^r R$, $\lambda \mapsto \sigma^r(\lambda)$. Note that $\sigma^r: R \rightarrow \sigma^r R$, $a \mapsto \sigma^r(a)$ is a morphism of k - σ -algebras.

For the sake of brevity, let us call a functor from k - σ -Alg to Sets a k - σ -functor. Similarly to Subsection 1.2.4, let us denote the k - σ -functor obtained from a k - σ -functor X by extension of scalars via $\sigma^r: k \rightarrow k$ by

$$\sigma^r X.$$

That is, for a k - σ -algebra R we have $\sigma^r X(R) = X(\sigma^r R)$. If X is a σ -variety (over k), then $\sigma^r X$ is a σ -variety (over k) and $k\{\sigma^r X\} = \sigma^r(k\{G\}) = k\{G\} \otimes_k k$ (cf. Subsection 1.2.3).

We define a morphism of k - σ -functors

$$F_X^r: X \rightarrow \sigma^r X$$

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

$$\begin{array}{ccc} R & \xrightarrow{\sigma^r} & \sigma^r R \\ \psi \downarrow & & \downarrow \psi \\ R' & \xrightarrow{\sigma^r} & \sigma^r R' \end{array}$$

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

$$\begin{array}{ccc} X(R) & \xrightarrow{(F_X^r)_R} & \sigma^r X(R) \\ X(\psi) \downarrow & & \downarrow \sigma^r X(\psi) \\ X(R') & \xrightarrow{(F_X^r)_{R'}} & \sigma^r X(R') \end{array}$$

commutes, so that F_X^r is indeed natural in R , as required. We write

$$F_X$$

for F_X^1 .

If $\phi: X \rightarrow Y$ is a morphism of k - σ -functors, then

$$\begin{array}{ccc} X(R) & \xrightarrow{\phi_R} & Y(R) \\ X(\sigma^r) \downarrow & & \downarrow Y(\sigma^r) \\ X(\sigma^r R) & \xrightarrow{\phi_{(\sigma^r R)}} & Y(\sigma^r R) \end{array}$$

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

$$\begin{array}{ccc} X & \xrightarrow{\phi} & Y \\ F_X^r \downarrow & & \downarrow F_Y^r \\ \sigma^r X & \xrightarrow{\sigma^r \phi} & \sigma^r Y \end{array}$$

of k - σ -functors.

If X is a σ -variety, the dual morphism $(F_X^r)^*: \sigma^r(k\{X\}) \rightarrow k\{X\}$ is the image of $\text{id} \in X(k\{X\}) = \text{Hom}(k\{X\}, k\{X\})$ in

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

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

$$(F_X^r)^*: \sigma^r(k\{X\}) \rightarrow k\{X\}, \quad f \otimes \lambda \mapsto \sigma^r(f)\lambda. \quad (6.4)$$

Note that if G is a σ -algebraic group. Then $F_G^r: G \rightarrow \sigma^r G$ is a morphism of σ -algebraic groups.

From now on we again assume that the base σ -ring k is a σ -field.

Example 6.3.22. Let G be a σ -algebraic group. By Theorem 2.1.17 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 GL_n (considered as σ -algebraic group) given by

$$\phi_R: \text{GL}_n(R) \rightarrow \text{GL}_n(R), \quad g \mapsto \sigma^r(g)$$

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

$$\phi^*: k\{x_{ij}, \frac{1}{\det(x)}\} \rightarrow k\{x_{ij}, \frac{1}{\det(x)}\}, \quad x_{ij} \mapsto \sigma^r(x_{ij}).$$

It follows that the dual map of $\phi: G \rightarrow \sigma^r G$ agrees with the dual map of F_G^r given in (6.4). 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 .)

We would like to understand when the σ -Frobenius map $F_G: G \rightarrow \sigma^r G$ is surjective. The following definition contains the answer.

Definition 6.3.23. A σ -algebraic group G is called *absolutely σ -reduced* if G_K is σ -reduced for every σ -field extension $K|k$.

Thus 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 6.3.24. Let k be a σ -field such that there exists a $\lambda \in k$ that is transcendental over $\sigma(k)$. (In particular, k is not inversive. For example, we may choose $k = \mathbb{Q}\langle y \rangle$ and $\lambda = y$.) Let G be the σ -closed subgroup of the additive group given by

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

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 we can find $\mu \in k^*$ such that $\sigma(\mu) = \lambda$ and then $\sigma(y) + \mu y$ lies in the kernel of σ on $k^*\{G_{k^*}\} = k^*[y, \sigma(y)]$.

In Corollary 6.4.2 we will show that an algebraic group, when considered as a σ -algebraic group is absolutely σ -reduced.

Lemma 6.3.25. *Let G be a σ -algebraic group. The following statements are equivalent:*

- (i) $F_G: G \rightarrow {}^\sigma G$ is surjective.
- (ii) $F_G^r: G \rightarrow {}^{\sigma^r} G$ is surjective for every $r \in \mathbb{N}$.
- (iii) G is absolutely σ -reduced.

Proof. By Proposition 1.1.8 the k - σ -algebra $k\{G\}$ is σ -separable over k if and only if $(F_G)^*: {}^\sigma(k\{G\}) \rightarrow k\{G\}$ is injective. Thus (i) and (iii) are equivalent. To see that (i) implies (ii), note that if $k\{G\}$ is σ -separable over k , then $k\{G\}$ is also σ^r -separable over k by Proposition 1.1.8. $\square$

Definition 6.3.26. *Let G be a σ -algebraic group and $r \in \mathbb{N}$. The kernel $G_{(r)}$ of the morphism $F_G^r: G \rightarrow {}^{\sigma^r} G$ is called the r -th σ -Frobenius kernel of G .*

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

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

Moreover, from equation (6.4) we see that

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

and

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

Example 6.3.27. The r -th σ -Frobenius kernel of GL_n is given by

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

for any k - σ -algebra R . Here I_n denotes the n by n identity matrix.

Example 6.3.28. The r -th σ -Frobenius kernel of $\mathbb{G}_a$ is given by

$$(\mathbb{G}_a)_{(r)}(R) = \{g \in R \mid \sigma^r(g) = 0\} \leq \mathbb{G}_a(R)$$

for any k - σ -algebra R .

Example 6.3.29. Let G be the σ -closed subgroup of GL_n given by

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

for any k - σ -algebra R . Then it is clear from Example 6.3.22 that all the σ -Frobenius kernels of G are trivial.

Example 6.3.30. Let $\mathbf{G}$ be a finite group and $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ an endomorphism. If G is the σ -algebraic group determined by this data as in Example 2.1.15, then $(\sigma^r(\mathfrak{m}_G)) = (e_g \mid \sigma^r(g) \neq 1) \subset k\{G\}$. Thus the r -th σ -Frobenius kernel of G corresponds to the kernel of $\sigma^r: \mathbf{G} \rightarrow \mathbf{G}$. In particular, if $\sigma: \mathbf{G} \rightarrow \mathbf{G}$ is an automorphism, all the σ -Frobenius kernels of G are trivial.

Example 6.3.31. Let G be a Frobenius algebraic group as in Example 2.1.14 (with $q = p$) and let $\mathcal{G}$ be the corresponding algebraic group. Then the σ -Frobenius kernels of G correspond to the Frobenius kernels of $\mathcal{G}$ (in the sense that their defining ideals are equal).

Proposition 6.3.32. *Let G be a σ -algebraic group. The σ -Frobenius kernels are characteristic subgroups of G .*

Proof. Let R be a k - σ -algebra and ϕ an automorphism of G_R . According to Definition 2.1.5 we have to show that ϕ induces an automorphism of $(G_{(r)})_R$. But $(G_{(r)})_R = (G_R)_{(r)}$. Therefore it suffices to show that every automorphism ϕ of a σ -algebraic group G over a σ -ring R induces an automorphism of $G_{(r)}$. But this is clear from the commutative diagram

$$\begin{array}{ccc} G & \xrightarrow{F_G^r} & \sigma^r G \\ \phi \downarrow & & \downarrow \sigma^r \phi \\ G & \xrightarrow{F_G^r} & \sigma^r G \end{array}$$

□

As a Corollary to Lemma 6.3.25 we obtain:

Corollary 6.3.33. *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 6.3.25 (and Theorem 5.2.1). □

Lemma 6.3.34. *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 $G_{(r)}$.*

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 (Proposition 6.3.16).

If $H \leq G$ is σ -infinitesimal. Then $\sigma^r(\mathfrak{m}_G) \subset \mathbb{I}(H)$ for some $r \in \mathbb{N}$. So $\mathbb{I}(G_{(r)}) = (\sigma^r(\mathfrak{m}_G)) \subset \mathbb{I}(H)$ and consequently $H \leq G_{(r)}$. □

Corollary 6.3.35. *Let G be a σ -algebraic group. Then G is σ -infinitesimal if and only if $G = G_{(r)}$ for $r \gg 0$.*

Proof. If G is σ -infinitesimal, there exists an integer $n \geq 1$ such that $\sigma^n(\mathfrak{m}_G) = 0$. Then $\mathbb{I}(G_{(r)}) = (\sigma^r(\mathfrak{m}_G)) = 0$ and therefore $G = G_{(r)}$ for $r \geq n$.

The converse statement follows from Lemma 6.3.34. □

For later use we record:

Lemma 6.3.36. *Let $N \trianglelefteq H \leq G$ be σ -algebraic groups. 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 3.2.7 we obtain a morphism

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

with kernel $(F_G^r)^{-1}(\sigma^r N)$. By Corollary 3.2.4 this yields an injective morphism

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

Since H/N is absolutely σ -reduced, $F_{H/N}^r$ is surjective (Lemma 6.3.25). Because

$$\begin{array}{ccc} H/N & \xrightarrow{\quad} & (F_G^r)^{-1}(\sigma^r H) / (F_G^r)^{-1}(\sigma^r N) \\ & \searrow F_{H/N}^r & \swarrow \phi \\ & \sigma^r(H/N) & \end{array}$$

commutes, this implies that ϕ is surjective. So ϕ is injective and surjective and therefore an isomorphism (Corollary 3.3.10). $\square$

6.4 Babbitt's decomposition for σ -étale difference algebraic groups

Babbitt's decomposition theorem is a very useful structure theorem for finitely σ -generated extensions of σ -fields such that the underlying field extension is Galois. (See [Lev08, Theorem 5.4.13, p. 336] and [Bab62]).

In this section we prove an analogous decomposition theorem (Theorem 6.4.10) for σ -étale σ -algebraic groups. The seemingly surprising fact that σ -algebraic groups have structural properties similar to σ -field extensions is to some extent explained by the σ -Galois theory of linear differential equations. (See [DVHW14].)

However, even if it was known that every σ -étale σ -algebraic group is the σ -Galois group of some σ -Picard-Vessiot extension (see [DVHW14]) it appears to be impossible to derive Babbitt's decomposition theorem for σ -algebraic groups from Babbitt's decomposition theorem for σ -field extensions. Our theorem is in some sense more general because we allow an arbitrary σ -field as the base σ -field. In a certain sense Babbitt's decomposition theorem for σ -field extensions only corresponds to the case of an algebraically closed base σ -field. Also, the σ -Galois theory of linear differential equations has so far only been developed in characteristic zero. Our Babbitt's decomposition theorem for σ -algebraic groups and its proof is also more general in another respect: In Babbitt's decomposition theorem for σ -fields it is assumed that the smaller σ -field is inversive and this property is used in a crucial way in several steps of the original proof. Via the σ -Galois theory the assumption that the smaller σ -field is inversive would imply that the corresponding σ -algebraic group is absolutely σ -reduced (see [DVHW14, Prop. 4.3]). But we do not need to make this assumption for Babbitt's decomposition theorem for σ -algebraic groups. In fact, in the course of proving Babbitt's decomposition theorem for σ -algebraic groups, the author was able to find a new proof of Babbitt's decomposition theorem for σ -field extensions that does not require the assumption that the smaller σ -field is inversive. This improved version of Babbitt's decomposition theorem for σ -field extensions will be published elsewhere.

For the proof of Babbitt's decomposition theorem for σ -algebraic groups we require some preparatory results and definitions.

Lemma 6.4.1. *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 $[\sigma]_k T$ is σ -reduced. And for this it suffices to show that $\sigma: T[i] \rightarrow T[i+1]$ is injective for every $i \geq 0$. But $\sigma: T[i] \rightarrow {}^\sigma(T[i]) \rightarrow T[i+1]$ is the composition of two injective maps. $\square$

From Lemma 6.4.1 we immediately obtain:

Corollary 6.4.2. *Let $\mathcal{G}$ be an algebraic group. Then $[\sigma]_k \mathcal{G}$ is an absolutely σ -reduced σ -algebraic group.*

Lemma 6.4.3. *Let G be a benign σ -algebraic group and K a σ -field extension of k . Then G_K is a benign σ -algebraic group (over K).*

Proof. If $\mathcal{G}$ is an étale algebraic group such that $G = [\sigma]_k \mathcal{G}$, then $\mathcal{G}_K$ is an étale algebraic group (over K) and therefore $G_K = [\sigma]_K \mathcal{G}_K$ is benign. $\square$

The following proposition is an important step in the proof of Babbitt's decomposition for σ -étale σ -algebraic groups. Roughly speaking, it shows that in a subnormal series we can get rid of the top σ -infinitesimal quotient.

Proposition 6.4.4. *Let G be a σ -algebraic group with a subnormal series*

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

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

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

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

Proof. Since G/G_1 is σ -infinitesimal, there exists an $r \in \mathbb{N}$ such that $(G/G_1)_{(r)} = G/G_1$ (Corollary 6.3.35). It is then clear from the commutative diagram

$$\begin{array}{ccc} G & \twoheadrightarrow & G/G_1 \\ F_G^r \downarrow & & \downarrow F_{G/G_1}^r \\ \sigma^r G & \twoheadrightarrow & \sigma^r(G/G_1) \end{array}$$

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

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

(So $H_0 = G$.) Because benign σ -algebraic groups are absolutely σ -reduced (Corollary 6.4.2) it follows from Lemma 6.3.36 that $H_i/H_{i+1} \simeq \sigma^r(G_{i-1}/G_i)$ is benign for $i = 0, \dots, n$ (Lemma 6.4.3). Finally, because $\sigma^r G_{n+1}$ is σ -infinitesimal (Lemma 6.3.19) the σ -algebraic group $H_n = (F_G^r)^{-1}(\sigma^r G_{n+1})$ is σ -infinitesimal by Lemma 6.3.21. $\square$

Let G be a σ -étale σ -algebraic group. Let $\mathcal{G}$ be an étale algebraic group and $\phi: G \rightarrow \mathcal{G}$ a morphism of σ -algebraic groups. Then $\phi(G) \leq \mathcal{G}$ is σ -étale (Lemma 6.1.5). Let $\phi(G)[0]$ and $\phi(G)[1]$ denote the Zariski closure 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 6.1.6). Let $\pi_1: \phi(G)[1] \twoheadrightarrow \phi(G)[0]$ be the natural projection (as in Section 2.2). We abbreviate

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

By Proposition 2.2.1 we have $|\phi|_1 \leq \text{ld}(\phi(G))$. If $\ker(\phi)$ is σ -infinitesimal (e.g, if ϕ is injective), then

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

by Corollary 3.2.14 and Theorem 6.3.20. So

$$|\phi|_1 \leq \text{ld}(G).$$

Definition 6.4.5. *Let G be a σ -étale σ -algebraic group. A morphism $\phi: G \rightarrow \mathcal{G}$ of σ -algebraic groups from G to an étale algebraic group $\mathcal{G}$ is called a standard embedding of G (into $\mathcal{G}$) if*

- ϕ is injective,
- $\phi(G)$ is Zariski dense in $\mathcal{G}$ and
- $\text{ld}(G) = |\phi|_1$.

Lemma 6.4.6. *Let G be a σ -étale σ -algebraic group. Then there exists a standard embedding of G .*

Proof. By Theorem 2.1.17 there exists an algebraic group $\mathcal{H}$ and an injective morphism $G \hookrightarrow \mathcal{H}$ of σ -algebraic groups. By Lemma 6.1.6 the Zariski closures $G[i]_{\mathcal{H}}$ of G in $\mathcal{H}$ are étale algebraic groups. As in Section 2.2 let $\mathcal{H}_i$ denote the kernel of the projection $\pi_i: G[i]_{\mathcal{H}} \rightarrow G[i-1]_{\mathcal{H}}$. By Proposition 2.2.1 there exists an $m \geq 0$ such that $\sigma_i: \mathcal{H}_i \rightarrow {}^\sigma(\mathcal{H}_{i-1})$ is an isomorphism for every $i > m$. So $|\mathcal{H}_{m+1}| = \text{ld}(G)$.

Set $\mathcal{G} = G[m]_{\mathcal{H}}$. By Lemma 2.1.16 the inclusion of k -Hopf algebras $k[\mathcal{G}] \subset k\{G\}$ induces a surjective morphism of k - σ -Hopf algebras $k\{G\} \twoheadrightarrow k\{G\}$. Let $\phi: G \hookrightarrow \mathcal{G}$ denote the corresponding injective morphism of σ -algebraic groups and for $i \geq 0$ 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 $i \geq 0$. Let $\mathcal{G}_i$ denote the kernel of the projection $\pi_i: G[i]_{\mathcal{G}} \rightarrow G[i-1]_{\mathcal{G}}$. Then $\mathcal{G}_i = \mathcal{H}_{m+i}$ for $i \geq 1$. Therefore $|\phi|_1 = |\mathcal{G}_1| = |\mathcal{H}_{m+1}| = \text{ld}(G)$. So ϕ is a standard embedding. $\square$

Lemma 6.4.7. *Let G be a σ -étale σ -algebraic group and $\mathcal{G}$ an étale algebraic group. If $\phi: G \hookrightarrow \mathcal{G}$ is an injective morphism of σ -algebraic groups such that $\text{ld}(G) = |\mathcal{G}|$, 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 $\mathcal{G}_i \leq G[i]$ denote the kernel of the projection $\pi_i: G[i] \twoheadrightarrow G[i-1]$ ($\mathcal{G}_0 = G[0]$). By Proposition 2.2.1 the sequence $(|\mathcal{G}_i|)_{i \in \mathbb{N}}$ is non-increasing and stabilizes with value $\text{ld}(G) = |\mathcal{G}|$. But as $\mathcal{G}_0$ is an algebraic subgroup of $\mathcal{G}$, we must have $|\mathcal{G}_i| = |\mathcal{G}|$ for $i \in \mathbb{N}$.

Since $|G[i]| = |G[i-1]| \cdot |\mathcal{G}_i|$ for $i \geq 1$ and $\mathcal{G}_0 = \mathcal{G}$ we have

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

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

Definition 6.4.8. Let G be a σ -étale σ -algebraic group and $\mathcal{G}$ an étale algebraic group. A morphism $\phi: G \rightarrow \mathcal{G}$ of σ -algebraic groups is called a *substandard embedding* of G (into $\mathcal{G}$) if

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

A substandard embedding $G \rightarrow \mathcal{G}$ of G is called *minimal* if $|\mathcal{G}| \leq |\mathcal{H}|$ for any substandard embedding $G \rightarrow \mathcal{H}$ 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 6.4.6 that for any σ -étale σ -algebraic group there exists a minimal substandard embedding.

Lemma 6.4.9. Let G be a σ -étale σ -algebraic group and let $\phi: G \rightarrow \mathcal{G}$ be a minimal substandard embedding. Then for every $r \in \mathbb{N}$ the dimension of $k[\sigma^r(k[\mathcal{G}])] \subset k\{G\}$ 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 Zariski dense in $\mathcal{G}$. By Corollary 6.4.2 the σ -algebraic group $[\sigma]_k \mathcal{G}$ is absolutely σ -reduced. It therefore follows from Corollary 6.3.33 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 comorphism of

$$\tilde{\phi}: G \xrightarrow{\phi} [\sigma]_k \mathcal{G} \rightarrow [\sigma]_k \mathcal{G} / ([\sigma]_k \mathcal{G})_{(r)} = [\sigma]_k ({}^{\sigma^r} \mathcal{G})$$

equals $k[\sigma^r(k[\mathcal{G}])]$. Let $\mathcal{G}' \leq {}^{\sigma^r} \mathcal{G}$ denote the Zariski closure of $\tilde{\phi}(G)$ in ${}^{\sigma^r} \mathcal{G}$. Then $k[\mathcal{G}'] = k[\sigma^r(k[\mathcal{G}])]$ and $\tilde{\phi}$ induces a morphism $\phi': G \rightarrow [\sigma]_k \mathcal{G}'$ of σ -algebraic groups (cf. Lemma 2.1.16).

We will show that ϕ' is a substandard embedding. By construction $\phi'(G)$ is Zariski dense in $\mathcal{G}'$. Because $\ker(\phi)$ and $([\sigma]_k \mathcal{G})_{(r)}$ are σ -infinitesimal (Lemma 6.3.34), it follows from Lemma 6.3.21 that $\ker(\phi') = \ker(\tilde{\phi}) = \phi^{-1}([\sigma]_k \mathcal{G})_{(r)}$ is σ -infinitesimal.

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

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

corresponds to a closed embedding $\phi'(G)[1] \hookrightarrow \sigma^r(\phi(G)[1])$ of algebraic groups, which maps $\mathcal{G}'_1$ into $\sigma^r \mathcal{G}_1$. Therefore $|\mathcal{G}'_1| \leq |\sigma^r \mathcal{G}_1| = |\mathcal{G}_1| = \text{ld}(G)$. On the other hand, $|\mathcal{G}'_1| \geq \text{ld}(\phi'(G))$ by Proposition 2.2.1 and

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

because $\ker(\phi')$ is σ -infinitesimal and therefore $\text{ld}(\ker(\phi')) = 1$ by Theorem 6.3.20. It follows that $|\mathcal{G}'_1| \geq \text{ld}(G)$ and thus $|\mathcal{G}'_1| = \text{ld}(G)$.

So ϕ' is a substandard embedding. Because ϕ is a minimal substandard embedding it follows that $|\mathcal{G}'| \geq |\mathcal{G}|$. But $\mathcal{G}' \leq \sigma^r \mathcal{G}$ 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 . $\square$

Finally, we are prepared for the proof of Babbitt's decomposition theorem for σ -algebraic groups.

Theorem 6.4.10 (Babbitt's decomposition for σ -étale σ -algebraic groups). *Let G be a σ -étale σ -algebraic group. Then there exists a subnormal series*

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

such that $G_1 = G^{\sigma o}$, G_i/G_{i+1} is benign for $i = 1, \dots, n-1$ and G_n is σ -infinitesimal.

Proof. We will prove the theorem by induction on $\text{ld}(G)$. If $\text{ld}(G) = 1$, then G is finite (Proposition 2.4.8) and $G^{\sigma o}$ is σ -infinitesimal by Lemma 6.3.11. Thus the theorem holds with $n = 1$.

So we may assume that $\text{ld}(G) > 1$. Replacing G with $G^{\sigma o}$, we may also assume that G is σ -connected (Corollary 4.2.37).

Step 1: Assume that there exists no normal σ -closed subgroup N of G such that $1 < \text{ld}(N) < \text{ld}(G)$. We will show that there exists a normal σ -infinitesimal σ -closed subgroup G_2 of G such that G/G_2 is benign. (Thus the theorem is satisfied with $n = 2$ and $G_1 = G$.)

Let $\phi: G \rightarrow \mathcal{G}$ be a minimal substandard embedding. We will show that

$$\text{ld}(G) = |\mathcal{G}|. \tag{6.5}$$

Note that (6.5) implies the above claim: The σ -algebraic group $G_2 := \ker(\phi)$ is σ -infinitesimal because ϕ is a substandard embedding and Lemma 6.4.7 applied to the induced embedding $G/G_2 \hookrightarrow \mathcal{G}$ shows that G/G_2 is benign because

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

by Theorem 6.3.20.

So let us prove (6.5). Let $\phi(G)[1] \leq \mathcal{G} \times {}^\sigma \mathcal{G}$ denote the first order Zariski closure of $\phi(G)$ in $\mathcal{G}$. As in Section 2.2 we have morphisms of algebraic groups

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

which induce morphisms $\pi_1: \phi(G)[1] \rightarrow \mathcal{G} (= \phi(G)[0])$ and $\sigma_1: \phi(G)[1] \rightarrow {}^\sigma \mathcal{G}$. Set $\mathcal{G}_1 = \ker(\pi_1)$ and $\mathcal{G}' = \ker(\sigma_1)$. Then $\mathcal{G}'\mathcal{G}_1 \leq \phi(G)[1]$ and we define $\mathcal{H} = \phi(G)[1]/\mathcal{G}'\mathcal{G}_1$. We will next show that

$$|\mathcal{G}| = |\mathcal{H}| \cdot \text{ld}(G). \tag{6.6}$$

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

$$|\mathcal{H}| \cdot |\mathcal{G}_1| = \frac{|\phi(G)[1]|}{|\mathcal{G}'|} = |\phi(G)[1]/\mathcal{G}'|. \quad (6.7)$$

As ϕ is a substandard embedding $|\mathcal{G}_1| = \text{ld}(G)$. Since $k[\phi(G)[1]/\mathcal{G}'] = k[\sigma(k[\mathcal{G}])] \subset k\{G\}$, it follows from Lemma 6.4.9 that $|\phi(G)[1]/\mathcal{G}'| = |\mathcal{G}|$. Thus (6.6) follows from (6.7).

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

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

Since $k[\mathcal{H}]$ is a Hopf subalgebra of $k\{G\}$ we have an induced morphism $k\{\mathcal{H}\} \rightarrow k\{G\}$ of k - σ -Hopf algebras (Lemma 2.1.16) which corresponds to a morphism $\phi': G \rightarrow \mathcal{H}$ of σ -algebraic groups. Let $N \trianglelefteq G$ denote the kernel of ϕ' . By our assumption on G , we have $\text{ld}(N) = 1$ or $\text{ld}(N) = \text{ld}(G)$. So we have to distinguish these two cases.

Case 1: Let us first suppose that $\text{ld}(N) = 1$. Then $\text{ld}(G/N) = \text{ld}(G)$. We will show that ϕ' is a substandard embedding. Because $k[\mathcal{H}] \subset k\{G\}$, we see that $\phi'(G)$ is Zariski dense in $\mathcal{H}$. Let $\phi'(G)[1] \leq \mathcal{H} \times {}^\sigma\mathcal{H}$ denote the first order Zariski closure of $\phi'(G)$ in $\mathcal{H}$ and let $\mathcal{H}_1$ denote the kernel of $\pi_1: \phi'(G)[1] \rightarrow \mathcal{H}$. Using Proposition 2.2.1 we see that

$$|\phi'(G)[1]| = |\mathcal{H}| \cdot |\mathcal{H}_1| \geq |\mathcal{H}| \cdot \text{ld}(\phi'(G)) = |\mathcal{H}| \cdot \text{ld}(G/N) = |\mathcal{H}| \cdot \text{ld}(G). \quad (6.8)$$

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

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

it suffices to show that $|\phi'(G)[1]| = |\phi(G)[1]/\mathcal{G}'|$. But using Lemma 6.4.9, we find that

$$|\phi'(G)[1]| \leq |\phi(G)[1]/\mathcal{G}'| = \dim_k(k[\sigma(k[\mathcal{G}])]) = |\mathcal{G}| = |\mathcal{H}| \cdot \text{ld}(G). \quad (6.9)$$

The combination of equations (6.8) and (6.9) shows that $|\phi'(G)[1]| = |\mathcal{H}| \cdot \text{ld}(G)$ and that $|\mathcal{H}_1| = \text{ld}(\phi'(G))$. 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 $k\{k[\mathcal{G}]\} = k\{\phi(G)\} \subset k\{G\}$, it follows that

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

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

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

Thus N is σ -infinitesimal by Lemmas 6.3.34 and 6.3.21. Therefore

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

by Theorem 6.3.20. In summary, we have shown that ϕ' is a substandard embedding. But $|\mathcal{H}| < |\mathcal{H}| \cdot \text{ld}(G) = |\mathcal{G}|$ because $\text{ld}(G) > 1$. This contradicts the assumption that ϕ is a minimal substandard embedding. Thus the case $\text{ld}(N) = 1$ cannot occur.

Case 2: So we must have $\text{ld}(N) = \text{ld}(G)$. Then $\text{ld}(G/N) = 1$ and therefore G/N is finite (Proposition 2.4.8). Because G is σ -connected, also G/N is σ -connected (Lemma 4.2.45). So G/N is a finite, σ -connected, σ -étale difference algebraic group and must therefore be σ -infinitesimal by Lemma 6.3.11. So by Proposition 6.3.16 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 $\mathfrak{m}_{\mathcal{H}} \subset \mathfrak{m}_{G/N}$, in particular $\sigma^r(\mathfrak{m}_{\mathcal{H}}) = 0$.

On the other hand, $\mathfrak{m}_{\mathcal{H}} \subset k[\mathcal{H}] \subset k[\mathcal{G}]$ and by Lemma 6.4.9 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 $|\mathcal{G}| = \text{ld}(G)$ by (6.6) and (6.5) is proved.

Step 2: Assume that there exists a normal σ -closed subgroup N of G such that $1 < \text{ld}(N) < \text{ld}(G)$. Because $N^{\sigma\sigma}$ is a characteristic subgroup of N (Theorem 4.2.40), it follows that $N^{\sigma\sigma}$ also is a normal σ -closed subgroup of G . We have $\text{ld}(N) = \text{ld}(N^{\sigma\sigma})$ by Proposition 4.2.44. Replacing N by $N^{\sigma\sigma}$ we may thus assume that N is σ -connected.

Because $\text{ld}(G/N) = \text{ld}(G)/\text{ld}(N) < \text{ld}(G)$ we can apply the induction hypothesis to G/N . As G is σ -connected, also G/N is σ -connected (Lemma 4.2.45). So we obtain a subnormal series

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

for G/N where $G \supset G_1 \supset \cdots \supset G_n \supset N$ 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 benign for $i = 0, \dots, n-1$, where $G_0 := G$ (cf. Theorem 5.2.4).

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

$$N \supset N_1 \supset \cdots \supset N_m,$$

with N_m σ -infinitesimal and N_i/N_{i+1} benign for $i = 0, \dots, m-1$ ($N_0 := N$). By Proposition 6.4.4, the subnormal series

$$G_n \supset N \supset N_1 \supset \cdots \supset N_m$$

can be replaced by a subnormal series

$$G_n \supset H_1 \supset \cdots \supset H_m,$$

with G_n/H_1 and H_i/H_{i+1} benign for $i = 1, \dots, m-1$ and H_m σ -infinitesimal. Then

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

is a subnormal series for G of the required form. $\square$

Example 6.4.11. 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. Let us find a Babbitt decomposition for G . We already noted in Example 4.2.49 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 4.2.49.) So a Babbitt decomposition for G is given by

$$G = G^{\sigma\sigma} = G_1 \supset G_2 \supset 1.$$

Example 6.4.12. Let G be the σ -algebraic group given

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

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 us find a Babbitt decomposition for G . Let G_1 and G_2 be the σ -closed subgroups of G given by

$$G_1(R) = \{(g_1, g_2, 1) \in (R^\times)^3 \mid g_1^4 = g_2^4 = 1, \sigma(g_1) = g_2^2\} \leq G(R)$$

and

$$G_2(R) = \{(g_1, 1, 1) \in (R^\times)^3 \mid g_1^4 = 1, \sigma(g_1) = 1\} \leq G(R)$$

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

$$G \supset G_1 \supset G_2 \supset 1$$

is a Babbitt decomposition for G .

Let H be the benign σ -algebraic group given by $H(R) = \{g \in R^\times \mid g^4 = 1\}$ for any k - σ -algebra R . The morphism $\phi: G_1 \rightarrow H$ given by

$$\phi_R: G_1(R) \rightarrow H(R), (g_1, g_2, 1) \mapsto g_2$$

has kernel G_2 . Moreover ϕ is surjective because the dual map $\phi^*: k\{H\} \rightarrow k\{G_1\}$ is injective. So $G_1/G_2 \simeq H$ is benign. Clearly G_2 is σ -infinitesimal. So it remains to show that $G_1 = G^{\sigma\sigma}$. We know that G_2 is σ -connected because G_2 is σ -infinitesimal (Theorem 6.3.20). We also know that G_1/G_2 is σ -connected because it is benign (Proposition 4.2.43). Therefore it follows from Proposition 4.2.42 that G_1 is σ -connected. To show that $G_1 = G^{\sigma\sigma}$ it now suffices to show that G/G_1 is strongly σ -étale (Proposition 4.2.41). But G/G_1 is isomorphic to the σ -algebraic group G' given by

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

which is strongly σ -étale (Example 4.2.28).

Nomenclature

- 1 trivial σ -algebraic group (or identity element of a ring), page 26
- $[\sigma]_k \mathcal{G}$ the algebraic group $\mathcal{G}$ interpreted as a σ -algebraic group, page 27
- $[\sigma]_k \mathcal{X}$ the variety $\mathcal{X}$ interpreted as σ -variety, page 19
- $[\sigma]_k A$ k - σ -algebra obtained from the k -algebra A , page 19
- $[F]$ difference ideal σ -generated by F , page 12
- Δ comultiplication, page 25
- ϕ morphism of σ -varieties, page 15
- $\phi(X)$ scheme theoretic image of a morphism of σ -varieties, page 18
- $\phi: G \hookrightarrow H$ σ -closed embedding of σ -algebraic groups, page 25
- $\phi: G \rightarrow H$ morphism of σ -algebraic groups, page 25
- $\phi: G \twoheadrightarrow H$ ϕ is a surjective morphism of σ -algebraic groups, page 55
- ϕ^* morphism dual to ϕ , page 16
- $\phi^{-1}(Z)$ inverse image of a σ -closed σ -subvariety, page 17
- $\mathcal{G}$ algebraic group, i.e., affine group scheme of finite type (over k), page 27
- $\mathcal{G}_i$ kernel of the projection $G[i] \rightarrow G[i-1]$, page 30
- $\mathbb{G}_a$ additive group (considered as an algebraic group or as a σ -algebraic group), page 27
- $\mathcal{G}$ absolute Galois group of k , page 75
- $\mathbf{G}$ profinite σ -group or finite group, page 108
- $\mathrm{GL}_n, \mathrm{GL}(V)$ general linear group, page 27
- $\mathbb{G}_m$ multiplicative group (considered as an algebraic group or as a σ -algebraic group), page 27
- $\mathbb{I}(X)$ σ -ideal of σ -polynomials vanishing on the σ -variety X , page 15
- $\mathbb{I}(X)$ defining ideal of the σ -variety X , page 17
- $\mathfrak{a}$ ideal or σ -ideal, page 12

- $\mathrm{Im}(\phi)$ set theoretic image of the morphism ϕ , page 17
- ι universal morphism, page 91
- $\ker(\phi)$ kernel of a morphism of σ -algebraic groups, page 49
- $k\text{-}\sigma\text{-Alg}$ category of k - σ -algebras, page 11
- $\mathcal{L}F$ $(\mathcal{L}F)(R) = \varinjlim \mathrm{Hom}(D, F)$, page 92
- $\mathrm{ld}(G)$ limit degree of G , page 38
- $\mathfrak{m}_A$ augmentation ideal of the Hopf algebra A , page 26
- $\mathfrak{m}_G$ augmentation ideal of $k\{G\}$, page 26
- $\mathrm{ord}(G)$ order of G , page 33
- $\bar{k}$ algebraic closure of the field k , page 13
- $\pi_0(A)$ union of all étale subalgebras of A , page 63
- $\pi_0(G)$ group of components of G , page 63
- π_i projection on the Zariski closures, page 20
- $\pi_0^\sigma(G)$ group of σ -connected components of G , page 79
- $\pi_0^\sigma(R)$ union of all strongly σ -étale k - σ -subalgebras of R , page 73
- $\rightsquigarrow$ assignment rule of a functor, page 27
- σ endomorphism, page 10
- σ_i morphism induced by σ on the Zariski closures, page 20
- $\sigma\text{-dim}(G)$ σ -dimension of G , page 33
- Sets** category of sets, page 15
- $\mathrm{Sp}^\sigma(R)$ $\mathrm{Hom}(R, -)$, page 89
- τ element in the Galois group, page 74
- τ^σ the formula to keep in mind is $\tau\sigma = \sigma\tau^\sigma$ and the way to remember it is $\tau^\sigma = \sigma^{-1}\tau\sigma$, page 75
- $\mathbb{V}(F)$ difference variety defined by F , page 15
- $\mathbb{V}_R(F)$ R -rational solutions of F , page 15
- ε counit, page 25
- $\mathcal{V}(\mathfrak{a})$ closed subset of the spectrum defined by $\mathfrak{a}$, page 60
- $\tilde{F}$ sheaf associated with F , page 94
- $\mathcal{X}$ variety (i.e. affine scheme of finite type over a field), page 19

- $\mathcal{X}[i]$ $\mathcal{X} \times^\sigma \mathcal{X} \times \cdots \times^{\sigma^i} \mathcal{X}$, page 20
- $\{\mathfrak{a}\}$ perfect closure, page 41
- $\{\mathfrak{a}\}_{\text{wm}}$ radical mixed closure, page 41
- ${}^{\sigma^i}A$ twist of the k -algebra A by $\sigma^i: k \rightarrow k$, page 19
- ${}_{\sigma^r}R$ k - σ -algebra obtained from R by restriction of scalars via $\sigma^r: k \rightarrow k$, page 124
- $A[i]$ $A \otimes_k {}^\sigma A \otimes_k \cdots \otimes_k {}^{\sigma^i} A$, page 19
- D fat subfunctor, page 89
- F a functor from k - σ -Alg to **Sets**, page 88
- $F(R)$ morphisms of k -algebras from R to k_s , page 110
- F_X σ -Frobenius map, page 124
- F_X^r σ -Frobenius map, page 124
- G, H σ -algebraic groups, page 25
- $G \times H$ direct product of the σ -algebraic groups G and H , page 26
- g^σ $\sigma g^\sigma = g\sigma$, page 108
- $G^{\sigma o}$ σ -identity component of G , page 79
- G^o identity component of G , page 63
- G^{so} strong identity component of G , page 100
- $G_{(r)}$ r -th σ -Frobenius kernel, page 126
- $G_{\sigma\text{-red}, \text{red}}$ $(G_{\text{red}})_{\sigma\text{-red}} = (G_{\sigma\text{-red}})_{\text{red}}$, page 84
- $H \leq G$ H is a σ -closed subgroup of G , page 26
- $HN = NH$ product of σ -algebraic groups, page 96
- $K\langle F \rangle$ σ -field extension of K σ -generated by F , page 11
- $k\{F\}$ k - σ -subalgebra σ -generated by F , page 11
- $k\{G\}$ coordinate ring of the σ -algebraic group G , page 26
- $k\{X\}$ coordinate ring of the σ -variety X , page 15
- k_s separable algebraic closure of the field k , page 13
- $N \trianglelefteq G$ N is a normal σ -closed subgroup of G , page 26
- R k - σ -algebra, page 11
- R difference ring, page 10

- R^* inversive closure of the difference ring R , page 12
- R^σ subring of constant elements, page 68
- $R^\sharp$ algebra obtained by forgetting σ , page 16
- V, W vector spaces or representations, page 46
- X, Y, Z σ -varieties, page 15
- $X \hookrightarrow Y$ σ -closed embedding of σ -varieties, page 18
- $X^\sharp$ scheme obtained from X by forgetting σ , page 16
- X_{per} largest σ -closed σ -subvariety of X that is perfectly σ -reduced, page 41
- X_{red} largest σ -closed σ -subvariety of X that is reduced, page 41
- X_{wm} largest σ -closed σ -subvariety of X that is reduced well-mixed, page 41
- $X_{\sigma\text{-red}}$ largest σ -closed σ -subvariety of X that is σ -reduced, page 41
- $X_{k'}$ σ -variety over k' obtained by base extension, page 18
- $Y[i]$ i -th order Zariski closure of Y in $\mathcal{X}$, page 20
- $Y \cap Z$ intersection of σ -varieties, page 17
- $Y \subset X$ Y is a σ -closed σ -subvariety of X , page 15
- ${}^\sigma\mathbf{G}$ same group as $\mathbf{G}$ but with twisted Galois action, page 112
- $\sigma^r X$ base extension of X via σ^r , page 124
- $\sigma^i \mathcal{X}$ variety obtained from $\mathcal{X}$ by base extension via $\sigma^i: k \rightarrow k$, page 20

Index

- R -covering family, 88
- σ -Frobenius kernel, 126
- σ -Hopf ideal, 26
- σ -étale σ -algebraic group, 62
- σ -étale k - σ -algebra, 62
- σ -algebraic group, 25
- σ -closed σ -subvariety, 15
- σ -closed embedding, 18
- σ -closed set, 67
- σ -closed subgroup, 26
- σ -component, 61
- σ -connected σ -algebraic group, 80
- σ -connected σ -topological space, 67
- σ -connected component of G , 79
- σ -connected components, 67
- σ -continuous action, 113
- σ -dimension of G , 33
- σ -domain, 12
- σ -field, 11
- σ -field σ -generated by F over K , 11
- σ -generated, 11
- σ -ideal, 12
- σ -ideal σ -generated by F , 12
- σ -identity component, 79
- σ -infinitesimal σ -algebraic group, 118
- σ -integral σ -variety, 16
- σ -prime, 12
- σ -projective system, 109
- σ -reduced, 12
- σ -reduced σ -variety, 16
- σ -ring, 10
- σ -separable, 13
- σ -stable, 11
- σ -subring, 11
- σ -topological space, 67
- σ -topology, 67
- σ -variety, 15
- σ -polynomial, 11
- i -th order Zariski closure, 20
- k - σ -Hopf algebra, 25
- k - σ -Hopf subalgebra, 26
- k - σ -functor, 124
- k - σ -algebra, 11
- k - σ -subalgebra, 11
- strongly σ -étale σ -algebraic group, 78
- absolutely σ -reduced, 125
- algebraic σ -group, 40
- algebraic σ -variety, 40
- almost-simple, 99
- benign, 107
- characteristic subgroup, 27
- classical σ -variety, 21
- components of a σ -algebraic group, 61
- connected, 64
- connected component, 60
- constant element, 68
- continuous σ -action, 117
- coordinate ring, 16
- core, 72
- decomposition series, 98
- defining ideal of a σ -variety, 17
- difference field, 11
- difference ideal, 12
- difference ring, 10
- equivalent subnormal series, 98
- exact sequence, 58
- faithful representation, 46
- faithfully flat, 51
- fat subfunctor, 89
- finite σ -algebraic group, 117
- finitely σ -generated σ -ideal, 12
- Frobenius algebraic group, 28
- group functor, 94
- group of σ -connected components, 79
- group of components, 63

- growth group of G , 31
- infinitesimal σ -algebraic group, 118
- injective morphism of σ -algebraic groups, 54
- integral σ -variety, 16
- inversive, 12
- inversive closure, 12
- irreducible component, 60
- isogenous, 103
- isogeny, 103
- kernel of a morphism of σ -algebraic groups, 49
- limit degree, 38
- minimal substandard embedding, 131
- mixed σ -ideal, 41
- morphism of σ -algebraic groups, 25
- normal σ -closed subgroup, 26
- order of G , 33
- perfect, 12
- perfect closure, 41
- perfectly σ -reduced, 12
- perfectly σ -reduced σ -variety, 16
- periodic element, 70
- profinite σ -group, 108
- profinite σ -group of finite σ -type, 110
- refinement of a subnormal series, 98
- reflexive, 12
- representation of G , 46
- semidirect product, 57
- semiinfinitesimal σ -algebraic group, 118
- sheaf, 88
- size of an algebraic group, 38
- standard embedding, 130
- strong identity component, 100
- strongly σ -étale k - σ -algebra, 70
- strongly connected, 100
- subnormal series, 98
- substandard embedding, 131
- surjective morphism of σ -algebraic groups, 55
- topological space of a σ -algebraic group, 60
- variety, 19
- well-mixed, 41
- Zariski closure, 20
- Zariski dense, 20

Bibliography

- [Bab62] Albert E. Babbitt, Jr. Finitely generated pathological extensions of difference fields. *Trans. Amer. Math. Soc.*, 102:63–81, 1962.
- [Bou72] Nicolas Bourbaki. *Elements of mathematics. Commutative algebra*. Hermann, Paris, 1972. Translated from the French.
- [Bou90] N. Bourbaki. *Algebra. II. Chapters 4–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1990. Translated from the French by P. M. Cohn and J. Howie.
- [Bou02] Élisabeth Bouscaren. Théorie des modèles et conjecture de Manin-Mumford (d’après Ehud Hrushovski). *Astérisque*, (276):137–159, 2002. Séminaire Bourbaki, Vol. 1999/2000.
- [Bui92] Alexandru Buium. *Differential algebraic groups of finite dimension*, volume 1506 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1992.
- [Bui93] Alexandru Buium. Geometry of differential polynomial functions. I. Algebraic groups. *Amer. J. Math.*, 115(6):1385–1444, 1993.
- [Bui98] Alexandru Buium. Differential subgroups of simple algebraic groups over p -adic fields. *Amer. J. Math.*, 120(6):1277–1287, 1998.
- [Cas72] Phyllis J. Cassidy. Differential algebraic groups. *Amer. J. Math.*, 94:891–954, 1972.
- [Cas75] Phyllis J. Cassidy. The differential rational representation algebra on a linear differential algebraic group. *J. Algebra*, 37(2):223–238, 1975.
- [Cas78] Phyllis J. Cassidy. Unipotent differential algebraic groups. In *Contributions to algebra (collection of papers dedicated to Ellis Kolchin)*, volume 51 of *Astérisque*, pages 83–115. Soc. Math. France, Paris, 1978.
- [Cas89] Phyllis J. Cassidy. The classification of the semisimple differential algebraic groups and the linear semisimple differential algebraic Lie algebras. *J. Algebra*, 121(1):169–238, 1989.
- [CH99] Zoé Chatzidakis and Ehud Hrushovski. Model theory of difference fields. *Trans. Amer. Math. Soc.*, 351(8):2997–3071, 1999.
- [CH08] Zoé Chatzidakis and Ehud Hrushovski. Difference fields and descent in algebraic dynamics. I. *J. Inst. Math. Jussieu*, 7(4):653–686, 2008.

- [Cha97] Zoé Chatzidakis. Groups definable in ACFA. In *Algebraic model theory (Toronto, ON, 1996)*, volume 496 of *NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci.*, pages 25–52. Kluwer Acad. Publ., Dordrecht, 1997.
- [Cha01] Zoé Chatzidakis. Difference fields: model theory and applications to number theory. In *European Congress of Mathematics, Vol. I (Barcelona, 2000)*, volume 201 of *Progr. Math.*, pages 275–287. Birkhäuser, Basel, 2001.
- [CHP02] Zoé Chatzidakis, Ehud Hrushovski, and Ya’acov Peterzil. Model theory of difference fields. II. Periodic ideals and the trichotomy in all characteristics. *Proc. London Math. Soc. (3)*, 85(2):257–311, 2002.
- [Coh65] Richard M. Cohn. *Difference algebra*. Interscience Publishers John Wiley & Sons, New York-London-Sydney, 1965.
- [CS07] Phyllis J. Cassidy and Michael F. Singer. Galois theory of parameterized differential equations and linear differential algebraic groups. In *Differential equations and quantum groups*, volume 9 of *IRMA Lect. Math. Theor. Phys.*, pages 113–155. Eur. Math. Soc., Zürich, 2007.
- [CS11] Phyllis J. Cassidy and Michael F. Singer. A Jordan-Hölder theorem for differential algebraic groups. *J. Algebra*, 328:190–217, 2011.
- [DG70] Michel Demazure and Pierre Gabriel. *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs*. Masson & Cie, Éditeur, Paris; North-Holland Publishing Co., Amsterdam, 1970.
- [DVHW] Lucia Di Vizio, Charlotte Hardouin, and Michael Wibmer. Difference algebraic relations among solutions of linear differential equations. arXiv:1310.1289.
- [DVHW14] Lucia Di Vizio, Charlotte Hardouin, and Michael Wibmer. Difference Galois theory of linear differential equations. *Adv. Math.*, 260:1–58, 2014.
- [EH00] David Eisenbud and Joe Harris. *The geometry of schemes*, volume 197 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.
- [FJ08] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden.
- [Fre] James Freitag. Indecomposability for differential algebraic groups. arXiv:1106.0695.
- [Gro70] *Schémas en groupes. I: Propriétés générales des schémas en groupes*. Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 151. Springer-Verlag, Berlin, 1970.
- [Har77] Robin Hartshorne. *Algebraic Geometry*. Number 52 in GTM. Springer, 1977.

- [Hru01] Ehud Hrushovski. The Manin-Mumford conjecture and the model theory of difference fields. *Ann. Pure Appl. Logic*, 112(1):43–115, 2001.
- [Hru04] Ehud Hrushovski. The elementary theory of the Frobenius automorphisms, 2004. arXiv:math/0406514v1, updated version available from <http://www.ma.huji.ac.il/~ehud/>.
- [HS08] Charlotte Hardouin and Michael F. Singer. Differential Galois theory of linear difference equations. *Math. Ann.*, 342(2):333–377, 2008.
- [Jan87] Jens Carsten Jantzen. *Representations of algebraic groups*, volume 131 of *Pure and Applied Mathematics*. Academic Press Inc., Boston, MA, 1987.
- [Kam13] Moshe Kamensky. Tannakian formalism over fields with operators. *Int. Math. Res. Not. IMRN*, 24:5571–5622, 2013.
- [Kol48] E. R. Kolchin. Algebraic matrix groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations. *Ann. of Math. (2)*, 49:1–42, 1948.
- [Kol85] E. R. Kolchin. *Differential algebraic groups*, volume 114 of *Pure and Applied Mathematics*. Academic Press Inc., Orlando, FL, 1985.
- [KP00] Piotr Kowalski and Anand Pillay. Pro-algebraic and differential algebraic group structures on affine spaces. *Amer. J. Math.*, 122(1):213–221, 2000.
- [KP02] Piotr Kowalski and A. Pillay. A note on groups definable in difference fields. *Proc. Amer. Math. Soc.*, 130(1):205–212 (electronic), 2002.
- [KP07] Piotr Kowalski and Anand Pillay. On algebraic σ -groups. *Trans. Amer. Math. Soc.*, 359(3):1325–1337 (electronic), 2007.
- [Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
- [Lan08] Peter Landesman. Generalized differential Galois theory. *Trans. Amer. Math. Soc.*, 360(8):4441–4495, 2008.
- [Lev] Alexander Levin. On the ascending chain condition for mixed difference ideals. *Int. Math. Res. Not. IMRN*. to appear, doi: 10.1093/imrn/rnu021.
- [Lev08] Alexander Levin. *Difference algebra*, volume 8 of *Algebra and Applications*. Springer, New York, 2008.
- [Mac97] Angus Macintyre. Generic automorphisms of fields. *Ann. Pure Appl. Logic*, 88(2-3):165–180, 1997. Joint AILA-KGS Model Theory Meeting (Florence, 1995).
- [Mal10] B. Malgrange. Differential algebraic groups. In *Algebraic approach to differential equations*, pages 292–312. World Sci. Publ., Hackensack, NJ, 2010.
- [Mil12] James S. Milne. Basic theory of affine group schemes, 2012. Available at www.jmilne.org/math/.

- [Mil15] James S. Milne. Algebraic groups (v1.10), 2015. Available at www.jmilne.org/math/.
- [Min] Andrey Minchenko. On central extensions of simple differential algebraic groups. arXiv:1401.0522.
- [MO11] Andrey Minchenko and Alexey Ovchinnikov. Zariski closures of reductive linear differential algebraic groups. *Adv. Math.*, 227(3):1195–1224, 2011.
- [MO13] Andrey Minchenko and Alexey Ovchinnikov. Extensions of differential representations of $\mathbf{SL}_2$ and tori. *J. Inst. Math. Jussieu*, 12(1):199–224, 2013.
- [MS10] Rahim Moosa and Thomas Scanlon. Jet and prolongation spaces. *J. Inst. Math. Jussieu*, 9(2):391–430, 2010.
- [MS11] Rahim Moosa and Thomas Scanlon. Generalized Hasse-Schmidt varieties and their jet spaces. *Proc. Lond. Math. Soc. (3)*, 103(2):197–234, 2011.
- [MS14] Alice Medvedev and Thomas Scanlon. Invariant varieties for polynomial dynamical systems. *Ann. of Math. (2)*, 179(1):81–177, 2014.
- [OWa] Alexey Ovchinnikov and Michael Wibmer. σ -Galois theory of linear difference equations. *Int. Math. Res. Not. IMRN*. to appear, doi: 10.1093/imrn/rnu060.
- [OWb] Alexey Ovchinnikov and Michael Wibmer. Tannakian categories with semi-group actions. arXiv:1403.3850.
- [Pil97] Anand Pillay. Some foundational questions concerning differential algebraic groups. *Pacific J. Math.*, 179(1):179–200, 1997.
- [Pil98] Anand Pillay. Differential Galois theory. I. *Illinois J. Math.*, 42(4):678–699, 1998.
- [Ros56] Maxwell Rosenlicht. Some basic theorems on algebraic groups. *Amer. J. Math.*, 78:401–443, 1956.
- [RR39] J. F. Ritt and H. W. Raudenbush, Jr. Ideal theory and algebraic difference equations. *Trans. Amer. Math. Soc.*, 46:445–452, 1939.
- [Sca05] Thomas Scanlon. A positive characteristic Manin-Mumford theorem. *Compos. Math.*, 141(6):1351–1364, 2005.
- [Sca06] Thomas Scanlon. Local André-Oort conjecture for the universal abelian variety. *Invent. Math.*, 163(1):191–211, 2006.
- [Sit74] William Yu Sit. Typical differential dimension of the intersection of linear differential algebraic groups. *J. Algebra*, 32(3):476–487, 1974.
- [Sit75] William Yu Sit. Differential algebraic subgroups of $\mathrm{SL}(2)$ and strong normality in simple extensions. *Amer. J. Math.*, 97(3):627–698, 1975.
- [Spr09] T. A. Springer. *Linear algebraic groups*. Modern Birkhäuser Classics. Birkhäuser Boston, Inc., Boston, MA, second edition, 2009.

- [Sta14] The Stacks Project Authors. Stacks Project. <http://stacks.math.columbia.edu>, 2014.
- [SV99] Thomas Scanlon and José Felipe Voloch. Difference algebraic subgroups of commutative algebraic groups over finite fields. *Manuscripta Math.*, 99(3):329–339, 1999.
- [Tak72] Mitsuhiro Takeuchi. A correspondence between Hopf ideals and sub-Hopf algebras. *Manuscripta Math.*, 7:251–270, 1972.
- [Tom] Ivan Tomašić. Twisted Galois stratification. arXiv:1112.0802.
- [Tom14] Ivan Tomašić. A twisted theorem of Chebotarev. *Proc. Lond. Math. Soc.*, 108(2):291–326, 2014.
- [vdPS97] Marius van der Put and Michael F. Singer. *Galois theory of difference equations*, volume 1666 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.
- [vdPS03] Marius van der Put and Michael F. Singer. *Galois theory of linear differential equations*, volume 328 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.
- [Wat79] William C. Waterhouse. *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.
- [Wib10] Michael Wibmer. *Geometric difference Galois theory*. PhD thesis, Heidelberg, 2010. <http://www.ub.uni-heidelberg.de/archiv/10685>.
- [Wib13] Michael Wibmer. Algebraic difference equations, 2013. Lecture notes, <http://www.algebra.rwth-aachen.de/en/Mitarbeiter/Wibmer/AlgebraicDifferenceEquations.pdf>.