TRIVIALIZING TORSORS FOR DIFFERENCE ALGEBRAIC GROUPS

MICHAEL WIBMER AND ANNETTE BACHMAYR

Dedicated to the memory of Zoé Chatzidakis

Abstract. We study torsors for groups defined by algebraic difference equations. Our main result provides necessary and sufficient conditions on the base difference field for all such torsors to be trivial. We also present an application to the uniqueness of difference Picard-Vessiot extensions for linear differential equations.

1. Introduction

It is a classical question in algebraic geometry and field arithmetic to understand conditions on the base field k that guarantee that $H^1(k, G)$ is trivial or small for large classes of linear algebraic groups G over k. (See e.g., [Ser02]). For example, perfect fields k of cohomological dimension at most one (which include C_1-fields) are characterized by the property that $H^1(k, G)$ is trivial for all connected linear algebraic groups over k and this is equivalent to $H^1(k, G)$ being trivial for all semisimple algebraic groups G over k. It is also known that $H^1(k, G)$ is finite for every linear algebraic group G over k if k is perfect and bounded, i.e., k has only finitely many algebraic extensions of any fixed degree. There has been a sustained interest in obtaining analogs of these results for differential algebraic groups ([Pil17], [MO19], [CP19], [SP21], [LSMP24], [MP25]). One of the most profound results in the area is the following theorem due to Anand Pillay.

Theorem 1.1 ([Pil17])**.** *For an ordinary differential field k of characteristic zero the following statements are equivalent:*

(i) *For every linear differential algebraic group G over k and every G-torsor X we have $X(k) \neq \emptyset$.*
(ii) *We have $H^1_\delta(k, G) = 0$ for every linear differential algebraic group G over k.*
(iii) *The field k is algebraically closed and for every $m \geq 1$ and every $A \in k^{m\times m}$ the linear differential equation $\delta(Y) = AY$ has a solution in $\mathrm{GL}_m(k)$.*

Here (ii) refers to Kolchin's constrained cohomology and the equivalence of (i) and (ii) is well known ([Kol85, Chapter VII]). So the striking part of Theorem 1.1 is that (iii) implies (i) or (ii). As a finite Galois extension defines a torsor for a finite constant group scheme, we see that a field k of characteristic zero is algebraically closed if and only if all torsors for all linear algebraic groups over k are trivial. Moreover, for a differential field k and $A \in k^{m\times m}$, the differential algebraic variety $X = \{Y \in \mathrm{GL}_m \mid \delta(Y) = AY\}$ over k is a torsor for the linear differential algebraic group $\mathrm{GL}_m^\delta = \{g \in \mathrm{GL}_m \mid \delta(g) = 0\}$. Thus, Theorem 1.1 can be reformulated as follows: If for all $m \geq 1$ all torsors for GL_m^δ are trivial and all torsors for linear algebraic groups are trivial, then all torsors for all linear differential algebraic groups are trivial.

Generalizations of Theorem 1.1 to partial differential fields are discussed in [CP19] and [MO19]. Another generalization of Theorem 1.1, that can be seen as a relative version, not requiring any assumptions on the ordinary base differential field, can be found in [MP25].

The question of an appropriate difference analog of Theorem 1.1 was raised in [Pil17, Section 3] and in [CP19] it is shown that the *immediate* analog of Theorem 1.1 fails for difference algebraic groups. The counterexample provided is related to the difference algebraic subgroup $G = \{g \in \mathbb{G}_m \mid x^{-2}\sigma(x) = 1\}$ of the multiplicative group $\mathbb{G}_m$ and the G-torsor $X = \{x \in \mathbb{G}_m \mid x^{-2}\sigma(x) = a\}$, where $a \in k^\times$. More

Date: September 29, 2025.
2020 *Mathematics Subject Classification.* 14L15, 14L17, 12H05.
This work was supported by DFG (Deutsche Forschungsgemeinschaft): SFB-TRR 195.

generally, for $\alpha_0,\ldots,\alpha_m\in\mathbb{Z}$ with $\alpha_m\neq 0$ and $a\in k^\times$, we have a difference algebraic subgroup $G=\{g\in\mathbb{G}_m|\ g^{\alpha_0}\sigma(g)^{\alpha_1}\ldots\sigma^m(g)^{\alpha_m}=1\}$ of $\mathbb{G}_m$ and a G-torsor $X=\{x\in\mathbb{G}_m|\ x^{\alpha_0}\sigma(x)^{\alpha_1}\ldots\sigma^m(x)^{\alpha_m}=a\}$.

The main result of this paper is an analog of Theorem 1.1 for difference algebraic groups. In essence, it states that the solvability of these multiplicative equations $y^{\alpha_0}\sigma(y)^{\alpha_1}\ldots\sigma^m(y)^{\alpha_m}=a$ is the only obstruction to the validity of the immediate difference analog of Theorem 1.1. However, as difference algebraic geometry is somewhat more intricate than differential algebraic geometry, this has to be taken with a grain of salt. Specifically, while differential algebraic geometry is more or less synonymous with the model theory of differential fields, the connections are more subtle in the difference case.

Before precisely stating our main result, we need to explain other obstructions to the validity of the immediate difference analog of Theorem 1.1, that are not related to difference algebraic subgroups of $\mathbb{G}_m$ and can be resolved by passing to higher powers of the endomorphism σ. We note that the philosophy that things can be smoothed out by passing to higher powers of σ is also present in other work (e.g., [CHP02] or [Wib12]).

Some torsors for linear difference algebraic groups do not have a point in any difference field. For example, the difference variety $X=\{x\in\mathbb{G}_m|\ x^2=1,\ \sigma(x)=-x\}$ is a torsor for the linear difference algebraic group $G=\{g\in\mathbb{G}_m|\ g^2=1,\ \sigma(g)=g\}$ (under left multiplication) but $X(k)=\emptyset$ for every difference field k. In other words, this torsor will never be trivial, no matter over which base difference field it is considered. From a model theoretic perspective, where one is confined to working inside a monster model of the theory of difference fields, the torsor X does not exist, i.e., it collapses to the empty set. However, this perspective is unsatisfactory from the point of view of difference algebraic geometry, because the system of equations $x^2=1,\ \sigma(x)=-x$ is consistent, in the sense that it has a solution in a difference ring. For example, $(1,-1,1,-1,1,\ldots)$ is a solution in the ring of sequences (equipped with the shift).

The problem that not every torsor has a point in a difference field can be resolved by looking for solutions slightly beyond the base difference field k. In the above example, we have $(1,-1)\in X(k^{[2]})$, where, for an integer $n\geq 1$, we let $k^{[n]}=k\times\ldots\times k$ denote the product of n copies of k, considered as a difference algebra over k via $k\to k^{[n]},\ a\mapsto(\sigma^{n-1}(a),\ldots,\sigma(a),a)$ and

$$\sigma\colon k^{[n]}\to k^{[n]},\ (a_1,\ldots,a_n)\mapsto(\sigma^n(a_n),a_1,\ldots,a_{n-1}).$$

A similar obstruction to the immediate difference analog of Theorem 1.1 occurs if we look at linear difference algebraic groups of the form $G=\{g\in\mathcal{G}|\ \sigma(g)=\psi(g)\}$, where $\mathcal{G}\leq\mathrm{GL}_m$ is an algebraic subgroup defined over $\mathbb{Q}$ and $\psi\colon\mathcal{G}\to\mathcal{G}$ is a morphism of algebraic groups. For example, we can take $G=\{g\in\mathrm{GL}_m\mid\sigma(g)=(g^T)^{-1}\}$. It is known that all G-torsors are of the form $X=\{x\in\mathrm{GL}_m\mid\sigma(x)=(x^T)^{-1}A\}$ for some $A\in\mathrm{GL}_m(k)$. The equation $x^T\sigma(x)=A$ is non-linear and there appears to be no reason why we should be able to find a solution in the base difference field k, just because k is algebraically closed and we can solve linear difference equations in k. However, if we pass from σ to σ^2, then every $x\in X$ satisfies $\sigma^2(x)=x(A^T)^{-1}\sigma(A)$ (a linear difference equation over (k,σ^2)) and we have a difference variety $X_2=\{x\in\mathrm{GL}_m\mid\sigma^2(x)=x(A^T)^{-1}\sigma(A)\}$ over the difference field (k,σ^2). Thus, if every linear difference equation over (k,σ^2) is solvable, then $X_2(k)\neq\emptyset$. Furthermore, $X_2(k)\neq\emptyset$ turns out to be equivalent to $X(k^{[2]})\neq\emptyset$ (Remark 3.6). In Section 3 below we will explain systematically how a difference variety X over (k,σ) gives rise to a difference variety X_n over (k,σ^n) for every $n\geq 1$. We will also see that for a linear difference algebraic group G, the cohomology sets $H^1_{\sigma^n}(k,G_n)$ naturally form a direct system. The main result of this paper is the following difference analog of Theorem 1.1.

Theorem 1.2. *For an ordinary difference field k of characteristic zero the following statements are equivalent:*

- (P1) *For every linear difference algebraic group G over k and for every G-torsor X, there exists an integer $n\geq 1$ such that $X(k^{[n]})\neq\emptyset$.*
- (P2) *We have $\lim\limits_{n\to\infty}H^1_{\sigma^n}(k,G_n)=0$ for every linear difference algebraic group G over k.*
- (P3) (a) *The field k is algebraically closed.*
  - (b) *For every $m\geq 1$ and every $A\in\mathrm{GL}_m(k)$ there exists an integer $n\geq 1$ such that the equation $\sigma(Y)=AY$ has a solution in $\mathrm{GL}_m(k^{[n]})$.*
  - (c) *For all $\alpha_1,\ldots,\alpha_m\in\mathbb{Z}$ with $\alpha_m\neq 0$ and $a\in k^\times$, there exists an $n\geq 1$ such that the equation $y^{\alpha_0}\sigma(y)^{\alpha_1}\ldots\sigma^m(y)^{\alpha_m}=a$ has a solution in $k^{[n]}$.*

We note that we do not make any assumptions on the constants $k^\sigma = \{a \in k \mid \sigma(a) = a\}$ of k. The constants of an algebraically closed differential field are automatically algebraically closed. However, this need not be the case in the difference world. Condition (P3) (b) is similar to what is called "strongly PV-closed" or "linearly closed" in [CP19], [CK23] and [KP07]. A difference field k is strongly PV-closed if for every $m \geq 1$ and every $A \in \mathrm{GL}_m(k)$ the equation $\sigma(Y) = AY$ has a solution in $\mathrm{GL}_m(k)$. Our condition (P3) (b) is weaker than being strongly PV-closed and is more in line with the Picard-Vessiot theory of linear difference equations ([vdPS97]), where one allows zero-divisors in the solution rings and usually assumes the constants to be algebraically closed. The constants of a strongly PV-closed difference field have absolute Galois group $\widehat{\mathbb{Z}}$ (because for every $m \geq 1$ the equation $\sigma^m(y) = y$ has to have m solutions in k that are linearly independent over the constants). On the other hand, our condition (P3) (b) does not obviously imply any restrictions on the constants (although it follows from (P3) (a) that the absolute Galois group of the constants is procyclic).

The multiplicative difference equations in (P3) (b) are intimately related to toric difference varieties studied in [GHWY17], [GHY17] [Wan20], [Wan18].

Condition (P3) (b) is equivalent to the special case of (P1) where $G = \mathrm{GL}_m^\sigma = \{g \in \mathrm{GL}_m \mid \sigma(g) = g\}$, while condition (P3) (c) is equivalent to the special case of (P1) for one-relator subgroups of $\mathbb{G}_m$, i.e., for difference algebraic subgroups of $\mathbb{G}_m$ of the form $G = \{g \in \mathbb{G}_m \mid g^{\alpha_0}\sigma(g)^{\alpha_1}\ldots\sigma^m(g)^{\alpha_m} = 1\}$.

For a linear difference algebraic group G over a difference field k, we say that k is *G-trivial* if for all G-torsors X there exists an $n \geq 1$ such that $X(k^{[n]}) \neq \emptyset$. With this nomenclature our main result can be reformulated as follows: If k is G-trivial for all G where G is a linear algebraic group, a difference algebraic group of the form $G = \mathrm{GL}_m^\sigma = \{g \in \mathrm{GL}_m \mid \sigma(g) = g\}$ (for some $m \geq 1$), or a one-relator subgroup of $\mathbb{G}_m$, then k is G-trivial for all linear difference algebraic groups G over k. In this sense, the one-relator subgroups of $\mathbb{G}_m$ are the only obstruction to the immediate difference analog of Theorem 1.1.

Note that the integer n in the first condition of Theorem 1.2 depends on both the difference algebraic group G and the G-torsors X. Similarly, in the third condition, the integer n depends on $A \in \mathrm{GL}_m(k)$ or $a \in k^\times$. We can replace both conditions by a stronger condition where an n has to exist uniformly for all G-torsors, and where n is not allowed to depend on A and a. As an additional result we show that these stronger conditions are still equivalent:

Theorem 1.3. *For an ordinary difference field k of characteristic zero the following statements are equivalent:*

- ($\mathrm{P1}^u$) *For every linear difference algebraic group G over k there exists an integer $n \geq 1$ such that $X(k^{[n]}) \neq \emptyset$ for every G-torsor X.*
- ($\mathrm{P2}^u$) *For every linear difference algebraic group G over k, there exists an integer $n \geq 1$ such that the natural map $H^1_\sigma(k, G) \to H^1_{\sigma^n}(k, G_n)$ is trivial.*
- ($\mathrm{P3}^u$) (a) *The field k is algebraically closed.*
  - (b) *For every $m \geq 1$, there exists an integer $n \geq 1$ such that for every $A \in \mathrm{GL}_m(k)$ the equation $\sigma(Y) = AY$ has a solution in $\mathrm{GL}_m(k^{[n]})$.*
  - (c) *For all $\alpha_1, \ldots, \alpha_m \in \mathbb{Z}$ with $\alpha_m \neq 0$, there exists an $n \geq 1$ such that for all $a \in k^\times$ the equation $y^{\alpha_0}\sigma(y)^{\alpha_1}\ldots\sigma^m(y)^{\alpha_m} = a$ has a solution in $k^{[n]}$.*

There appears to be no previous difference analogs of Theorem 1.1 in the literature. However, the connection between $H^1(k, \mathrm{GL}_m^\sigma)$ and solutions of linear difference equations was already noted in [CK23, Section 7.3], where also the counterexample from [CP19] is interpreted in cohomological terms.

In Section 6 we show that every σ-closed difference field satisfies the equivalent conditions of Theorem 1.3. While we establish our main result ((P3)$\Rightarrow$(P1)) only in characteristic zero, we think that it is interesting to note that an algebraically closed field k of positive characteristic p, equipped with a Frobenius endomorphism $\sigma_q\colon k \to k,\ a \mapsto a^q$ (with q a power of p), satisfies property ($\mathrm{P3}^u$). Indeed, that (k, σ_q) satisfies ($\mathrm{P3}^u$) (b) with $n = 1$ is a special case of the Lang-Steinberg Theorem and that (k, σ_q) satisfies ($\mathrm{P3}^u$) (c) with $n = 1$ follows from k being algebraically closed.

Our main result has applications in the difference Galois theory of linear differential equations ([DVHW14]), a special case of the parameterized Picard-Vessiot theory, where one considers a linear differential equation and an auxiliary operator such as a derivation or an endomorphism that is acting on the coefficients of the linear differential equation. A typically example is a linear differential equation with coefficients that depend on a parameter and the auxiliary operator is the derivation with respect to the parameter or a shift operator on the parameter. Our application concerns the uniqueness of the solution rings in the context of this Galois theory, known as σ-Picard-Vessiot rings. This is similar to the application in [Pil17, Cor. 1.4] of Theorem 1.1 to the uniqueness of the solution rings in the case when the auxiliary operator is a derivation. However, our situation is slightly different because σ-Picard-Vessiot rings are generally not unique, even when the constants are σ-closed. In general, two σ-Picard-Vessiot rings for the same equation only become isomorphic when passing to higher powers of σ. More precisely, in [DVHW14, Cor. 1.17] it is shown that if K is a $\delta\sigma$-field such that the δ-constants K^δ are a σ-closed σ-field and R_1, R_2 are two σ-Picard-Vessiot rings for the equation $\delta(y) = Ay$ (for some $A \in K^{m\times m}$), then there exists an integer $n \geq 1$ such that R_1 and R_2 are isomorphic as K-$\delta\sigma^n$-algebras. We note that the integer n is allowed to depend on R_1 and R_2. In particular, the need to pass to higher powers of σ also naturally arises in the parameterized Picard-Vessiot theory and this phenomenon is well-aligned with our philosophy underlying the statements of Theorems 1.3 and 1.2.

We improve the above uniqueness result in two ways. Firstly, we show that the same uniqueness result also holds if we only assume that K^δ satisfies the equivalent conditions of Theorem 1.2. Secondly, we show that if K^δ satisfies the equivalent conditions of Theorem 1.3 (e.g., K^δ is σ-closed), then the integer n can be chosen uniformly for all pairs R_1, R_2 of σ-Picard-Vessiot rings.

We conclude the introduction with an outline of the content. In Section 2 we set the stage by recalling definitions and introducing our notation. In Section 3 we formally introduce, for every difference variety X over (k, σ), the difference varieties X_n over (k, σ^n) and we establish the important induction principle. It states that if N is a normal difference algebraic subgroup of a difference algebraic group G, such that $\lim\limits_{n\to\infty} H^1_{\sigma^n}(k, N) = 0$ and $\lim\limits_{n\to\infty} H^1_{\sigma^n}(k, (G/N)_n) = 0$, then $\lim\limits_{n\to\infty} H^1_{\sigma^n}(k, G_n) = 0$. This principle allows us to use decomposition theorems for difference algebraic groups to reduce the proof to certain types of mostly quite explicitly described classes of difference algebraic groups. In Section 3 we also show that (P1) and (P2) are equivalent, which is fairly straight forward once the appropriate definitions are in place. The fact that (P1) implies (P3) is also fairly immediate and established in Section 4 along with some reformulations of property (P3). The most difficult part of the proof of Theorem 1.3 is the implication (P3)⇒(P1). This relies on several structure and decomposition theorems for difference algebraic groups. We first treat special classes of difference algebraic groups (e.g., order zero, diagonalizable, difference dimension theory zero) and build up to the general case. In Section 6 we show that a σ-closed difference field satisfies the equivalent conditions of Theorem 1.3. Finally, in Section 7 we present the application to the parameterized Picard-Vessiot theory.

The authors are grateful to Zoé Chatzidakis and Anand Pillay for helpful discussions during the preparation of the article.

2. Basic definitions and constructions

In this section we recall the basic definitions from difference algebra and some results about difference algebraic groups. The reader with a solid grounding in difference algebra may prefer to skip this section.

We start by recalling some definitions from difference algebra. Standard references for difference algebra are [Coh65] and [Lev08]. Our main references for difference algebraic groups are [Wib22] and [Wib21]. All rings are assumed to be commutative and unital. A *difference ring* (or *σ-ring* for short) R is a ring together with a ring endomorphism $\sigma\colon R \to R$. A morphism of σ-rings is a morphism of rings that commutes with σ.

Let k be a σ-ring. A *k-σ-algebra* is a σ-ring R together with a k-algebra structure such that $k \to R$ is a morphism of σ-rings. A morphism of k-σ-algebras $R \to S$ is a morphism of σ-rings that also is a morphism of k-algebras. We will write $\mathrm{Hom}_{k,\sigma}(R, S)$ for the set of morphisms of k-σ-algebras.

If R and S are k-σ-algebras, then $R \otimes_k S$ is a k-σ-algebra via $\sigma(r \otimes s) = \sigma(r) \otimes \sigma(s)$. A k-σ-algebra R is *finitely σ-generated* if there exists a finite subset $B \subseteq R$ such that $R = k[B, \sigma(B), \ldots]$. We write $R = k\{B\}$ for a k-σ-algebra R if $B \subseteq R$ is such that $R = k[B, \sigma(B), \ldots]$.

An ideal $\mathfrak{a}$ of a σ-ring R is a *σ-ideal* if $\sigma(\mathfrak{a}) \subseteq \mathfrak{a}$. If $\sigma^{-1}(\mathfrak{a}) = \mathfrak{a}$, then $\mathfrak{a}$ is a *reflexive* σ-ideal. If $f\sigma(f) \in \mathfrak{a}$ implies that $f \in \mathfrak{a}$, then $\mathfrak{a}$ is a *perfect* σ-ideal. For a subset B of R, the σ-ideal $[B] = (B, \sigma(B), \sigma^2(B), \ldots) \subseteq R$ is the σ-ideal *σ-generated by B*.

Let k be a σ-field. A *σ-polynomial* over k in the σ-variables $y_1,\ldots,y_n$ is a polynomial in the variables $y_1,\ldots,y_n,\sigma(y_1),\ldots,\sigma(y_n),\sigma^2(y_1),\ldots$ over k. The k-σ-algebra of all σ-polynomials is denoted by $k\{y\}=k\{y_1,\ldots,y_n\}$.

Informally speaking, a *σ-variety* X over k (or a *k-σ-variety*) is the set of solutions of a set $F\subseteq k\{y\}$ of σ-polynomials. To make this precise, we can define X to be the functor from the category of k-σ-algebras to the category of sets that assigns to every k-σ-algebra R the R-valued solutions of F. A morphism of k-σ-varieties is then simply a natural transformation of functors. Alternatively, we can fix a sufficiently large[1] k-σ-algebra $\mathcal{U}$ and define a k-σ-variety to be the set of $\mathcal{U}$-valued solutions of F. Then a morphism of k-σ-varieties is simply a map that is given by σ-polynomials in the coordinates. A *σ-algebraic group*[2] (over k) is a group object in the category of σ-varieties (over k). A morphism of σ-algebraic groups (over k) is a morphism of σ-varieties (over k) that respects the group structure.

In practice it does not matter if we work with functors or inside $\mathcal{U}$. In fact, we will suppress the R or the $\mathcal{U}$ from the notation most of the time. For example, we may write $\phi\colon \mathbb{G}_m\to\mathbb{G}_m,\ g\mapsto\sigma(g)g$ to specify a morphism ϕ of σ-algebraic group from the multiplicative group to the multiplicative group. This can either be read as the transformation of functors such that $\phi_R\colon \mathbb{G}_m(R)\to\mathbb{G}_m(R),\ g\mapsto\sigma(g)g$ for every k-σ-algebra R or as the map $\mathbb{G}_m(\mathcal{U})\to\mathbb{G}_m(\mathcal{U}),\ g\mapsto\sigma(g)g$.

For a k-σ-variety X
$$\mathbb{I}(X)=\{f\in k\{y\}|\ f(x)=0\ \forall\ x\in X\}$$
is a σ-ideal of $k\{y\}$. The k-σ-algebra $k\{X\}=k\{y\}/\mathbb{I}(X)$ is called the *σ-coordinate ring* of X. The functor $X\rightsquigarrow k\{X\}$ induces an equivalence of categories between the category of k-σ-varieties and the category of finitely σ-generated k-σ-algebras. Moreover $X\simeq \operatorname{Hom}_{k,\sigma}(k\{X\},-)$ as functors. (See [Wib22, Section 1.2].) Allowing ourselves the freedom of calling any functor isomorphic to a k-σ-variety (as defined above) a k-σ-variety, it follows that a functor from the category of k-σ-algebras to the category of sets is a k-σ-variety if and only if it is representable by a finitely σ-generated k-σ-algebra. The category of σ-algebraic groups over k is equivalent to the category of finitely σ-generated k-σ-Hopf algebras, i.e., Hopf algebras over k, that are finitely σ-generated k-σ-algebras such that the Hopf algebra structure maps are morphisms of k-σ-algebras.

A σ-ring R is called *σ-reduced* if $\sigma\colon R\to R$ is injective. The quotient $R_{\sigma\text{-}\mathrm{red}}=R/(0)^*$ of R by the reflexive closure $(0)^*=\{f\in R\mid \exists\ n\geq 1:\ \sigma^n(f)=0\}$ of the zero ideal is σ-reduced. A k-σ-variety X is *σ-reduced* if $k\{X\}$ is σ-reduced. If the zero ideal of $k\{X\}$ is perfect, then X is called *perfectly σ-reduced*. If $k\{X\}$ is σ-reduced and an integral domain, then X is called *σ-integral*.

A subfunctor Y of a k-σ-variety X is a *σ-closed σ-subvariety* if it is defined by a σ-ideal $\mathbb{I}(Y)\subseteq k\{X\}$, i.e.,

$$\begin{tikzcd}
Y(R) \arrow[r, hook] \arrow[d, "\simeq"'] & X(R) \arrow[d, "\simeq"] \\
\operatorname{Hom}_{k,\sigma}(k\{X\}/\mathbb{I}(Y),R) \arrow[r, hook] & \operatorname{Hom}_{k,\sigma}(k\{X\},R)
\end{tikzcd}$$

commutes for every k-σ-algebra R. A morphism $\phi\colon X\to Y$ of k-σ-varieties is a *σ-closed embedding* if it induces an isomorphism between X and a σ-closed σ-subvariety of Y; equivalently, the dual map $\phi^*\colon k\{Y\}\to k\{X\}$ is surjective ([Wib22, Lemma 1.6]).

If $\phi\colon X\to Y$ is a morphism of k-σ-varieties, we denote with $\phi(X)$ the smallest σ-closed σ-subvariety of Y such that ϕ factors through the inclusion $\phi(X)\hookrightarrow Y$ (cf. [Wib22, Lemma 1.5]).

If K is a σ-field extension of k and X a σ-variety over k, we denote the base change of X from k to K by X_K. So $X_K(R)=X(R)$ for every K-σ-algebra R. Then X_K is a σ-variety over K with σ-coordinate ring $K\{X_K\}=k\{X\}\otimes_k K$.

If G is a σ-algebraic group and H a σ-closed σ-subvariety such that $H(R)$ is a subgroup of $G(R)$ for every k-σ-algebra R, then H is a called a *σ-closed subgroup* of G and we will write $H\leq G$. If moreover $H(R)$ is a normal subgroup of $G(R)$ for every k-σ-algebra R, then H is *normal* in G and we indicate this by $H\trianglelefteq G$.

[1]The precise requirement here is that $\mathcal{U}$ contains an isomorphic copy of every finitely σ-generated k-σ-algebra.

[2]It may seems more accurate to add the word affine or linear here. However, since we will only consider affine σ-varieties we refrain from doing so.

The forgetful functor from k-σ-algebras to k-algebras has a left adjoint $S \rightsquigarrow [\sigma]_k S$ which we need to describe explicitly. For a k-algebra S and $i \geq 1$ we set ${}^{\sigma^i}S = S \otimes_k k$ where the tensor product is formed by using $\sigma^i \colon k \to k$. More generally, if X is an object over k, we denote by ${}^{\sigma^i}X$ the base change of X via $\sigma^i \colon k \to k$. We set $S[i] = S \otimes_k {}^{\sigma}S \otimes_k \ldots \otimes_k {}^{\sigma^i}S$ and let $[\sigma]_k S$ denote the direct limit (i.e., the union) of the $S[i]$'s. We define the structure of a k-σ-algebra on $[\sigma]_k S$ by setting

$$\sigma(f_0 \otimes (f_1 \otimes \lambda_1) \otimes \ldots \otimes (f_i \otimes \lambda_i)) = 1 \otimes (f_0 \otimes 1) \otimes (f_1 \otimes \sigma(\lambda_1)) \otimes \ldots \otimes (f_i \otimes \sigma(\lambda_i)) \in S[i+1]$$

for $f_0, \ldots, f_i \in S$ and $\lambda_1, \ldots, \lambda_i \in k$.

Example 2.1. Consider the univariate polynomial ring $S = k[y]$. Then

$$S[i] = k[y, 1 \otimes (y \otimes 1), \ldots, 1 \otimes \cdots \otimes (y \otimes 1)]$$

and $\sigma \colon S[i] \to S[i+1]$ shifts each generator to the next one. Hence $[\sigma]_k S = k\{y\}$, the difference polynomial ring in one variable.

For the sake of brevity and to be consistent with our nomenclature for difference algebraic geometry, we use the term *variety over* k to mean affine scheme of finite type over k. If $\mathcal{X}$ is a variety over k, then the functor $R \rightsquigarrow [\sigma]_k \mathcal{X}(R) = \mathcal{X}(R)$ is a σ-variety over k. Indeed, $k\{[\sigma]_k \mathcal{X}\} = [\sigma]_k k[\mathcal{X}]$ where $k[\mathcal{X}]$ is the coordinate ring of $\mathcal{X}$. (Cf. [Wib22, Section 1.3].)

By an *algebraic group* over k we mean an affine group scheme of finite type over k. By a *closed subgroup* of an algebraic group we mean a closed subgroup scheme. Let $\mathcal{G}$ be an algebraic group over k. Then $[\sigma]_k \mathcal{G}$ is a σ-algebraic group over k. If confusion is unlikely we will simply write $\mathcal{G}$ for $[\sigma]_k \mathcal{G}$. In particular, by a σ-closed subgroup of $\mathcal{G}$, we mean a σ-closed subgroup of $[\sigma]_k \mathcal{G}$.

Let G be a σ-closed subgroup of an algebraic group $\mathcal{G}$. Then G is defined by a σ-ideal $\mathbb{I}(G) \subseteq [\sigma]_k k[\mathcal{G}]$. For $i \geq 0$ the intersection $\mathbb{I}(G) \cap k[\mathcal{G}][i] \subseteq k[\mathcal{G}][i] = k[\mathcal{G} \times \ldots \times {}^{\sigma^i}\mathcal{G}]$ defines a closed subgroup $G[i]$ of $\mathcal{G} \times \ldots \times {}^{\sigma^i}\mathcal{G}$. We call $G[i]$ the *i-th order Zariski closure* of G in $\mathcal{G}$. For $i = 0$ we simply speak of the *Zariski closure*. If $G[0] = \mathcal{G}$, we say that G is *Zariski-dense* in $\mathcal{G}$.

In [Wib22, Theorem 3.7] it is shown that there exist integers $d, e \geq 0$ such that $\dim(G[i]) = d(i+1)+e$ for $i \gg 0$. Moreover every σ-algebraic group G is isomorphic to a σ-closed subgroup of an algebraic group $\mathcal{G}$ ([Wib22, Prop. 2.16]), e.g., $\mathcal{G}$ can be chosen as GL_m for some m, and the integer d does not depend on the choice of $\mathcal{G}$ or the choice of such an embedding. We call d the *σ-dimension* of G and denote it by $\sigma\text{-}\dim(G)$. Furthermore, if $\sigma\text{-}\dim(G) = 0$, then the integer $\mathrm{ord}(G) = e \geq 0$ only depends on G and is called the *order* of G. If $\sigma\text{-}\dim(G) > 0$, we set $\mathrm{ord}(G) = \infty$.

Example 2.2. As an example, consider $\mathcal{G} = \mathbb{G}_a$ and $G = \{g \in \mathcal{G} \mid \sigma^2(g) - \sigma(g) - 1 = 0\}$. Then $G[0] = \mathcal{G}$ and $G[1] = \mathcal{G} \times {}^{\sigma}\mathcal{G}$ as they do not see the defining equation. But $G[2]$ is the closed subgroup of $\mathcal{G} \times {}^{\sigma}\mathcal{G} \times {}^{\sigma^2}\mathcal{G}$ defined by $\sigma^2(x) - \sigma(x) - 1 = 0$, so it has dimension 2. The dimension of $G[3]$ equals 2, since it is defined by the two equations $\sigma^2(x) - \sigma(x) - 1 = 0$ and $\sigma^3(x) - \sigma^2(x) - 1 = 0$ inside $\mathcal{G} \times {}^{\sigma}\mathcal{G} \times {}^{\sigma^2}\mathcal{G} \times {}^{\sigma^3}\mathcal{G}$. Similarly, it follows that $d_i = 2$ for all $i \geq 2$. Hence $\sigma\text{-}\dim(G) = 0$ and $\mathrm{ord}(G) = 2$.

Let G be a σ-algebraic group and let $N \trianglelefteq G$ be a normal σ-closed subgroup. The quotient G/N can be defined by a universal property ([Wib21, Def. 3.1]). It exists (Ibid., Theorem 3.3) and is well-behaved with respect to the σ-dimension and the order (Ibid. Corollary 3.13): Namely, $\sigma\text{-}\dim(G) = \sigma\text{-}\dim(N) + \sigma\text{-}\dim(G/N)$ and $\mathrm{ord}(G) = \mathrm{ord}(N) + \mathrm{ord}(G/N)$. Furthermore, the isomorphism theorems hold for σ-algebraic groups (Ibid., Section 5).

A morphism $\phi \colon G \to H$ of σ-algebraic groups is called a *quotient map* if $\phi(G) = H$. (For other equivalent characterizations of quotient maps see Proposition 4.10 in [Wib21].) In particular, ϕ is a quotient map if and only if $H \simeq G/N$ for a normal σ-closed subgroup N of G. Any morphism of σ-algebraic groups factors uniquely as a quotient map followed by a σ-closed embedding ([Wib21, Theorem 4.14]).

The kernel $\ker(\phi)$ of a morphism $\phi \colon G \to H$ of σ-algebraic groups is given by $\ker(\phi)(R) = \ker(\phi_R)$ for every k-σ-algebra R. It is a normal σ-closed subgroup of G. Indeed, $\mathbb{I}(\ker(\phi)) \subseteq k\{G\}$ is the ideal of $k\{G\}$ generated by $\phi^*(\mathfrak{m}_H)$, where $\mathfrak{m}_H$ is the kernel of the counit $k\{H\} \to k$. A sequence $1 \to N \xrightarrow{\alpha} G \xrightarrow{\beta} H \to 1$ of σ-algebraic groups is called *exact* if β is a quotient map and α is a σ-closed embedding that identifies N with the kernel of β.

A σ-algebraic group G is called *σ-étale* if every element of $k\{G\}$ satisfies a separable polynomial over k. Recall that a finite dimensional k-algebra S is étale if every element of S satisfies a separable polynomial over k. For a k-algebra R, let $\pi_0(R)$ denote the union of all étale k-subalgebras of R.

Let G be a σ-algebraic group. Among all morphisms from G to a σ-étale σ-algebraic group, there exists a universal one $G \to \pi_0(G)$. See [Wib22, Prop. 6.13]. Indeed $k\{\pi_0(G)\} = \pi_0(k\{G\})$. The kernel G^o of $G \to \pi_0(G)$ is called the *identity component* of G. If $G = G^o$, then G is called *connected*. See [Wib21, Lemma 6.7] for other characterizations of connectedness.

Let G be a σ-algebraic group over k. A *G-torsor* is a k-σ-variety X together with a morphism $G \times X \to X$ of k-σ-varieties such that $G(R) \times X(R) \to X(R)$ is a simply transitive group action of the group $G(R)$ on the set $X(R)$ for every k-σ-algebra R. A morphism of G-torsors is a G-equivariant morphism of k-σ-varieties. A G-torsor isomorphic to G with left-translation is called *trivial*. A G-torsor X is trivial if and only if $X(k) \neq \emptyset$ ([BW22, Remark 1.3]).

Throughout this article k denotes a σ-field. All varieties, σ-varieties, algebraic groups and σ-algebraic groups are assumed to be over k unless the contrary is indicated.

3. The induction principle

Let $1 \to N \to G \to H \to 1$ be an exact sequence of σ-algebraic groups over k. The principle alluded to in the title of this section is the statement that $\lim_{n\to\infty} H^1_{\sigma^n}(k, G_n) = 0$ if $\lim_{n\to\infty} H^1_{\sigma^n}(k, N_n) = 0$ and $\lim_{n\to\infty} H^1_{\sigma^n}(k, H_n) = 0$. The induction principle is crucial for the proof of (P3)⇒(P1) because, after decomposing a general σ-algebraic group into more manageable pieces, it allows us to restrict our considerations to those more manageable pieces. In this section we also show that (P1) and (P2) are equivalent and similarly, their uniform variants (P1^u) and (P2^u) are equivalent.

Throughout Section 3 we denote with k a σ-field (of arbitrary characteristic).

3.1. **From σ to σ^n.** In this subsection we introduce the σ^n-varieties X_n for every σ-variety X. Throughout this subsection we fix an integer $n \geq 1$. We use the prefix k-σ^n or σ^n instead of k-σ or σ to indicate that we are working over the difference field (k, σ^n) instead of (k, σ).

We need to be able to pass from k-σ-varieties to k-σ^n-varieties and vice versa. The most conceptual way to do this is to consider the left adjoint and the right adjoint of the functor $(R, \sigma) \rightsquigarrow (R, \sigma^n)$ from k-σ-algebras to k-σ^n-algebras which we will now construct. Let (S, τ) be a k-σ^n-algebra. We define

$$ {}_1S = S \otimes_k {}^{\sigma}S \otimes_k \ldots \otimes_k {}^{\sigma^{n-1}}S $$

and $\sigma\colon {}_1S \to {}_1S$ by

$$\sigma(a_0 \otimes (a_1 \otimes \lambda_1) \otimes \ldots \otimes (a_{n-1} \otimes \lambda_{n-1})) = \tau(a_{n-1})\sigma(\lambda_{n-1}) \otimes (a_0 \otimes 1) \otimes (a_1 \otimes \sigma(\lambda_1)) \otimes \ldots \otimes (a_{n-2} \otimes \sigma(\lambda_{n-2})),$$

where $a_0, \ldots, a_{n-1} \in S$ and $\lambda_1, \ldots, \lambda_{n-1} \in k$. Then ${}_1S$ is a k-σ-algebra and the inclusion into the first factor $S \to {}_1S$ is a morphism of k-σ^n-algebras. If R is a k-σ-algebra and ${}_1S \to R$ is a morphism of k-σ-algebras, then $S \to {}_1S \to R$ is a morphism of k-σ^n-algebras. Conversely, if $\psi\colon S \to R$ is a morphism of k-σ^n-algebras, then

$$ {}_1S \to R,\ a_0 \otimes (a_1 \otimes \lambda_1) \otimes \ldots \otimes (a_{n-1} \otimes \lambda_{n-1}) \mapsto \psi(a_0)\sigma(\psi(a_1))\lambda_1 \ldots \sigma^{n-1}(\psi(a_{n-1}))\lambda_{n-1} $$

is a morphism of k-σ-algebras. It is straight forward to check that these two constructions are inverse to each other. So

$$ \mathrm{Hom}_{k,\sigma^n}(S, R) \simeq \mathrm{Hom}_{k,\sigma}({}_1S, R) $$

for every k-σ-algebra R. Thus the functor $S \rightsquigarrow {}_1S$ (with the obvious definition on morphisms) is the left adjoint of $(R, \sigma) \rightsquigarrow (R, \sigma^n)$. (This is why the 1 is on the left side.)

Example 3.1. Consider the difference polynomial ring $S = k\{y\}_{\sigma^n} = k[y_1, \ldots, y_m, \sigma^n(y_1), \ldots, \sigma^n(y_m), \ldots]$ over the difference field (k, σ^n) in the σ^n-variables $y_1, \ldots, y_m$. Then ${}_1(k\{y\}_{\sigma^n})$ can be identified with $k\{y\}_\sigma$, the difference polynomial ring over (k, σ) in the σ-variables $y_1, \ldots, y_m$. The identification is such that for $1 \leq i \leq n-1$ and $1 \leq j \leq m$, the variable $\sigma^i(y_j) \in k\{y\}_\sigma$ corresponds to the image of $y_j \otimes 1 \in {}^{\sigma^i}S$ under the inclusion ${}^{\sigma^i}S \to {}_1S$.

More generally, if $S = k\{y\}_{\sigma^n}/[F]_{\sigma^n}$ is a quotient of $k\{y\}_{\sigma^n}$ by the σ^n-ideal $[F]_{\sigma^n}$ of $k\{y\}_{\sigma^n}$ σ^n-generated by $F \subseteq k\{y\}_{\sigma^n}$, then ${}_1S$ can be identified with $k\{y\}_\sigma/[F]_\sigma$, the quotient of $k\{y\}_\sigma$ by the σ-ideal generated by $F \subseteq k\{y\}_{\sigma^n} \subseteq k\{y\}_\sigma$.

Next we will construct the right adjoint of $(R, \sigma) \rightsquigarrow (R, \sigma^n)$. If S is any k-algebra, then we write ${}_{\sigma^i}S$ for the k-algebra that equals S as a ring and where we multiply with elements in k via $\sigma^i \colon k \to k$. In other words, ${}_{\sigma^i}S$ is obtained from S by restriction of scalars via $\sigma^i \colon k \to k$.

Let (S, τ) be a k-σ^n-algebra. We define

$$S_1 = {}_{\sigma^{n-1}}S \times {}_{\sigma^{n-2}}S \times \ldots \times {}_{\sigma}S \times S$$

as a k-algebra and we consider S_1 as a k-σ-algebra via

$$\sigma(a_1, a_2, \ldots, a_n) = (\tau(a_n), a_1, \ldots, a_{n-1}).$$

The projection $S_1 \to S$ onto the last factor is a morphism of k-σ^n-algebras. So if $R \to S_1$ is a morphism of k-σ-algebras, then $R \to S_1 \to S$ is a morphism of k-σ^n-algebras. Conversely, if $\psi \colon R \to S$ is a morphism of k-σ^n-algebras, then

$$R \to S_1, \ a \mapsto (\psi(\sigma^{n-1}(a)), \ldots, \psi(\sigma(a)), \psi(a))$$

is a morphism of k-σ-algebras. One can check that these two constructions are inverse to each other. So

$$\mathrm{Hom}_{k,\sigma^n}(R, S) \simeq \mathrm{Hom}_{k,\sigma}(R, S_1)$$

for every k-σ-algebra R. In other words, $S \rightsquigarrow S_1$ is the right adjoint of $(R, \sigma) \rightsquigarrow (R, \sigma^n)$. (This is why the one is on the right.) Note that with $k^{[n]}$ defined as on page 2, we have $k^{[n]} = (k, \sigma^n)_1$. More generally, for a k-σ-algebra R we define the k-σ-algebra $R^{[n]}$ by

$$R^{[n]} = (R, \sigma^n)_1 = {}_{\sigma^{n-1}}R \times \ldots \times R.$$

One can verify directly that for $l \geq 1$ the map

$$R^{[n]} \to R^{[nl]}, \ (a_1, \ldots, a_n) \mapsto (\sigma^{n(l-1)}(a_1), \ldots, \sigma^{n(l-1)}(a_n), \ldots, \sigma^n(a_1), \ldots, \sigma^n(a_n), a_1, \ldots, a_n)$$

is a morphism of k-σ-algebras.

If X is a k-σ-variety, then we can define a functor X_n from k-σ^n-algebras to sets by

$$X_n(S) = X(S_1)$$

for any k-σ^n-algebra S. Conversely, if Z is a k-σ^n-variety, then we can define a functor Z_1 from k-σ-algebras to sets by

$$Z_1(R) = Z(R, \sigma^n)$$

for any k-σ-algebra R.

Lemma 3.2.

(i) *If X is a k-σ-variety, then X_n is a k-σ^n-variety. Indeed, the σ^n-coordinate ring $k\{X_n\}$ of X_n is $(k\{X\}, \sigma^n)$.*

(ii) *If Z is a k-σ^n-variety, then Z_1 is a k-σ-variety. Indeed, $k\{Z_1\} = {}_1(k\{Z\})$.*

Proof. (i) For a k-σ^n-algebra S we have $X_n(S) = \mathrm{Hom}_{k,\sigma}(k\{X\}, S_1) = \mathrm{Hom}_{k,\sigma^n}(k\{X\}, S)$. As $(k\{X\}, \sigma)$ is finitely σ-generated, $(k\{X\}, \sigma^n)$ is finitely σ^n-generated. So X_n is indeed a k-σ^n-variety.

(ii) For a k-σ-algebra R we have $Z_1(R) = \mathrm{Hom}_{k,\sigma^n}(k\{Z\}, R) = \mathrm{Hom}_{k,\sigma}({}_1(k\{Z\}), R)$. As $k\{Z\}$ is finitely σ^n-generated, ${}_1(k\{Z\})$ is finitely σ-generated. So Z_1 is indeed a k-σ-variety. $\square$

So $X \rightsquigarrow X_n$ is a functor from the category of k-σ-varieties to the category of k-σ^n-varieties and $Z \rightsquigarrow Z_1$ is a functor from the category of k-σ^n-varieties to the category of k-σ-varieties. For a k-σ-variety X and a k-σ^n-variety Z we have

$$\mathrm{Hom}(X, Z_1) = \mathrm{Hom}_{k,\sigma}({}_1(k\{Z\}), k\{X\}) = \mathrm{Hom}_{k,\sigma^n}(k\{Z\}, k\{X\}) = \mathrm{Hom}(X_n, Z).$$

So the functors $X \rightsquigarrow X_n$ and $Z \rightsquigarrow Z_1$ are adjoint. Note that we can identify $(X_n)_m$ with X_{nm}, a fact that we will use frequently.

Example 3.3. Note that the σ-polynomial ring $k\{y\}_\sigma$ over k in the m σ-variables $y_1,\ldots,y_m$ is, as a k-σ^n-algebra, the σ^n-polynomial ring over (k,σ^n) in the nm σ^n-variables

$$(z_1,\ldots,z_{nm})=(y_1,\ldots,y_m,\sigma(y_1),\ldots,\sigma(y_m),\ldots,\sigma^{n-1}(y_1),\ldots,\sigma^{n-1}(y_m)).$$

We may therefore write $k\{y\}_\sigma=k\{z\}_{\sigma^n}$. Furthermore, if $F\subseteq k\{y\}$ σ-generates the σ-ideal I of $k\{y\}_\sigma$, then $F,\sigma(F),\ldots,\sigma^{n-1}(F)\subseteq k\{y\}_\sigma=k\{z\}_{\sigma^n}$ σ^n-generates the σ^n-ideal I of $k\{z\}_{\sigma^n}$. Thus, if X is the k-σ-variety defined by $F\subseteq k\{y\}_\sigma$, then X_n is the k-σ^n-variety defined by $F,\sigma(F),\ldots,\sigma^{n-1}(F)\subseteq k\{z\}_{\sigma^n}$.

For a concrete example, let us consider, as on page 2, the k-σ-variety $X=\{x\in \mathrm{GL}_m \mid \sigma(x)=(x^T)^{-1}A\}$, where $A\in\mathrm{GL}_m(k)$. As X is defined by $\sigma(x)-(x^T)^{-1}A=0$, X_2 is defined by $\sigma(x)-(x^T)^{-1}A=0$ and $\sigma^2(x)-(\sigma(x)^T)^{-1}\sigma(A)=0$, where x and $y=\sigma(x)$ are to be considered as σ^2-variables. Thus

$$\begin{aligned} X_2&=\{(x,y)\in\mathrm{GL}_m\times\mathrm{GL}_m \mid y=(x^T)^{-1}A,\ \sigma^2(x)=(y^T)^{-1}\sigma(A)\}\\ &\simeq\{x\in\mathrm{GL}_m\mid \sigma^2(x)=x(A^T)^{-1}\sigma(A)\}\end{aligned}$$

as claimed on page 2.

Example 3.4. If X comes from an affine variety $\mathcal{X}$ over k, then the σ^n-variety X_n corresponds to $\mathcal{X}\times{}^\sigma\mathcal{X}\times\ldots\times{}^{\sigma^{n-1}}\mathcal{X}$. In other words,

$$([\sigma]_k\mathcal{X})_n\simeq[\sigma^n]_k(\mathcal{X}\times\ldots\times{}^{\sigma^{n-1}}\mathcal{X}).$$

Proof. This follows from Example 3.3 but can also be seen in a more functorial fashion as follows: For every k-σ^n-algebra S we have

$$\begin{aligned}([\sigma]_k\mathcal{X})_n(S)&=\mathcal{X}({}_{\sigma^{n-1}}S\times\ldots\times S)\simeq\mathrm{Hom}_k(k[\mathcal{X}],{}_{\sigma^{n-1}}S\times\ldots\times S)\\ &\simeq\mathrm{Hom}_k(k[\mathcal{X}],{}_{\sigma^{n-1}}S)\times\ldots\times\mathrm{Hom}_k(k[\mathcal{X}],S)\\ &\simeq\mathrm{Hom}_k({}^{\sigma^{n-1}}(k[\mathcal{X}]),S)\times\ldots\times\mathrm{Hom}_k(k[\mathcal{X}],S)\\ &=\mathrm{Hom}_k({}^{\sigma^{n-1}}(k[\mathcal{X}])\otimes_k\ldots\otimes_k k[\mathcal{X}],S)\simeq(\mathcal{X}\times\ldots\times{}^{\sigma^{n-1}}\mathcal{X})(S).\end{aligned}$$

□

Example 3.5. If Z is the k-σ^n-variety defined by $F\subseteq k\{y\}_{\sigma^n}$. Then Z_1 is the k-σ-variety defined by $F\subseteq k\{y\}_{\sigma^n}\subseteq k\{y\}_\sigma$. Cf. Example 3.1. Thus, concretely, to compute Z_1 from Z we simply have to interpret the defining σ^n-equations of Z as σ-equations.

Remark 3.6. *Let X be a k-σ-variety. We have $X(k^{[n]})\neq\emptyset$ if and only if $X_n(k)\neq\emptyset$.*

Proof. In fact, $X_n(k)=X(k^{[n]})$. □

If G is a σ-algebraic group and X a G-torsor, then G_n is a σ^n-algebraic group and X_n is a G_n-torsor. Remark 3.6 then shows that $X(k^{[n]})\neq\emptyset$ if and only if X_n is trivial.

The following three lemmas relate properties of the σ-algebraic group G to properties of the σ^n-algebraic group G_n.

Lemma 3.7. *Let G be a σ-algebraic group over k. If G is connected, then G_n is connected.*

Proof. Recall (e.g., from [Wib21, Lemma 6.7]) that G is connected if and only if $\pi_0(k\{G\})=k$. As $\pi_0(k\{G\})$ does not depend on σ the claim follows. □

Lemma 3.8. *Let G be a σ-algebraic group over k. Then $\sigma^n\text{-}\dim(G_n)=\sigma\text{-}\dim(G)\cdot n$ and $\mathrm{ord}(G_n)=\mathrm{ord}(G)$.*

Proof. We consider G as a Zariski-dense, σ-closed subgroup of some algebraic group $\mathcal{G}$ via a σ-closed embedding $G\hookrightarrow\mathcal{G}$. Algebraically this means that we have an inclusion of Hopf algebras $k[\mathcal{G}]\subseteq k\{G\}$ such that $k[\mathcal{G}]$ generates $k\{G\}$ as a k-σ-algebra. In particular, if B is a finite subset of $k[\mathcal{G}]$ such that $k[\mathcal{G}]=k[B]$, then $k\{G\}=k\{B\}$.

The σ-closed embedding $G\hookrightarrow[\sigma]_k\mathcal{G}$ yields a σ^n-closed embedding $G_n\hookrightarrow([\sigma]_k\mathcal{G})_n=[\sigma^n]_k(\mathcal{G}\times\ldots\times{}^{\sigma^{n-1}}\mathcal{G}$ (Example 3.4). So we can consider G_n as a σ^n-closed subgroup of the algebraic group $\mathcal{G}\times{}^\sigma\mathcal{G}\times\ldots\times{}^{\sigma^{n-1}}\mathcal{G}$. Algebraically, this corresponds to the inclusion of Hopf algebras $k[B,\ldots,\sigma^{n-1}(B)]\subseteq$

$k\{G\}$. For $i \geq 0$ let $d_i = \dim(k[B, \ldots, \sigma^i(B)])$. Then, for $i \gg 0$, we have $d_i = \sigma\text{-}\dim(G)(i+1) + e$ for some integer $e \geq 0$.

Similarly, for $i \gg 0$, we have $d_{(i+1)n-1} = \sigma^n\text{-}\dim(G_n)(i+1) + e'$ for some integer $e' \geq 0$. Therefore

$$\sigma\text{-}\dim(G)((i+1)n) + e = \sigma^n\text{-}\dim(G_n)(i+1) + e'$$

and thus σ^n-$\dim(G_n) = \sigma\text{-}\dim(G) \cdot n$. Moreover, $\sigma\text{-}\dim(G) = 0$ if and only if σ^n-$\dim(G_n) = 0$ and in this case $e = e'$, i.e., $\operatorname{ord}(G) = \operatorname{ord}(G_n)$. □

Lemma 3.9. *If $1 \to N \to G \to H \to 1$ is an exact sequence of σ-algebaic groups, then $1 \to N_n \to G_n \to H_n \to 1$ is an exact sequence of σ^n-algebraic groups for every $n \geq 1$.*

Proof. The exactness of $1 \to N \to G \to H \to 1$ can be reformulated in terms of the corresponding morphisms $k\{H\} \to k\{G\} \to k\{N\}$ of k-σ-Hopf algebras. Exactness at N means that $k\{G\} \to k\{N\}$ is surjective, exactness at H means that $k\{H\} \to k\{G\}$ is injective and exactness at G means that the kernel of $k\{G\} \to k\{N\}$ agrees with the ideal of $k\{G\}$ generated by the image of $\mathfrak{m}_H$ in $k\{G\}$, where $\mathfrak{m}_H$ is the kernel of the counit $k\{H\} \to k$. These properties do not depend on the power of σ considered. Thus $1 \to N_n \to G_n \to H_n \to 1$ is exact. □

3.2. **Exact sequences and H^1.** In this subsection we establish the induction principle. We also observe that (P1)$\Leftrightarrow$(P2) and (P1^u)$\Leftrightarrow$(P2^u).

Let G be a σ-algebraic group over k. A cohomology set $H^1(k, G)$ that classifies G-torsors was introduced in [BW22]. Far more general and elaborate approaches to cohomology in difference algebraic geometry can be found in [Tom] and [CK23]. For our purposes, the elementary approach from [BW22] is sufficient.

We begin by recalling the definition of the cohomology set $H^1(A/k, G)$, which, for a k-σ-algebra A, classifies G-torsors X with $X(A) \neq \emptyset$. The morphisms of k-σ-algebras

$$A \rightrightarrows A \otimes_k A \mathrel{\substack{\longrightarrow\\[-1ex]\longrightarrow\\[-1ex]\longrightarrow}} A \otimes_k A \otimes_k A$$

induce morphisms of groups

$$G(A) \underset{\delta_2}{\overset{\delta_1}{\rightrightarrows}} G(A \otimes_k A) \underset{\partial_3}{\overset{\partial_1}{\mathrel{\substack{\longrightarrow\\[-1ex]\xrightarrow{\partial_2}\\[-1ex]\longrightarrow}}}} G(A \otimes_k A \otimes_k A),$$

where δ_1 is induced from $a \mapsto 1 \otimes a$, δ_2 is induced from $a \mapsto a \otimes 1$, ∂_1 is induced from $a \otimes b \mapsto 1 \otimes a \otimes b$ and so on.

An element $\chi \in G(A \otimes_k A)$ is called a *cocycle* if $\partial_2(\chi) = \partial_1(\chi)\partial_3(\chi)$. Two cocycles χ_1 and χ_2 are called equivalent if there exists a $g \in G(A)$ such that $\chi_1 = \delta_1(g)\chi_2\delta_2(g)^{-1}$. The set of all equivalence classes of cocycles is denoted by $H^1_\sigma(A/k, G)$. It is a pointed set with the usual functorial properties. The distinguished element is the equivalence class of $1 \in G(A \otimes_k A)$.

We set $H^1_\sigma(k, G) = \varinjlim H^1_\sigma(A/k, G)$, where the limit is taken over the set of isomorphism classes of finitely σ-generated k-σ-algebras. (See [BW22, Section 5] for more details.) Let $\Sigma_\sigma(G)$ denote the pointed set of all isomorphism classes of G-torsors. The distinguished element in $\Sigma_\sigma(G)$ is the class of the trivial torsor. According to [BW22, Theorem 4.2] we have an isomorphism of pointed sets

$$\Sigma_\sigma(G) \simeq H^1_\sigma(k, G).$$

Fix $n \geq 1$. If X is a G-torsor, then X_n is a G_n-torsor. As $X(k) \subseteq X(k^{[n]}) = X_n(k)$, we see that X_n is trivial if X is trivial. Thus we have a map of pointed sets

$$\Sigma_\sigma(G) \to \Sigma_{\sigma^n}(G_n).$$

Example 3.10. Let $G = \{g \in \mathrm{GL}_m \mid \sigma(g) = (g^T)^{-1}\}$. For every $A \in \mathrm{GL}_m(k)$ the k-σ-variety $X = \{x \in \mathrm{GL}_m \mid \sigma(x) = (x^T)^{-1}A\}$ is a G-torsor under left multiplication. We have $G_2 = \{g \in \mathrm{GL}_m \mid \sigma^2(g) = g\}$ and $X_2 = \{x \in \mathrm{GL}_m \mid \sigma^2(x) = x(A^T)^{-1}\sigma(A)\}$. See Example 3.3.

We also have a canonical map

$$H^1_\sigma(k, G) \to H^1_{\sigma^n}(k, G_n),$$

which we will describe next. Let X be a k-σ-variety and A a k-σ-algebra. The morphism $A \to A^{[n]}$, $a \mapsto (\sigma^{n-1}(a), \ldots, a)$ of k-σ-algebras induces a map $X(A) \to X(A^{[n]}) = X((A, \sigma^n)_1) = X_n(A)$. Under the identifications $X(A) = \mathrm{Hom}_{k,\sigma}(k\{X\}, A)$ and $X_n(A) = \mathrm{Hom}_{k,\sigma^n}(k\{X\}, A)$, this map is simply interpreting a morphism $k\{X\} \to A$ of k-σ-algebras as a morphism of k-σ^n-algebras.

If $A \to B$ is a morphism of k-σ-algebras, then

$$\begin{tikzcd} X(A) \arrow[r] \arrow[d] & X_n(A) \arrow[d] \\ X(B) \arrow[r] & X_n(B) \end{tikzcd}$$

commutes. Similarly, if $X \to Y$ is a morphism of k-σ-varieties, then

$$\begin{tikzcd} X(A) \arrow[r] \arrow[d] & X_n(A) \arrow[d] \\ Y(A) \arrow[r] & Y_n(A) \end{tikzcd} \tag{1}$$

commutes. Moreover, if G is a σ-algebraic group over k, then $G(A) \to G_n(A)$ is a morphism of groups. The commutative diagram

$$\begin{tikzcd} G(A) \arrow[r, shift left] \arrow[r, shift right] \arrow[d] & G(A \otimes_k A) \arrow[r, shift left=2] \arrow[r] \arrow[r, shift right=2] \arrow[d] & G(A \otimes_k A \otimes_k A) \arrow[d] \\ G_n(A) \arrow[r, shift left] \arrow[r, shift right] & G_n(A \otimes_k A) \arrow[r, shift left=2] \arrow[r] \arrow[r, shift right=2] & G_n(A \otimes_k A \otimes_k A) \end{tikzcd}$$

shows that $G(A \otimes_k A) \to G_n(A \otimes_k A)$ maps cocycles to cocycles and equivalent cocycles to equivalent cocycles. We therefore have a well-defined map $H^1_\sigma(A/k, G) \to H^1_{\sigma^n}(A/k, G_n)$, which we may compose with the inclusion $H^1_{\sigma^n}(A/k, G_n) \to H^1_{\sigma^n}(k, G_n)$. If $A \to B$ is a morphism of k-σ-algebras, then

$$\begin{tikzcd} H^1_\sigma(A/k, G) \arrow[dd] \arrow[dr] & \\ & H^1_{\sigma^n}(k, G_n) \\ H^1_\sigma(B/k, G) \arrow[ur] & \end{tikzcd}$$

commutes. Thus we have an induced map of pointed sets $H^1_\sigma(k, G) \to H^1_{\sigma^n}(k, G_n)$. The construction of this map also applies with (k, σ) replaced by (k, σ^d) (for some $d \geq 1$) and so we have maps $H^1_{\sigma^d}(k, G_d) \to H^1_{(\sigma^d)^n}(k, (G_d)_n) = H^1_{\sigma^{dn}}(k, G_{dn})$. If X is a k-σ^n-variety, (A, τ) a k-σ^n-algebra and $d, d' \geq 1$, then the composition $X(A, \tau) \to X_d(A, \tau^d) \to (X_d)_{d'}(A, (\tau^d)^{d'}) = X_{dd'}(A, \tau^{dd'})$ agrees with $X(A, \tau) \to X_{dd'}(A, \tau^{dd'})$ because all maps are just reinterpreting the same morphism from $X(A, \tau) = \mathrm{Hom}_{k,\sigma^n}(k\{X\}, A)$. From this it follows that for integers $n, n', n'' \geq 1$ with $n|n'$ and $n'|n''$, the composition $H^1_{\sigma^n}(k, G_n) \to H^1_{\sigma^{n'}}(k, G_{n'}) \to H^1_{\sigma^{n''}}(k, G_{n''})$ agress with $H^1_{\sigma^n}(k, G_n) \to H^1_{\sigma^{n''}}(k, G_{n''})$. The maps $H^1_{\sigma^n}(k, G_n) \to H^1_{\sigma^{n'}}(k, G_{n'})$ for $n|n'$ thus form a directed system over the directed set of all integers greater or equal to one, partially ordered by $n \leq n'$ if and only if $n|n'$. We can therefore consider the direct limit $\varinjlim_{n\to\infty} H^1_{\sigma^n}(k, G_n)$.

Example 3.11. Let $\mathcal{G}$ be an algebraic group over k and $G = [\sigma]_k\mathcal{G}$. By [BW22, Prop. 3.5] we have $H^1_\sigma(k, G) = H^1(k, \mathcal{G})$. Furthermore $G_n = [\sigma^n]_k(\mathcal{G} \times \ldots \times {}^{\sigma^{n-1}}\mathcal{G})$ (Example 3.4) and so $H^1_{\sigma^n}(k, G_n) = H^1(k, \mathcal{G} \times \ldots \times {}^{\sigma^{n-1}}\mathcal{G}) = H^1(k, \mathcal{G}) \times \ldots \times H^1(k, {}^{\sigma^{n-1}}\mathcal{G})$. To understand the maps $H^1_{\sigma^n}(k, G_n) \to H^1_{\sigma^{n'}}(k, G_{n'})$ for $n|n'$, we first need an explicit description of the map $X_n(A, \tau) \to (X_n)_d(A, \tau^d)$ for $d \geq 1$, X a k-σ^n-variety and (A, τ) a k-σ^n-algebra. Now $X_n(A, \tau) \to (X_n)_d(A, \tau^d) = X_n((A, \tau)^{[d]})$ is obtained by applying the functor X_n to the morphism $(A,\tau)\to(A,\tau)^{[d]}$ of k-σ^n-algebras. As $X_n(A,\tau)=X((A,\tau)_1)$, this means that we need to apply the functor X to the morphism $(A,\tau)_1\to((A,\tau)^{[d]})_1$ of k-σ-algebras. As

$$(A,\tau)\to(A,\tau)^{[d]}={}_{(\sigma^n)^{d-1}}A\times\ldots\times{}_{\sigma^n}A\times A,\quad a\mapsto(\tau^{d-1}(a),\ldots,\tau(a),a),$$

we see that

$$(A,\tau)_1={}_{\sigma^{n-1}}A\times\ldots\times A\longrightarrow((A,\tau)^{[d]})_1={}_{\sigma^n}({}_{(\sigma^{n(d-1)}}A\times\ldots\times A)\times\ldots\times{}_{\sigma^{n(d-1)}}A\times\ldots\times A$$

is given by

$$(a_1,\ldots,a_n)\longmapsto(\tau^{d-1}(a_1),\ldots,a_1,\ldots,\tau^{d-1}(a_n)\ldots,a_n).$$

Thus, after reordering the factors as ${}_{\sigma^{nd-1}}A\times\ldots\times{}_{\sigma}A\times A$, the map is given by

$$(a_1,\ldots,a_n)\mapsto(\tau^{d-1}(a_1),\ldots,\tau^{d-1}(a_n),\ldots,a_1,\ldots,a_n).$$

Applying $X=[\sigma]_k\mathcal{G}$ to this (as in Example 3.4), we find the map

$$\begin{aligned}\mathcal{G}(A)\times\ldots\times{}^{\sigma^{n-1}}\mathcal{G}(A)&\longrightarrow\mathcal{G}(A)\times\ldots\times{}^{\sigma^{nd-1}}\mathcal{G}(A),\\ (g_1,\ldots,g_n)&\longmapsto(g_1,\ldots,g_n,\ldots,\tau^{d-1}(g_1),\ldots,\tau^{d-1}(g_n)),\end{aligned}\tag{2}$$

where $\tau^j\colon{}^{\sigma^i}\mathcal{G}(A)\to{}^{\sigma^{i+n}}\mathcal{G}(A)$ (for $0\leq i\leq n-1$ and $1\leq j\leq d-1$) is given by applying τ to the coordinates. Without coordinates, if $g\colon{}^{\sigma^i}(k[\mathcal{G}])\to A$, then $\tau^j(g)\colon{}^{\sigma^n}({}^{\sigma^i}(k[G]))\to A,\ f\otimes\lambda\mapsto\tau^j(g(f))\lambda$.

If $k\to k'$ is a morphism of fields, we have a map $H^1(k,\mathcal{G})\to H^1(k',\mathcal{G}_{k'})$, which on isomorphism classes of torsors corresponds to base change. Applying this with $\sigma^n\colon k\to k$, we obtain maps $\sigma^n\colon H^1(k,{}^{\sigma^i}\mathcal{G})\to H^1(k,{}^{\sigma^{i+n}}\mathcal{G})$.

Base change via $\sigma^n\colon k\to k$ takes $g\colon{}^{\sigma^i}(k[\mathcal{G}])\to A$ and returns ${}^{\sigma^n}g\colon{}^{\sigma^{i+n}}(k[\mathcal{G}])\to{}^{\sigma^n}A$. The map $\tau^j(g)\colon{}^{\sigma^{i+n}}(k[\mathcal{G}])\to A$ is then obtained from ${}^{\sigma^n}g$ by composing with the morphism ${}^{\sigma^n}A\to A,\ a\otimes\lambda\mapsto\tau(a)\lambda$ of k-algebras. Since a morphism of k-algebras does not matter when we pass to cohomology sets, we see that $\tau^j\colon{}^{\sigma^i}\mathcal{G}(A)\to{}^{\sigma^{i+n}}\mathcal{G}(A)$ induces $\sigma^n\colon H^1(k,{}^{\sigma^i}\mathcal{G})\to H^1(k,{}^{\sigma^{i+n}}\mathcal{G})$.

Based on (2), we thus find that for $n|n'$, the map

$$H^1_{\sigma^n}(k,G_n)=H^1(k,\mathcal{G})\times\ldots\times H^1(k,{}^{\sigma^{n-1}}\mathcal{G})\longrightarrow H^1_{\sigma^{n'}}(k,G_{n'})=H^1(k,\mathcal{G})\times\ldots\times H^1(k,{}^{\sigma^{n'-1}}\mathcal{G})$$

is given by

$$(a_1,\ldots,a_n)\longmapsto(a_1,\ldots,a_n,\sigma^n(a_1),\ldots,\sigma^n(a_n),\ldots,\sigma^{n'-n}(a_1),\ldots,\sigma^{n'-n}(a_n)).$$

Therefore the limit $\lim\limits_{n\to\infty}H^1_{\sigma^n}(k,G_n)$ can be identified with the set of all "periodic" elements of $\prod_{n\geq1}H^1(k,{}^{\sigma^n}\mathcal{G})$, i.e., all elements of the form $(a_1,\ldots,a_n,\sigma^n(a_1),\ldots,\sigma^n(a_n),\sigma^{2n}(a_1),\ldots,\sigma^{2n}(a_n),\ldots)$ for some $n\geq1$.

We will need two more commutative diagrams.

Lemma 3.12. *Let G be a σ-algebraic group over k. Then*

$$\begin{tikzcd}\Sigma_\sigma(G)\arrow[r]\arrow[d] & \Sigma_{\sigma^n}(G_n)\arrow[d]\\ H^1_\sigma(k,G)\arrow[r] & H^1_{\sigma^n}(k,G_n)\end{tikzcd}$$

commutes.

Proof. Let X be a G-torsor and A a finitely σ-generated k-σ-algebra such that $X(A)\neq\emptyset$. Choose $x\in X(A)$. The corresponding cocycle $\chi\in G(A\otimes_kA)$ is determined by $f_1(x)=\chi.f_2(x)$, where $f_1,f_2\colon X(A)\to X(A\otimes_kA)$. (See the proof of [BW22, Theorem 4.1].) Under $G(A\otimes_kA)\to G_n(A\otimes_kA)$ the cocycle χ maps to the unique cocycle $\widetilde{\chi}\in G_n(A\otimes_kA)$ that satisfies $f_1(\widetilde{x})=\widetilde{\chi}.f_2(\widetilde{x})$, where $\widetilde{x}$ is the image of x under $X(A)\to X_n(A)$.

On the other hand, for the G_n-torsor X_n we have $\widetilde{x}\in X_n(A)$ and so the corresponding cocycle in $G_n(A\otimes_kA)$ is exactly $\widetilde{\chi}$. Now the claim follows by taking equivalence classes and passing to the limit. $\square$

Example 3.13. The map $H^1_\sigma(k,G)\to H^1_{\sigma^n}(k,G_n)$ is in general neither injective nor surjective, i.e., there may exist a G_n-torsor that does not come from a G-torsor and there may be two non-isomorphic G-torsors that become isomorphic as G_n-torsors. For a non-surjective example see Example 3.11. For a non-injective example consider the σ-algebraic group $G=\{g\in\mathbb{G}_m|\ g^2=1,\ \sigma(g)=g\}$ and the G-torsor $X=\{x\in\mathbb{G}_m|\ x^2=1,\ \sigma(x)=-x\}$ (under left multiplication). Then X is non-trivial but X_2 is trivial because $X_2(k)=X(k^{[2]})\neq\emptyset$.

Lemma 3.14. *Let $G\to H$ be a morphism of σ-algebraic groups over k. Then*

$$\begin{array}{ccc} H^1_\sigma(k,G) & \longrightarrow & H^1_\sigma(k,H) \\ \downarrow & & \downarrow \\ H^1_{\sigma^n}(k,G_n) & \longrightarrow & H^1_{\sigma^n}(k,H_n) \end{array}$$

commutes.

Proof. This follows from the commutativity of (1). □

Definition 3.15. *Let G be a σ-algebraic group over k. To simplify our statements we call k*

- G-trivial *if for every G-torsor X, there exists an integer $n\geq 1$ such that $X(k^{[n]})\neq\emptyset$. If in addition the integer n can be chosen uniformly for all X, then we call k* uniformly G-trivial.
- *(uniformly)* strongly G-trivial *if (k,σ^n) is (uniformly) G_n-trivial for all $n\geq 1$.*

Thus k is uniformly strongly G-trivial if for every $n\geq 1$ and every σ-algebraic group G over k, there exists a $d\geq 1$ such that for every G_n-torsor we have $X((k,\sigma^n)^{[d]})=X((k,(\sigma^n)^d)_1)=X_d(k,(\sigma^n)^d)\neq\emptyset$. The notion of being (uniformly) strongly G-trivial is important for making the induction principle work.

Property property (P1) means that k is G-trivial for every σ-algebraic group G over k, while (P1^u) means that k is uniformly G-trivial for every σ-algebraic group G over k. The following lemma is needed for (P1)⇒(P2).

Lemma 3.16. *If k is G-trivial for every σ-algebraic group G over k, then k is strongly G-trivial for every σ-algebraic group G over k.*

Proof. Let G be a σ-algebraic group over k and let X be a G_n-torsor for some $n\geq 1$. Then X_1 is a $(G_n)_1$-torsor and by assumption there exists a $d\geq 1$ such that $X_1(k^{[d]})\neq\emptyset$. As $X_1(k^{[d]})=X(k^{[d]},\sigma^n)$ there exists a morphism $k\{X\}\to k^{[d]}$ of k-σ^n-algebras. The projection $k^{[d]}\to k$ to the last factor is a morphism of k-σ^d-algebras. Thus the composition $k\{X\}\to k^{[d]}\to k$ is a morphism of k-σ^{nd}-algebras. Therefore $X_d(k,(\sigma^n)^d)=X((k,(\sigma^n)^d)_1)=X((k,\sigma^n)^{[d]})\neq\emptyset$ as desired. □

The following lemma will allow us to pass to higher powers of σ in the proof of (P3)⇒(P1).

Lemma 3.17. *Let G be a σ-algebraic group over k. If (k,σ^n) is (strongly) G_n-trivial, then k is (strongly) G-trivial.*

Proof. Assume that (k,σ^n) is G_n-trivial and let X be a G-torsor. Then X_n is a G_n-torsor, so there exists an integer $d\geq 1$ with $(X_n)_d(k)\neq\emptyset$ (Remark 3.6). Define $m=nd$. As $(X_n)_d=X_m$ we have $X_m(k)\neq\emptyset$ and thus $X(k^{[m]})\neq\emptyset$ (Remark 3.6). We conclude that k is G-trivial.

If (k,σ^n) is strongly G_n-trivial, then $(k,(\sigma^n)^d)$ is $(G_n)_d$-trivial for every integer $d\geq 1$. In other words, $(k,(\sigma^d)^n)$ is $(G_d)_n$-trivial for every integer $d\geq 1$. By the statement proven in the first paragraph, (k,σ^d) is G_d-trivial for every $d\geq 1$. Hence k is strongly G-trivial. □

Lemma 3.18. *Let G be a σ-algebraic group over k, X a G_n-torsor and $d\geq 1$. Then $X((k,\sigma^n)^{[d]})\neq\emptyset$ if and only if the image of X in $H^1_{\sigma^n}(k,G_n)$ maps to the distinguished element under $H^1_{\sigma^n}(k,G)\to H^1_{\sigma^{nd}}(k,G_{nd})$.*

Proof. We have $X((k,\sigma^n)^{[d]})\neq\emptyset$ if and only if $X_d(k,(\sigma^n)^d)\neq\emptyset$ by Remark 3.6. So the claim follows from Lemma 3.12. □

At this point the equivalence of (P1) and (P2) is self-evident:

Proposition 3.19. *Properties* (P1) *and* (P2) *are equivalent. Similarly, properties* (P1^u) *and* (P2^u) *are equivalent.*

Proof. The equivalence (P1^u)$\Leftrightarrow$(P2^u) follows from Lemma 3.18. According to that lemma, property (P2) means that k is strongly G-trivial for every σ-algebraic group G over k. Thus (P1)$\Leftrightarrow$(P2) follows from Lemma 3.16. $\square$

We are now prepared to establish the induction principle. Essentially this is an application of the exact cohomology sequence. Recall that a sequence $M' \to M \to M''$ of pointed sets is exact at M if the kernel of $M \to M''$ (i.e., the inverse image of the distinguished element of M'') agrees with the image of $M' \to M$.

Proposition 3.20 (Induction principle)**.** *Let $1 \to N \to G \to H \to 1$ be an exact sequence of σ-algebraic groups over k.*

(i) *If k is (uniformly) H-trivial and (uniformly) strongly N-trivial, then k is (uniformly) G-trivial.*
(ii) *If k is (uniformly) strongly N-trivial and (uniformly) strongly H-trivial, then k is (uniformly) strongly G-trivial.*

Proof. According to Lemma 3.14 we have a commutative diagram for all integers $n, m, l \geq 1$:

$$\begin{tikzcd}
 & H^1_{\sigma^n}(k, G_n) \arrow[r] \arrow[d, "\alpha"] & H^1_{\sigma^n}(k, H_n) \arrow[d] \\
H^1_{\sigma^{nm}}(k, N_{nm}) \arrow[r] \arrow[d] & H^1_{\sigma^{nm}}(k, G_{nm}) \arrow[r] \arrow[d, "\beta"] & H^1_{\sigma^{nm}}(k, H_{nm}) \\
H^1_{\sigma^{nml}}(k, N_{nml}) \arrow[r] & H^1_{\sigma^{nml}}(k, G_{nml}) &
\end{tikzcd}$$

We prove (i) and (ii) simultaneously and set $n = 1$ in case (i) and $n \geq 1$ arbitrary in case (ii). Because $1 \to N_{nm} \to G_{nm} \to H_{nm} \to 1$ is exact by Lemma 3.9, the exact cohomology sequence ([BW22, Prop. 5.6]) shows that the middle row in the above diagram is exact.

Start with an element in $\gamma \in H^1_{\sigma^n}(k, G_n)$. As k is (strongly) H-trivial, there exists an $m \geq 1$ such that its image in $H^1_{\sigma^n}(k, H_n)$ lies in the kernel of the vertical map $H^1_{\sigma^n}(k, H_n) \to H^1_{\sigma^{nm}}(k, H_{nm})$. Moreover, m can be chosen uniformly for all elements in $H^1_{\sigma^n}(k, G_n)$ if k is uniformly (strongly) H-trivial. By the exactness of the middle row, $\alpha(\gamma)$ is contained in the image of $H^1_{\sigma^{nm}}(k, N_{nm}) \to H^1_{\sigma^{nm}}(k, G_{nm})$. Since k is strongly N-trivial, there exists an $l \geq 1$ such that its preimage in $H^1_{\sigma^{nm}}(k, N_{nm})$ is mapped to the trivial element in $H^1_{\sigma^{nml}}(k, N_{nml})$ and we conclude that $\beta(\alpha(\gamma))$ is trivial. Moreover, if N is uniformly strongly N-trivial, then l does not depend on the choice of γ. All claims now follow with Lemma 3.18. $\square$

By induction we obtain from Proposition 3.20 (ii):

Corollary 3.21. *If a σ-algebraic group G has a subnormal series*

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = 1$$

such that k is (uniformly) strongly G_i/G_{i+1}-trivial for $i = 0, \ldots, n-1$, then k is (uniformly) strongly G-trivial. $\square$

4. First observations regarding property (P3)

In this section we discuss some equivalent reformulations of property (P3) (b) (and (P3^u) (b)). We also show that (P1)$\Rightarrow$(P3) and similarly (P1^u)$\Rightarrow$(P3^u).

Throughout Section 4 we denote with k a σ-field (of arbitrary characteristic).

Lemma 4.1. *For given integers $m, d \geq 1$ and an algebraic group $\mathcal{G} \leq \mathrm{GL}_m$ defined over $\mathbb{Q}$ the following are equivalent for every $A \in \mathcal{G}(k)$:*

(i) *There exists an integer $n \geq 1$ and an element $Y \in \mathcal{G}(k^{[n]})$ such that $\sigma^d(Y) = AY$.*
(ii) *There exists an integer $l \geq 1$ and an element $Y \in \mathcal{G}(k)$ such that $\sigma^{dl}(Y) = \sigma^{(l-1)d}(A) \ldots \sigma^d(A)AY$.*

Moreover, n can be chosen uniformly for all $A \in \mathcal{G}(k)$ if and only if l can be chosen uniformly for all $A \in \mathcal{G}(k)$.

Proof. Let us first show that (i) implies (ii). Finding a solution in $k^{[n]}$ for some set of difference equations is equivalent to finding a morphism of k-σ-algebras $R \to k^{[n]}$ for some appropriate k-σ-algebra R. If $n|\tilde{n}$, say $\tilde{n} = nl$, then we have a morphism of k-σ-algebras

$$k^{[n]} \to k^{[\tilde{n}]},\ (a_1, \dots, a_n) \mapsto (\sigma^{n(l-1)}(a_1), \dots, \sigma^{n(l-1)}(a_n), \dots, \sigma^n(a_1), \dots, \sigma^n(a_n), a_1, \dots, a_n).$$

We can therefore assume that $d|n$, say $n = dl$. By assumption, there exists a $Y \in \mathcal{G}(k^{[n]})$ with $\sigma^d(Y) = AY$, and thus $\sigma^{dl}(Y) = \sigma^{(l-1)d}(A) \dots \sigma^d(A)AY$. The projection $k^{[n]} \to k$ onto the last factor is a morphism of k-σ^n-algebras. Therefore the equation $\sigma^{dl}(Y) = \sigma^{(l-1)d}(A) \dots \sigma^d(A)AY$ has a solution in $\mathcal{G}(k)$.

Next we will show that (ii) implies (i). Let $Z \in \mathcal{G}(k)$ be a solution to $\sigma^{dl}(Y) = \sigma^{(l-1)d}(A) \dots \sigma^d(A)AY$. Then

$$Z' = (\sigma^{d-1}(\sigma^{(l-2)d}(A) \dots AZ), \dots, \sigma^{(l-2)d}(A) \dots AZ, \dots \dots, \sigma^{d-1}(AZ), \dots, AZ, \sigma^{d-1}(Z), \dots, Z) \in \mathcal{G}(k^{[n]})$$

is a solution to $\sigma^d(Y) = AY$, where $n = dl$.

Note that if n does not depend on A, then l does not depend on A and vice versa, so the second statement also holds. □

Lemma 4.2. *Condition* (P3) *(b) is equivalent to each of the following statements:*

- (P3) (b') *For every $m \geq 1$ and for every $A \in \mathrm{GL}_m(k)$ there exists an $l \geq 1$ such that the equation $\sigma^l(Y) = \sigma^{(l-1)}(A) \cdots \sigma(A)AY$ has a solution in $\mathrm{GL}_m(k)$.*
- (P3) (b_d) *For every $m \geq 1$ and every $d \geq 1$ and for every $A \in \mathrm{GL}_m(k)$ there exists an integer $n \geq 1$ such that the equation $\sigma^d(Y) = AY$ has a solution in $\mathrm{GL}_m(k^{[n]})$.*
- (P3) (b_d') *For every $m \geq 1$ and $d \geq 1$ and for every $A \in \mathrm{GL}_m(k)$ there exists an $l \geq 1$ such that the equation $\sigma^{dl}(Y) = \sigma^{(l-1)d}(A) \dots \sigma^d(A)AY$ has a solution in $\mathrm{GL}_m(k)$.*

Similarly, Condition ($\mathrm{P3}^u$) (b) is equivalent to each of the following statements:

- ($\mathrm{P3}^u$) (b') For every $m \geq 1$ there exists an $l \geq 1$ such that for every $A \in \mathrm{GL}_m(k)$ the equation $\sigma^l(Y) = \sigma^{(l-1)}(A) \cdots \sigma(A)AY$ has a solution in $\mathrm{GL}_m(k)$.
- ($\mathrm{P3}^u$) (b_d) For every $m \geq 1$ and every $d \geq 1$, there exists an $n \geq 1$ such that for every $A \in \mathrm{GL}_m(k)$ the equation $\sigma^d(Y) = AY$ has a solution in $\mathrm{GL}_m(k^{[n]})$.
- ($\mathrm{P3}^u$) (b_d') For every $m \geq 1$ and $d \geq 1$ there exists an $l \geq 1$ such that for every $A \in \mathrm{GL}_m(k)$ the equation $\sigma^{dl}(Y) = \sigma^{(l-1)d}(A) \dots \sigma^d(A)AY$ has a solution in $\mathrm{GL}_m(k)$.

Proof. The equivalence of (b) and (b') follows (in both cases (P3) and ($\mathrm{P3}^u$)) from Lemma 4.1 with $\mathcal{G} = \mathrm{GL}_m$ and $d = 1$. Similarly, the equivalence of (b_d) and (b_d') follows from Lemma 4.1 with $\mathcal{G} = \mathrm{GL}_m$ in both cases. So it remains to show that (b') implies (b_d') in both cases. We start with the ($\mathrm{P3}^u$) case and assume that ($\mathrm{P3}^u$) (b') holds and fix integers $m, d \geq 1$. Then by ($\mathrm{P3}^u$) (b'), there exists an integer l_d such that for every $B \in \mathrm{GL}_{md}(k)$, there exists a $Z \in \mathrm{GL}_{md}(k)$ with $\sigma^{l_d}(Z) = \sigma^{(l_d-1)}(B) \cdots \sigma(B)BZ$. By possibly replacing l_d with dl_d, we may assume that d divides l_d and define $l = \frac{l_d}{d}$. We claim that ($\mathrm{P3}^u$) (b_d') holds for this l. Fix a matrix $A \in \mathrm{GL}_m(k)$. It remains to show that there exists a matrix $Y \in \mathrm{GL}_m(k)$ with $\sigma^{dl}(Y) = \hat{A}Y$ where $\hat{A} = \sigma^{(l-1)d}(A) \dots \sigma^d(A)A$. By assumption, there exists a $Z \in \mathrm{GL}_{md}(k)$ with $\sigma^{l_d}(Z) = \hat{B}Z$, where we define B as block matrix

$$B = \begin{pmatrix} 0 & I_m & 0 & \\ \vdots & & \ddots & 0 \\ 0 & & & I_m \\ A & 0 & \dots & 0 \end{pmatrix} \in \mathrm{GL}_{md}(k)$$

and set $\hat{B}=\sigma^{(l_d-1)}(B)\cdots\sigma(B)B$. Recall that d divides l_d, so the product $\hat{B}$ with l_d factors is the block diagonal matrix:

$$\hat{B}=\begin{pmatrix}\hat{A} & & & \\ & \sigma(\hat{A}) & & \\ & & \ddots & \\ & & & \sigma^{d-1}(\hat{A})\end{pmatrix}.$$

Now the md columns of $Z\in \mathrm{GL}_{md}(k)$ are k-linearly independent, so we can choose m columns $z_1,\ldots,z_m$ of Z such that their projections $y_1,\ldots,y_m\in k^m$ to the first m coordinates are still k-linearly independent. Define $Y\in\mathrm{GL}_m(k)$ as the matrix with columns $y_1,\ldots,y_m$. By construction, $\sigma^{dl}(z_i)=\sigma^{l_d}(z_i)=\hat{B}z_i$, so $\sigma^{dl}(y_i)=\hat{A}y_i$ for all i and thus $\sigma^{dl}(Y)=\hat{A}Y$ as claimed. The proof in the (P3) case is analogous, but here we start with a fixed matrix $A\in\mathrm{GL}_m(k)$, define $B\in\mathrm{GL}_{md}(k)$ as above and obtain an integer l_d from (P3)(b') (depending on B and thus on A) and a matrix $Z\in\mathrm{GL}_{md}(k)$ with $\sigma^{l_d}(Z)=\hat{B}Z$ (with $\hat{B}$ defined as above). Again, we may assume that d divides l_d and set $l=l_d$ (which now depends on A) and the same computations as above yield a matrix $Y\in\mathrm{GL}_m(k)$ with $\sigma^{dl}(Y)=\hat{A}Y$ as claimed in (P3)(b$_d$'). □

Lemma 4.3. *A σ-field satisfying* (P3) (c) is inversive.

Proof. For $a\in k$, consider the multiplicative equation $\sigma(y)=a$. By (P3)(c), there exists an $n\geq 1$ and a solution $(a_1,\ldots,a_n)\in k^{[n]}$, i.e., $(\sigma^n(a_n),a_1,\ldots,a_{n-1})=(\sigma^{n-1}(a),\ldots,\sigma(a),a)$. Thus $\sigma^{n-1}(\sigma(a_n)-a)=0$ and so $\sigma(a_n)=a$, hence $\sigma\colon k\to k$ is surjective. □

The following lemma shows that property (P3) is preserved when passing to higher powers of σ.

Lemma 4.4. *If the difference field (k,σ) satisfies* (P3)*, then also the difference field (k,σ^d) satisfies* (P3) *for every $d\geq 1$. Similarly, if (k,σ) satisfies* (P3^u)*, then (k,σ^d) satisfies* (P3^u) *for every $d\geq 1$.*

Proof. No need to worry about (P3) (a) and (P3^u) (a). For property (b), we use Lemma 4.2 to conclude that it suffices to show that (b') holds for the difference field (k,σ^d) in both cases. But that condition equals (b$_d$') for the difference field (k,σ) which does hold by Lemma 4.2 in both cases (P3) and (P3^u).

For (c) let $\alpha_0,\ldots,\alpha_m\in\mathbb{Z}$ with $\alpha\neq 0$ and for $a\in k^\times$ consider the multiplicative σ^d-equation

$$y^{\alpha_0}\sigma^d(y)^{\alpha_1}\ldots\sigma^{dm}(y)^{\alpha_m}=a. \tag{3}$$

If (P3)(c) holds, there exists an $n\geq 1$ such that (3), when considered as a σ-equations has a solution in $k^{[n]}$. So (3), when considered as a system of σ^d-equations, has a solution in the k-σ^d-algebra $(k^{[n]},\sigma^d)$. As in the proof of Lemma 4.1, we can assume that $d|n$, say $n=dl$. Then we have a morphism

$$(k^{[n]},\sigma^d)\to(k,\sigma^d)^{[l]},\ (a_1,\ldots,a_n)\mapsto(a_d,a_{2d},\ldots,a_n)$$

of k-σ^d-algebras. Thus (3), when considered as a system of σ^d-equations, has a solution in $(k,\sigma^d)^{[l]}$. We conclude that (k,σ^d) satisfies (P3) (c). Moreover, if (k,σ) satisfies the stronger condition (P3^u) (c), then n does not depend on the choice of a and thus l does not depend on it either and thus (k,σ^d) satisfies the stronger condition (P3^u) (c). □

As indicated in the introduction, to show that (P1) implies (P3) it suffices to consider (P1) for a few particular σ-algebraic groups, namely, algebraic groups, GL_m^σ and one-relator subgroups of $\mathbb{G}_m$.

Proposition 4.5. *If a σ-field k satisfies* (P1)*, then it satisfies* (P3)*. Similarly,* (P1^u) *implies* (P3^u)*.*

Proof. To prove (a) in both cases, we need to show that (P1) implies that k is algebraically closed. As every finite Galois extension of k defines a torsor for a finite (constant) algebraic group over k, it is clear that a field with the property that every torsor for every algebraic group over k is trivial, has to be separably closed. Moreover, if k has positive characteristic p, then $\mathcal{G}=\{g\in\mathbb{G}_m|\ g^p=1\}$ is a (non-reduced) algebraic group and for every $a\in k^\times$ we have a $\mathcal{G}$-torsor $\mathcal{X}=\{x\in\mathbb{G}_m|\ x^p=a\}$. Thus if all these torsors are trivial, k must be algebraically closed.

So let $\mathcal{G}$ be an algebraic group over k and let $\mathcal{X}$ be a $\mathcal{G}$-torsor. We have to show that $\mathcal{X}(k)\neq\emptyset$. Set $G=[\sigma]_k\mathcal{G}$ and $X=[\sigma]_k\mathcal{X}$. Then X is a G-torsor. So, by assumption, there exists $n\geq 1$ such that

$X(k^{[n]}) = \mathcal{X}(k^{[n]}) \neq \emptyset$. In other words, there exists a morphism of k-algebras $k[\mathcal{X}] \to k^{[n]}$. Composing with the last projection $k^{[n]} \to k$ yields a morphism of k-algebras $k[\mathcal{X}] \to k$. So $\mathcal{X}(k) \neq \emptyset$ and k is algebraically closed.

To prove (b), consider the σ-algebraic group $G = \mathrm{GL}_m^\sigma = \{g \in \mathrm{GL}_m \mid \sigma(g) = g\}$. For $A \in \mathrm{GL}_m(k)$ consider the σ-variety X given by $X = \{x \in \mathrm{GL}_m \mid \sigma(x) = Ax\}$. It is straight forward to check that X is a G-torsor under the action $(g, x) \mapsto xg^{-1}$. We conclude that (P1) implies (P3)(b) and (P1^u) implies (P3^u)(b).

To prove (c) consider the σ-algebraic group $G = \{g \in \mathbb{G}_m \mid g^{\alpha_0}\sigma(g)^{\alpha_1} \ldots \sigma^m(g)^{\alpha_m} = 1\}$. Then the σ-variety $X = \{x \in \mathbb{G}_m \mid x^{\alpha_0}\sigma(x)^{\alpha_1} \ldots \sigma^m(x)^{\alpha_m} = a\}$ is a G-torsor. We conclude that (P1) implies (P3)(c) and (P1^u) implies (P3^u)(c). □

5. The proof of (P3)⇒(P1)

By now we have seen that (P1) and (P2) are equivalent (Proposition 3.19) and that (P1) implies (P3) (Propsition 4.5) and similarly for their uniform variants. Thus to complete the proof of our main result, it suffices to prove (P3)⇒(P1) (and (P3^u)⇒(P1^u)). This however is the most difficult part.

From now on we assume that k is a σ-field of characteristic zero.

It is an interesting question to ask for a generalization of Theorem 1.3 to positive characteristic. It may seem plausible to expect that the theorem also holds for a difference field k of positive characteristic p if (P3^u) (b) is replaced by

(P3^u) (b_p) *For every $m \geq 1$ and every power q of p there exists an integer $n \geq 1$ such that for every $A \in \mathrm{GL}_m(k)$ the equation $\sigma_q(Y) = AY$ has a solution in $\mathrm{GL}_m(k^{[n]})$.*

Here σ_q is defined by $\sigma_q(y) = \sigma(y)^q$. Note that the equation $\sigma_q(Y) = AY$ defines a torsor for the σ-algebraic group $G = \mathrm{GL}_m^{\sigma_q} = \{g \in \mathrm{GL}_m \mid \sigma_q(g) = g\}$. Moreover, any Frobenius difference field, i.e., an algebraically closed field of positive characteristic equipped with a Frobenius endomorphism, satisfies (P3^u) (b_p) with $n = 1$ (due to the Lang-Steinberg Theorem).

Many of our intermediate results (and proofs) in this section also work in arbitrary characteristic. However, there are also several steps where we make use of the characteristic zero assumption. At those steps, in positive characteristic, one usually would have to contend with non-reduced algebraic or σ-algebraic groups and the Frobenius endomorphism. We hope to establish a variant of Theorem 1.3 in positive characteristic in a future project dedicated to the study of torsors for σ-algebraic groups over Frobenius difference fields.

One of the advantages of working in characteristic zero is that every Hopf algebra is reduced. Therefore, a σ-algebraic group G is connected if and only if it is integral ([Wib21, Lemma 6.7]).

In this section we show that if k satisfies (P3) (or (P3^u)), then k is (uniformly) strongly G-trivial for any σ-algebraic group G over k. The proof heavily relies on the induction principle from Section 3 and the structure theory of σ-algebraic groups. Any σ-algebraic group can be decomposed into σ-algebraic groups belonging to certain more manageable classes of σ-algebraic groups and we first show that if k satisfies (P3), then k is uniformly strongly G-trivial for any G belonging to one of those more manageable classes. We start from classes of small (e.g., finite, order zero, σ-dimension zero) σ-algebraic groups and then build up to the general case.

5.1. **The proof for σ-algebraic groups of order zero.** In this subsection we show that an inversive, algebraically closed σ-field is uniformly strongly G-trivial for every σ-algebraic group G of order zero. The key ingredient for the proof is a decomposition theorem for σ-étale σ-algebraic groups ([Wib24, Theorem 6.38]). We first show that an algebraically closed σ-field is uniformly strongly G-trivial for every σ-algebraic group G coming from an algebraic group and for finite σ-algebraic groups.

Lemma 5.1. *Let k be an algebraically closed σ-field. If $G = [\sigma]_k\mathcal{G}$ for some algebraic group $\mathcal{G}$ over k, then k is uniformly strongly G-trivial.*

Proof. Because G_n comes from an algebraic group (Example 3.4), it suffices to show that k is uniformly G-trivial. By [BW22, Cor. 3.3] every G-torsor X is of the form $X = [\sigma]_k\mathcal{X}$ for some $\mathcal{G}$-torsor $\mathcal{X}$. Thus $X(k) = \mathcal{X}(k) \neq \emptyset$ because k is algebraically closed. □

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

Lemma 5.2. *Let G be a finite σ-algebraic group over an algebraically closed σ-field k. Then k is uniformly strongly G-trivial.*

Proof. Because G_n is a finite σ^n-algebraic group for every $n \geq 1$, it suffices to show that k is uniformly G-trivial.

Let $m = \dim_k(k\{G\})$ denote the dimension of $k\{G\}$ as a k-vector space. We claim that $X_n(k) \neq \emptyset$ for every G-torsor X, where $n = \operatorname{lcm}(1, \ldots, m)$. As $k\{X\} \otimes_k k\{X\} \simeq k\{G\} \otimes_k k\{X\}$, we see that $\dim_k(k\{X\}) = m$. So there are at most m prime ideals in $k\{X\}$. Considering the map $\mathfrak{p} \mapsto \sigma^{-1}(\mathfrak{p})$ on $\operatorname{Spec}(k\{X\})$ shows that there exists a prime ideal $\mathfrak{p}$ in $k\{X\}$ such that $\sigma^{-l}(\mathfrak{p}) = \mathfrak{p}$ for some l with $1 \leq l \leq m$. As l divides $n = \operatorname{lcm}(1, \ldots, m)$, we also have $\sigma^{-n}(\mathfrak{p}) = \mathfrak{p}$. Since k is algebraically closed, the residue field $k(\mathfrak{p})$ of $\mathfrak{p}$ equals k. The canonical map $k\{X\} \to k(\mathfrak{p}) = k$ is a morphism of k-σ^n-algebras. So $X_n(k) \neq \emptyset$. □

Proposition 5.3. *Let G be a σ-algebraic group of order zero over an algebraically closed σ-field k. Then k is uniformly strongly G-trivial.*

Proof. Since we work in characteristic zero, a σ-algebraic group of order zero is σ-étale ([Wib24, Cor. 4.9]). According to [Wib24, Theorem 6.38] any σ-étale σ-algebraic group has a Babbitt decomposition, i.e., there exists a subnormal series

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

such that

(i) $G_1 = G^{\sigma o}$ is the *σ-identity component* of G as defined in [Wib24, Def. 3.16]. The exact definition of $G^{\sigma o}$ is not relevant for our purpose. All we need to know is that the quotient $G/G^{\sigma o} = \pi_0^\sigma(G)$ is finite (cf. [Wib24, Prop. 3.13]).

(ii) G_i/G_{i+1} is isomorphic to a σ-algebraic group of the form $[\sigma]_k\mathcal{G}$ where $\mathcal{G}$ is an étale algebraic group for $i = 1, \ldots, n-1$ and

(iii) G_n is *σ-infinitesimal*. Again, for our purpose, the exact meaning of σ-infinitesimal is not relevant. It suffices to know that G_n is finite and this is the case because a σ-closed subgroup of σ-étale σ-algebraic group is σ-étale ([Wib24, Lemma 4.6]) and a σ-infinitesimal σ-étale σ-algebraic group is finite ([Wib24, Cor. 6.6]).

It follows from Lemma5.2 that k is uniformly strongly G/G_1-trivial and uniformly strongly G_n-trivial. Furthermore, k is uniformly strongly G_i/G_{i+1}-trivial for $i = 1, \ldots, n-1$ by Lemma 5.1. Thus, according to the induction principle (Corollary 3.21), k is uniformly strongly G-trivial. □

The following corollary will allow us to reduce to the case of connected σ-algebraic groups in the sequel.

Corollary 5.4. *Assume that k is algebraically closed and let G be a σ-algebraic group. If k is (uniformly) strongly G^o-trivial, then k is (uniformly) strongly G-trivial.*

Proof. As G/G^o is σ-étale it has order zero ([Wib24, Prop. 4.8]). So the assertion follows from Proposition 5.3 and Proposition 3.20(ii) applied to the exact sequence $1 \to G^o \to G \to G/G^o \to 1$. □

5.2. **A Jordan-Hölder type theorem.** With the order zero case out of the way, the next step is to look at σ-algebraic groups of finite positive order, i.e., σ-algebraic groups of σ-dimension zero. This is the most elaborate part of the proof.

We first treat some special cases (diagonalizable σ-algebraic groups, abelian σ-algebraic groups and Zariski dense σ-closed subgroups of simple algebraic groups) and then combine these via a Jordan-Hölder type decomposition. Since the Jordan-Hölder type decomposition is also helpful for the diagonalizable case we establish it first.

Definition 5.5. *Let G be a σ-algebraic group of finite positive order. Then G is* almost-simple *if* $\operatorname{ord}(N) = 0$ *for every proper normal σ-closed subgroup N of G.*

As G^o is a normal σ-closed subgroup of G with $\operatorname{ord}(G^o) = \operatorname{ord}(G)$ ([Wib21, Cor. 6.13]), we see that an almost-simple σ-algebraic group is connected.

Lemma 5.6. *Let G be a connected σ-algebraic of finite positive order. If H is a proper σ-closed subgroup of G, then* $\operatorname{ord}(H) < \operatorname{ord}(G)$.

Proof. Fix an embedding of G into some algebraic group and let $H[i] \leq G[i]$ denote the corresponding Zariski closures. Because G is connected, all the $G[i]$'s are connected ([Wib21, Lemma 6.12]). We have $\operatorname{ord}(G) = \dim(G[i])$ and $\operatorname{ord}(H) = \dim(H[i])$ for all sufficiently large i. Suppose $\operatorname{ord}(H) = \operatorname{ord}(G)$ so that $\dim(H[i]) = \dim(G[i])$. Because we are in characteristic zero and $G[i]$ is connected, this implies $H[i] = G[i]$ for all i. Thus $H = G$; a contradiction. □

The classical Jordan-Hölder Theorem decomposes a finite group into simple groups. Our variant decomposes a connected σ-algebraic group of finite positive order into almost-simple σ-algebraic groups.

Theorem 5.7. *Let G be a connected σ-algebraic group of finite positive order. Then there exists a subnormal series*

$$G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = 1$$

such that G_i is connected and G_i/G_{i+1} is almost-simple for $i = 0, \ldots, n-1$.

Proof. We proceed by induction on $\operatorname{ord}(G)$. If $\operatorname{ord}(G) = 1$, then any proper σ-closed subgroup of G has order 0 by Lemma 5.6. Thus the theorem holds with $n = 1$.

Assume $\operatorname{ord}(G) > 1$. If every proper normal σ-closed subgroup of G has order 0 the theorem also holds with $n = 1$. So we may assume that there exists a proper normal σ-closed subgroup of G of positive order. Among all such subgroups let N be of maximal order. Because N^o is a characteristic subgroup of N ([Wib21, Prop. 6.17]) and N is normal in G, it follows that N^o is normal in G.

We claim that G/N^o is almost-simple. A proper normal σ-closed subgroup of G/N^o is of the form N'/N^o for some proper normal σ-closed subgroup N' of G containing N^o ([Wib21, Theorem 5.9]). By the choice of N we have $\operatorname{ord}(N') \leq \operatorname{ord}(N) = \operatorname{ord}(N^o)$, where the last equality uses [Wib21, Cor. 6.13]. Thus $\operatorname{ord}(N') = \operatorname{ord}(N^o)$ and $\operatorname{ord}(N'/N^o) = \operatorname{ord}(N') - \operatorname{ord}(N^o) = 0$. This shows that G/N^o is almost-simple.

Set $G_1 = N^o$. Then G_1 is connected, normal in G and G_0/G_1 is almost-simple. As $\operatorname{ord}(G_1) < \operatorname{ord}(G)$ (Lemma 5.6) it follows from the induction hypothesis there exists a subnormal series $G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n = 1$ with G_i connected and G_i/G_{i+1} almost-simple for $i = 1, \ldots, n-1$. So the subnormal series $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_n = 1$ has the desired properties. □

5.3. **The proof for diagonalizable σ-algebraic groups of σ-dimension zero.** A σ-algebraic group is *diagonalizable* if it is isomorphic to a σ-closed subgroup of $\mathbb{G}_m^n$ for some $n \geq 1$. These groups and their torsors are well understood. Abbreviating $g^\alpha = g^{\alpha_0}\sigma(g)^{\alpha_1} \ldots \sigma^m(g)^{\alpha_m}$ for $\alpha = \alpha_0 + \alpha_1\sigma + \ldots + \alpha^m\sigma^m \in \mathbb{Z}[\sigma]$ and $g^\beta = g_1^{\beta_1} \ldots g_n^{\beta_n}$ for $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}[\sigma]^n$, every σ-closed subgroup of $\mathbb{G}_m^n$ is of the form

$$G = \{g \in \mathbb{G}_m^n | \; g^{\beta_1} = 1, \ldots, g^{\beta_m} = 1\},$$

for some $\beta_1, \ldots, \beta_m \in \mathbb{Z}[\sigma]^n$. Every G-torsor is of the form

$$X = \{x \in \mathbb{G}_m^n | \; x^{\beta_1} = a_1, \ldots, x^{\beta_m} = a_m\}$$

for some $a_1, \ldots, a_m \in k^\times$. So X is described by a system of m multiplicative difference equations in n difference variables. We need to show that this system has a solution in some $k^{[d]}$ using (P3^u) (b), which only states that *one* multiplicative difference equation in *one* difference variable has a solution in some $k^{[d]}$. In other words, we need to reduce the general case to the case of one-relator subgroups of $\mathbb{G}_m$. Before going into the details of the reduction proof, we need to provide the foundational properties of diagonalizable σ-algebraic groups.

5.3.1. *Diagonalizable σ-algebraic groups.* In this section we discuss the basic properties of diagonalizable σ-algebraic groups, as relevant for the proof of our main results. Diagonalizable algebraic groups are equivalent to finitely generated abelian groups. Diagonalizable σ-algebraic groups are equivalent to abelian groups M equipped with an endomorphism $\sigma\colon M \to M$ such that M is finitely σ-generated, i.e., there exists a finite subset B of M such that $B, \sigma(B), \sigma^2(B), \ldots$ generates M as an abelian group. Let $\mathbb{Z}[\sigma]$ denote the univariate polynomial ring in the variable σ aver the integers. To specify an endomorphism of an abelian group M is equivalent to defining a $\mathbb{Z}[\sigma]$-module structure on M. Moreover, M is finitely

σ-generated if and only M is a finitely generated as $\mathbb{Z}[\sigma]$-module. As a matter of convenience, we mostly use the language of $\mathbb{Z}[\sigma]$-modules, rather than classical difference algebra jargon.

For $\alpha = \alpha_0 + \alpha_1\sigma + \ldots + \alpha^m\sigma^m \in \mathbb{Z}[\sigma]$ and $g \in R^\times$, where R is a k-σ-algebra, we set

$$g^\alpha = g^{\alpha_0}\sigma(g)^{\alpha_1}\ldots\sigma^m(g)^{\alpha_m}.$$

Then $(gh)^\alpha = g^\alpha h^\alpha$ for $g,h \in R^\times$ and $(g^\alpha)^\beta = g^{\alpha\beta}$ for $\alpha,\beta \in \mathbb{Z}[\sigma]$. Thus $R^\times$ is a $\mathbb{Z}[\sigma]$-module under $(\alpha, g) \mapsto g^\alpha$. For a $\mathbb{Z}[\sigma]$-module M we denote with $\operatorname{Hom}_{\mathbb{Z}[\sigma]}(M, R^\times)$ the abelian group of morphisms of $\mathbb{Z}[\sigma]$-modules from M to $R^\times$.

Lemma 5.8. *Let M be a finitely generated $\mathbb{Z}[\sigma]$-module. The functor $D_\sigma(M)$ from the category of k-σ-algebras to the category of groups, given by $D_\sigma(M)(R) = \operatorname{Hom}_{\mathbb{Z}[\sigma]}(M, R^\times)$, is a σ-algebraic group over k. It is represented by $k\{D(M)\} = k[M]$, the group algebra of M over k, equipped with the natural extension of σ.*

Proof. Let $k[M]$ denote the group algebra of the abelian group M over k. As M is abelian, $k[M]$ is a commutative k-algebra. We define $\sigma\colon k[M] \to k[M]$ by $\sigma(\sum_i \lambda_i m_i) = \sum_i \sigma(\lambda_i)\sigma(m_i)$ for $\lambda_i \in k$ and $m_i \in M$. This makes $k[M]$ a k-σ-algebra. If $B \subseteq M$ generates M as a $\mathbb{Z}[\sigma]$-module, then $B \subseteq M \subseteq k[M]$ generated $k[M]$ as a k-σ-algebra. Thus $k[M]$ is finitely σ-generated over k. Moreover,

$$\operatorname{Hom}_{k,\sigma}(k[M], R) \simeq \operatorname{Hom}_{\mathbb{Z}[\sigma]}(M, R^\times)$$

functorially in R. □

Definition 5.9. *A σ-algebraic group is* diagonalizable *if it is isomorphic to $D_\sigma(M)$ for some finitely generated $\mathbb{Z}[\sigma]$-module M.*

Example 5.10. Specifying a morphism $\mathbb{Z}[\sigma]^m \to R^\times$ of $\mathbb{Z}[\sigma]$-modules, is equivalent to choosing n elements from $R^\times$ (the images of the n basis vectors). It follows that $D_\sigma(\mathbb{Z}[\sigma]^n) = [\sigma]_k\mathbb{G}_m^n$.

Example 5.11. Let $\alpha \in \mathbb{Z}[\sigma]$ and let G be the σ-closed subgroup of $\mathbb{G}_m$ given by $G = \{g \in \mathbb{G}_m |\ g^\alpha = 1\}$. To specify an element of $\mathbb{G}_m(R) = R^\times$ is equivalent to specifying a morphism $\mathbb{Z}[\sigma] \to R^\times$ of $\mathbb{Z}[\sigma]$-modules. The element of $R^\times$ lies in $G(R)$ if and only if α lies in the kernel of the corresponding morphism. Thus $G \simeq D_\sigma(\mathbb{Z}[\sigma]/(\alpha))$.

Let M be a finitely generated $\mathbb{Z}[\sigma]$-module. We define $\operatorname{rank}_{\mathbb{Z}[\sigma]}(M)$ as the dimension of $M \otimes_{\mathbb{Z}[\sigma]} \mathbb{Q}(\sigma)$ as a $\mathbb{Q}(\sigma)$-vector space. This agrees with the maximal number of $\mathbb{Z}[\sigma]$-linearly independent elements in M. We define $\operatorname{rank}_{\mathbb{Z}}(M)$ as the dimension of $M \otimes_{\mathbb{Z}} \mathbb{Q}$ as a $\mathbb{Q}$-vector space. This is understood to be simply ∞ in case it is not finite. We say that M has no $\mathbb{Z}$-torsion if $nm = 0$ implies $n = 0$ or $m = 0$ for $n \in \mathbb{Z}$ and $m \in M$. We will need the following basic lemma connecting the two different ranks of M.

Lemma 5.12. *Let M be a finitely generated $\mathbb{Z}[\sigma]$-module. If $\operatorname{rank}_{\mathbb{Z}[\sigma]}(M) = 0$, then $\operatorname{rank}_{\mathbb{Z}}(M) < \infty$.*

Proof. Because $\operatorname{rank}_{\mathbb{Z}[\sigma]}(M) = 0$ and M is finitely generated, we see that there exists a non-zero $\alpha \in \mathbb{Z}[\sigma]$ such that $\alpha m = 0$ for all $m \in M$. So M is a finitely generated $\mathbb{Z}[\sigma]/(\alpha)$-module. It follows that $M \otimes_{\mathbb{Z}} \mathbb{Q}$ is a finitely generated module over $(\mathbb{Z}[\sigma]/(\alpha)) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}[\sigma]/(\alpha)$. As $\mathbb{Q}[\sigma]/(\alpha)$ is a finite dimensional $\mathbb{Q}$-vector space, it follows that also $M \otimes_{\mathbb{Z}} \mathbb{Q}$ is a finite dimensional $\mathbb{Q}$-vector space. Thus $\operatorname{rank}_{\mathbb{Z}}(M) < \infty$. □

The following proposition collects all the properties of diagonalizable σ-algebraic groups that we will need.

Proposition 5.13.

(i) *The (contravariant) functor $M \rightsquigarrow D_\sigma(M)$ from the category of finitely generated $\mathbb{Z}[\sigma]$-modules to the category of diagonalizable σ-algebraic groups is an equivalence of categories.*
(ii) *A sequence $0 \to M' \to M \to M'' \to 0$ of finitely generated $\mathbb{Z}[\sigma]$-modules is exact if and only if the sequence $1 \to D_\sigma(M'') \to D_\sigma(M) \to D_\sigma(M') \to 1$ of σ-algebraic groups is exact.*
(iii) *A σ-algebraic group is diagonalizable if and only if it is isomorphic to a σ-closed subgroup of $\mathbb{G}_m^n$ for some $n \geq 1$.*
(iv) *Quotients and σ-closed subgroups of diagonalizable σ-algebraic groups are diagonalizable.*
(v) *For a finitely generated $\mathbb{Z}[\sigma]$-module M we have $\sigma\text{-}\dim(D_\sigma(M)) = \operatorname{rank}_{\mathbb{Z}[\sigma]}(M)$ and $\operatorname{ord}(D_\sigma(M)) = \operatorname{rank}_{\mathbb{Z}}(M)$.*

(vi) *The σ-algebraic group $D_\sigma(M)$ is connected if and only if M has no $\mathbb{Z}$-torsion.*

Proof. For a σ-algebraic group G let $X(G)$ denote the abelian group of all morphisms $G \to \mathbb{G}_m$ of σ-algebraic groups. Then $X(G)$ is a $\mathbb{Z}[\sigma]$-module with action of σ obtained by composition with $\sigma\colon \mathbb{G}_m \to \mathbb{G}_m,\ g \mapsto \sigma(g)$. We will show that X defines a quasi-inverse to D_σ.

Recall that an element a in a k-Hopf algebra is group-like if $\Delta(a) = a \otimes a$. For example, the variable $y \in k\{y, y^{-1}\} = k\{\mathbb{G}_m\}$ is group-like. A morphism $G \to \mathbb{G}_m$ of σ-algebraic groups is determined by the image of y under the dual map $k\{y, y^{-1}\} = k\{\mathbb{G}_m\} \to k\{G\}$ and this is a group-like element of $k\{G\}$. Conversely, a group-like element $a \in k\{G\}$ defines a morphism $\chi\colon G \to \mathbb{G}_m$ of σ-algebraic groups via $\chi(g) = g(a)$ for $g \in G(R) = \operatorname{Hom}_{k,\sigma}(k\{G\}, R)$ for any k-σ-algebra R. The group-like elements of $k\{G\}$ are stable under σ and this action of σ corresponds to the action of σ on $X(G)$. We can therefore identify $X(G)$ (as a $\mathbb{Z}[\sigma]$-module) with the set of all group-like elements of $k\{G\}$.

If M is a finitely generated $\mathbb{Z}[\sigma]$-module, the elements of M are group-like elements of $k[M]$. Moreover, since group-like elements are k-linearly independent ([Wat79, Lemma 2.2]), it follows that M agrees with the set of group-like elements of $k[M]$. Thus $X(D_\sigma(M)) \simeq M$ and it follows that X is a quasi-inverse to D_σ. This implies (i).

Let $0 \to M' \to M \to M'' \to 0$ be a sequence of finitely generated $\mathbb{Z}[\sigma]$-modules. First assume it is exact. The dual map $k[M''] \to k[M]$ to $D_\sigma(M'') \to D_\sigma(M)$ is just the k-linear extension of $M'' \to M$. So, since $M \to M''$ is surjective, also $k[M] \to k[M'']$ is surjective. Therefore, $D_\sigma(M'') \to D_\sigma(M)$ is a σ-closed embedding. Similarly, since $M' \to M$ is injective, also $k[M'] \to k[M]$ is injective. So $D_\sigma(M) \to D_\sigma(M')$ is a quotient map. For a k-σ-algebra R we have

$$\begin{aligned}\ker(D_\sigma(M) \to D_\sigma(M'))(R) &= \ker\left(\operatorname{Hom}_{\mathbb{Z}[\sigma]}(M, R^\times) \to \operatorname{Hom}_{\mathbb{Z}[\sigma]}(M', R^\times)\right) \\ &= \{g \in \operatorname{Hom}_{\mathbb{Z}[\sigma]}(M, R^\times) \mid g|_{M'} = 1\} \simeq \operatorname{Hom}_{\mathbb{Z}[\sigma]}(M'', R^\times) = D_\sigma(M'')\end{aligned}$$

Thus the sequence of σ-algebraic groups is exact.

Conversely, if $1 \to D_\sigma(M'') \to D_\sigma(M) \to D_\sigma(M') \to 1$ is exact, then, as $k[M'] \to k[M]$ is injective and $k[M] \to k[M'']$ is surjective, it follows that $M' \to M$ is injective and $M \to M''$ is surjective. Thus $D_\sigma(M'') \to D_\sigma(M)$ is a σ-closed embedding and $D_\sigma(M) \to D_\sigma(M')$ is a quotient map. The exactness at $D_\sigma(M)$ means that for every k-σ-algebra R, the map

$$\operatorname{Hom}_{\mathbb{Z}[\sigma]}(M'', R^\times) \to \{g \in \operatorname{Hom}_{\mathbb{Z}[\sigma]}(M, R^\times) \mid g|_{M'} = 1\} \tag{4}$$

is bijective. Let m_0 be in the kernel of $M \to M''$. Then, using (4), we see that m_0 gets mapped to $1 \in R^\times$ under every $g \in \operatorname{Hom}_{\mathbb{Z}[\sigma]}(M, R^\times)$ with $g|_{M'} = 1$ for any k-σ-algebra R. Choosing $R = k[M/M']$ and $g\colon M \to R^\times$ the map that sends m to the equivalence class of m in M/M', it follows that m_0 lies in M'. This shows that $0 \to M' \to M \to M'' \to 0$ is exact and completes the proof of (ii).

If H is a σ-closed subgroup of a diagonalizable σ-algebraic group $D_\sigma(M)$, then we have a surjective morphism $k[M] \to k\{H\}$ of k-σ-Hopf algebras. As $k[M]$ is generated by group-like elements as a k-vector space, it follows that also $k\{H\}$ is generated by group-like elements as a k-vector space. From the discussion in the proof of (i), we see that $k\{H\} = k[M'']$, where M'' is the $\mathbb{Z}[\sigma]$-module of all group-like elements of $k\{H\}$. Thus H is diagonalizable.

If $G = D_\sigma(M)$ is a diagonalizable σ-algebraic group, we can find an $n \geq 1$ and a surjective morphism $\mathbb{Z}[\sigma]^n \to M$ of $\mathbb{Z}[\sigma]$-modules. According to (ii) this corresponds to a σ-closed embedding $G = D_\sigma(M) \to D_\sigma(\mathbb{Z}[\sigma]^n) = \mathbb{G}_m^n$. Conversely, if G is a σ-closed subgroup of $\mathbb{G}_m^n$, then G is diagonalizable because, as seen above, σ-closed subgroups of diagonalizable σ-algebraic groups are diagonalizable. This proves (iii).

A quotient of a diagonalizable σ-algebraic group, is a quotient by a diagonalizable σ-closed subgroup, so the quotient is diagonalizable by (ii). This completes the proof of (iv).

Let M be a finitely generated $\mathbb{Z}[\sigma]$-module and fix a surjective morphism $\mathbb{Z}[\sigma]^n \to M$ with kernel N. As discussed above, this corresponds to a σ-closed embedding of $G = D_\sigma(M)$ into $\mathbb{G}_m^n$. Explicitly, we have

$$D_\sigma(M) = \{(g_1, \ldots, g_n) \in \mathbb{G}_m^n \mid g_1^{\alpha_1} \ldots g_n^{\alpha_n} = 1\ \forall\ (\alpha_1, \ldots, \alpha_n) \in N\}.$$

For $i \geq 0$, the i-th order Zariski closure $G[i]$ of G in $\mathbb{G}_m^n$ is then the closed subgroup of $(\mathbb{G}_m^n)^{i+1} = \mathbb{G}_m^{n(i+1)}$ defined by all equations corresponding to tuples in N whose components are polynomials of degree at most i. So if $\mathbb{Z}[\sigma]_{\leq i}$ denotes the $\mathbb{Z}$-submodule of $\mathbb{Z}[\sigma]$ of all polynomials of degree at most i, then

$G[i]$ is the diagonalizable algebraic group corresponding to the $\mathbb{Z}$-module $\mathbb{Z}[\sigma]^n_{\leq i}/\mathbb{Z}[\sigma]^n_{\leq i} \cap N$. Note that if $B \subseteq M$ is the image of the standard basis of $\mathbb{Z}[\sigma]^n$ in M, then $\mathbb{Z}[\sigma]^n_{\leq i}/\mathbb{Z}[\sigma]^n_{\leq i} \cap N$ identifies with $\langle B, \sigma(B), \ldots, \sigma^i(B)\rangle$, the $\mathbb{Z}$-submodule of M generated by $B, \sigma(B), \ldots, \sigma^i(B)$. In particular, $\dim(G[i]) = \operatorname{rank}_{\mathbb{Z}}(\langle B, \ldots, \sigma^i(B)\rangle)$.

First assume that $\operatorname{rank}_{\mathbb{Z}[\sigma]}(M) = 0$. Then $\operatorname{rank}_{\mathbb{Z}}(M)$ is finite by Lemma 5.12 and bounds $\dim(G[i]) = \operatorname{rank}_{\mathbb{Z}}(\langle B, \ldots, \sigma^i(B)\rangle)$ for all i. Thus $\sigma\text{-}\dim(G) = 0$ and

$$\operatorname{ord}(G) = \max_i \dim(G[i]) = \max_i \operatorname{rank}_{\mathbb{Z}}(\langle B, \ldots, \sigma^i(B)\rangle) = \operatorname{rank}_{\mathbb{Z}}(M).$$

If $d = \operatorname{rank}_{\mathbb{Z}[\sigma]}(M) > 0$, then we can find an exact sequence $0 \to \mathbb{Z}[\sigma]^d \to M \to N \to 0$ with $\operatorname{rank}_{\mathbb{Z}[\sigma]}(N) = 0$. By (ii) this corresponds to an exact sequence $1 \to D_\sigma(N) \to D_\sigma(M) \to \mathbb{G}_m^d \to 1$. Therefore $D_\sigma(M)/D_\sigma(N) = \mathbb{G}_m^d$. As $\operatorname{rank}_{\mathbb{Z}[\sigma]}(N) = 0$, we have $\sigma\text{-}\dim(D_\sigma(N)) = 0$ (as argued above). Therefore $\sigma\text{-}\dim(D_\sigma(M)) = \sigma\text{-}\dim(\mathbb{G}_m^d) = d = \operatorname{rank}_{\mathbb{Z}[\sigma]}(M)$. Moreover, we have $\operatorname{rank}_{\mathbb{Z}}(M) = \infty$ so that $\operatorname{ord}(D_\sigma(M)) = \operatorname{rank}_{\mathbb{Z}}(M)$ also in this case. This proves (v).

We know that G is connected if and only if $G[i]$ is connected for all $i \geq 0$ ([Wib21, Lemma 6.12]). But a diagonalizable algebraic group corresponding to a finitely generated $\mathbb{Z}$-module is connected if and only if the $\mathbb{Z}$-module has no ($\mathbb{Z}$-)torsion (using our characteristic zero assumption). Thus G is connected if and only $\langle B, \ldots, \sigma^i(B)\rangle$ has no torsion for all $i \geq 0$ and this is equivalent to M having no $\mathbb{Z}$-torsion. ☐

Example 5.14. For $G = \{g \in \mathbb{G}_m |\ g^\alpha = 1\}$ with $\alpha \in \mathbb{Z}[\sigma]$ non-zero, we have $\operatorname{ord}(G) = \deg(\alpha)$ because $(\mathbb{Z}[\sigma]/(\alpha)) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}[\sigma]/(\alpha)$ is a $\mathbb{Q}$-vector space of dimension $\deg(\alpha)$.

Lemma 5.15. *If G is a diagonalizable σ-algebraic group, then G_n is a diagonalizable σ^n-algebraic group for every $n \geq 1$.*

Proof. If G is a σ-closed subgroup of $\mathbb{G}_m^m$, then G_n is a σ^n-closed subgroup of $(\mathbb{G}_m^m)^n$. Now use Proposition 5.13 (iii). ☐

5.3.2. *Reduction to one-relator subgroups of* $\mathbb{G}_m$. We will need the following result about ideals in $\mathbb{Z}[\sigma]$.

Lemma 5.16. *Let I be an ideal of $\mathbb{Z}[\sigma]$ such that $I \cap \mathbb{Z} = \{0\}$. Then there exists an $\alpha \in \mathbb{Z}[\sigma]$ of positive degree such that $I \subseteq (\alpha)$.*

Proof. We may assume that I is not the zero ideal. The prime ideals of $\mathbb{Z}[\sigma]$ are

- the zero ideal,
- ideals of the form (p) with p a prime number,
- ideals of the form (α), where $\alpha \in \mathbb{Z}[\sigma]$ is irreducible and of positive degree,
- ideals of the form (p, α), where p is a prime number and $\alpha \in \mathbb{Z}[\sigma]$ is a monic polynomial, irreducible mod p ([Mum99, Chapter II, §1, Example H]).

Suppose that all prime ideals minimal above I are of the form (p) or (p, α). Then their intersection, which agrees with the radical of I, contains a non-zero integer (the product of all the relevant p's). Thus also I contains a non-zero integer; a contradiction.

Therefore, at least one of the prime ideals minimal above I is of the form (α). In particular, $I \subseteq (\alpha)$. ☐

Lemma 5.17. *Let $\alpha \in \mathbb{Z}[\sigma]$ have positive degree. Then $G = \{g \in \mathbb{G}_m |\ g^\alpha = 1\}$ is almost-simple if and only if $\alpha \in \mathbb{Z}[\sigma]$ is irreducible.*

Proof. Assume that G is almost-simple and that α factors as $\alpha = \beta\gamma$. Without loss of generality, we assume that β has positive degree. As $\{g \in \mathbb{G}_m |\ g^\beta = 1\}$ is a σ-closed subgroup of G of order $\deg(\beta) > 0$, it follows that the morphism $\mathbb{Z}[\sigma]/(\alpha) \to \mathbb{Z}[\sigma]/(\beta)$ is an isomorphism, i.e., $(\alpha) = (\beta)$. This is only possible if $\alpha = \pm\beta$. Thus α is irreducible.

Assume that α is irreducible and let N be a proper σ-closed subgroup of G. By Proposition 5.13 the inclusion $N \leq G$ corresponds to a surjection $\mathbb{Z}[\sigma]/(\alpha) \to \mathbb{Z}[\sigma]/I$ for some ideal I of $\mathbb{Z}[\sigma]$ with $(\alpha) \subsetneqq I$. Suppose $I \cap \mathbb{Z} = \{0\}$. Then, by Lemma 5.16, there exists a polynomial $\beta \in \mathbb{Z}[\sigma]$ with $I \subseteq (\beta)$. So $(\alpha) \subsetneqq (\beta)$. This contradicts the irreducibility of α. Thus $I \cap \mathbb{Z} \neq \{0\}$ and therefore $\operatorname{rank}_{\mathbb{Z}}(\mathbb{Z}[\sigma]/I) = 0$. Hence $\operatorname{ord}(N) = 0$ as desired. ☐

We now work towards showing that in fact every almost-simple σ-closed subgroup of $\mathbb{G}_m$ is of the form described in Lemma 5.17. We call a σ-closed subgroup G of $\mathbb{G}_m$ a *one-relator subgroup* if there exists a non-zero $\alpha \in \mathbb{Z}[\sigma]$ such that $G = \{g \in \mathbb{G}_m |\ g^\alpha = 1\}$.

Lemma 5.18. *Let G be a σ-closed subgroup of $\mathbb{G}_m$ of finite positive order. Then there exists a σ-closed subgroup H of G such that H is a one-relator subgroup of $\mathbb{G}_m$ and* $\operatorname{ord}(H) > 0$.

Proof. By Proposition 5.13 we have $G = D_\sigma(\mathbb{Z}[\sigma]/I)$ for some ideal I of $\mathbb{Z}[\sigma]$. Moreover, $I \cap \mathbb{Z} = \{0\}$ because otherwise we would have $\operatorname{ord}(G) = \operatorname{rank}_{\mathbb{Z}}(\mathbb{Z}[\sigma]/I) = 0$. We know from Lemma 5.16 that there exists an $\alpha \in \mathbb{Z}[\sigma]$ of positive degree such that $I \subseteq (\alpha)$. The surjection $\mathbb{Z}[\sigma]/I \to \mathbb{Z}[\sigma]/(\alpha)$ corresponds to the inclusion of $H = \{h \in \mathbb{G}_m |\ h^\alpha = 1\}$ into G. □

Corollary 5.19. *Let G be an almost-simple σ-closed subgroup of $\mathbb{G}_m$ of finite positive order. Then G is a one-relator subgroup of $\mathbb{G}_m$.*

Proof. This is clear from Lemma 5.18. □

Our next goal is to show that a σ-field satisfying (P3^u) is uniformly strongly G-trivial for every almost-simple diagonalizable σ-algebraic group of order one. To this end, we have to take a closer look at the almost-simple σ-closed subgroups of $\mathbb{G}_m$ of order one.

Lemma 5.20. *Let G be an almost-simple σ-closed subgroup of $\mathbb{G}_m$ of order one. Then $G = \{g \in \mathbb{G}_m |\ g^\alpha \sigma(g)^\beta = 1\}$ for some integers α, β with $\beta \neq 0$ and* $\gcd(\alpha, \beta) = 1$.

Proof. We know from Corollary 5.19 that G is a one-relator subgroup and from Lemma 5.17 we know that G is defined by an irreducible polynomial $\beta\sigma + \alpha$ of degree one. Thus $\beta \neq 0$ and $\gcd(\alpha, \beta) = 1$. □

We now work towards showing that if k satisfies (P3^u), then k is uniformly strongly G-trivial for G a σ-algebraic group of the form described in Lemma 5.20.

Lemma 5.21. *Let α, β be integers with $\beta \neq 0$ and $\gcd(\alpha, \beta) = 1$ and let G be the σ-closed subgroup of $\mathbb{G}_m^n$ defined by the equations*

$$y_1^\alpha y_2^\beta = 1,\ y_2^\alpha y_3^\beta = 1, \ldots, y_{n-1}^\alpha y_n^\beta = 1,\ y_n^\alpha \sigma(y_1)^\beta = 1.$$

If k satisfies (P3) *(or* (P3^u)*), then k is (uniformly) G-trivial.*

Proof. By [BW22, Example 4.2], every G-torsor is isomorphic to a σ-closed σ-subvariety X of $\mathbb{G}_m^n$ defined by equations

$$y_1^\alpha y_2^\beta = a_1,\ y_2^\alpha y_3^\beta = a_2, \ldots, y_{n-1}^\alpha y_n^\beta = a_{n-1},\ y_n^\alpha \sigma(y_1)^\beta = a_n \tag{5}$$

for some $a_1, \ldots, a_n \in k^\times$. If $\alpha = 0$, then $\beta = \pm 1$ and (5) has a (unique) solution in k^n by Lemma 4.3. We can thus assume that $\alpha \neq 0$. By assumption, the equation

$$y_1^{(-1)^{n+1}\alpha^n} \sigma(y_1)^{\beta^n} = a_n^{\beta^{n-1}} a_{n-1}^{-\alpha\beta^{n-2}} a_{n-2}^{\alpha^2\beta^{n-3}} \ldots a_2^{(-1)^{n-2}\alpha^{n-2}\beta} a_1^{(-1)^{n-1}\alpha^{n-1}} \tag{6}$$

has a solution $b_1 \in k^{[d]}$ for some $d \geq 1$. Moreover, if k satisfies (P3^u), then $[d]$ can be chosen uniformly for all $a_1, \ldots, a_n$. Note that b_1 is automatically invertible. For $i = 2, \ldots, n$ choose $b_i \in k^{[d]}$ such that

$$b_i^{\alpha^{n-i+1}} = a_i^{\alpha^{n-i}} a_{i+1}^{-\alpha^{n-i-1}\beta} a_{i+2}^{\alpha^{n-i-2}\beta^2} \ldots a_n^{(-1)^{n-i}\beta^{n-i}} \sigma(b_1)^{(-1)^{n-i+1}\beta^{n-i+1}}. \tag{7}$$

This is possible because k is algebraically closed. The choice of b_i is not unique but any other possible choice is of the form ζb_i, where $\zeta = (\zeta_1, \ldots, \zeta_d) \in k^{[d]}$ with $\zeta_i \in k$ an α^{n-i+1}-th root of unity, i.e., $\zeta_i^{\alpha^{n-i+1}} = 1$. Note that formula (7) also holds for $i = 1$ by (6). Then

$$(b_i^\alpha b_{i+1}^\beta)^{\alpha^{n-i}} = a_i^{\alpha^{n-i}}$$

for $i = 1, \ldots, n-1$. Thus $b_i^\alpha b_{i+1}^\beta$ and a_i agree up to multiplication with an α^{n-i}-th root of unity in every component. Note that the choice of b_{i+1} is only unique up to multiplication with an α^{n-i}-th root of unity in every component. Moreover, as $\gcd(\alpha^{n-i}, \beta) = 1$, the map $\zeta \mapsto \zeta^\beta$ is a bijection on the set of α^{n-i}-th roots of unity in k. This shows that we can adjust all the roots of unity in the choice of $b_2, \ldots, b_n$ such that $b_i^\alpha b_{i+1}^\beta = a_i$ for $i = 1, \ldots, n-1$. More precisely, b_1 is already fixed and we adjust b_2 such that $b_1^\alpha b_2^\beta = a_1$. Then we adjust b_3 such that $b_2^\alpha b_3^\beta = a_2$. We continue like this until we adjust b_n such that

$b_{n-1}^{\alpha}b_n^{\beta}=a_n$. Thus $b=(b_1,\ldots,b_n)$ satisfies the first $n-1$ equations in (5). Evaluating (7) for $i=n$ shows that b also satisfies the last equation. Therefore $b\in X(k^{[d]})\neq\emptyset$ as desired. □

Lemma 5.22. *Let α,β be integers with $\beta\neq 0$ and $\gcd(\alpha,\beta)=1$ and set $G=\{g\in\mathbb{G}_m|\ g^{\alpha}\sigma(g)^{\beta}=1\}$. If k satisfies* (P3) *(or* (P3^u)*), then k is (uniformly) strongly G-trivial.*

Proof. Let $n\geq 1$. We have to show that (k,σ^n) is (uniformly) G_n-trivial for every $n\geq 1$. Note that G_n is the σ^n-closed subgroup of $\mathbb{G}_m^n$ defined by the equations

$$y_1^{\alpha}y_2^{\beta}=1,\ y_2^{\alpha}y_3^{\beta}=1,\ldots,y_{n-1}^{\alpha}y_n^{\beta}=1,\ y_n^{\alpha}\sigma^n(y_1)^{\beta}=1.$$

Because (k,σ^n) satisfies (P3) (or (P3^u)) by Lemma 4.4, the claim follows from Lemma 5.21. □

Lemma 5.23. *Let G be a non-trivial diagonalizable σ-algebraic group. Then there exists a proper σ-closed subgroup N of G such that G/N is isomorphic to a σ-closed subgroup of $\mathbb{G}_m$.*

Proof. As G is diagonalizable, we can assume that G is a σ-closed subgroup of some $\mathbb{G}_m^n$. As G is non-trivial, at least one of the projections $G\to\mathbb{G}_m$ will have non-trivial image. The kernel N has the required properties. □

Lemma 5.24. *Let G be an almost-simple diagonalizable σ-algebraic group of order one. If k satisfies* (P3) *(or* (P3^u)*), then k is (uniformly) strongly G-trivial.*

Proof. By Lemma 5.23, there exists an exact sequence $1\to N\to G\to H\to 1$ with N a proper σ-closed subgroup of G and H a σ-closed subgroup of $\mathbb{G}_m$. Because N has order zero, we know that k is uniformly strongly N-trivial by Proposition 5.3. Moreover, H is an almost-simple diagonalizable σ-algebraic group of order one. Thus, by the induction principle (Proposition 3.20 (ii)), we can assume that G is a σ-closed subgroup of $\mathbb{G}_m$. So $G=\{g\in\mathbb{G}_m|\ g^{\alpha}\sigma(g)^{\beta}=1\}$ with $\beta\neq 0$ $\gcd(\alpha,\beta)=1$ by Lemma 5.20 and therefore k is (uniformly) strongly G-trivial by Lemma 5.22. □

With the order one case completed, we need two more lemmas to get to the general case of a diagonalizable σ-algebraic group of σ-dimension zero. We need the strong G-triviality but first we record the G-triviality for almost-simple diagonalizable σ-algebraic groups.

Lemma 5.25. *Let G be an almost-simple diagonalizable σ-algebraic group of finite positive order. If k satisfies* (P3) *(or* (P3^u)*), then k is (uniformly) G-trivial.*

Proof. By Lemma 5.23, there exists an exact sequence $1\to N\to G\to H\to 1$ with H a non-trivial σ-closed subgroup of $\mathbb{G}_m$. As N has order zero, k is (uniformly) strongly N-trivial (Proposition 5.3). By the induction principle (Proposition 3.20 (i) in this case), we can thus assume that G is a σ-closed subgroup of $\mathbb{G}_m$. By Lemma 5.19 every almost-simple σ-closed subgroup of $\mathbb{G}_m$ is a one-relator subgroup. So G is of the form $G=\{g\in\mathbb{G}_m|\ g^{\alpha}=1\}$ for some $\alpha\in\mathbb{Z}[\sigma]$. By [BW22, Example 4.2] every G-torsor is of the form $X=\{x\in\mathbb{G}_m|\ x^{\alpha}=a\}$ for some $a\in k^{\times}$. So k is (uniformly) G-trivial by (P3) (c) (or (P3^u) (c)). □

Lemma 5.26. *Let G be an almost-simple diagonalizable σ-algebraic group of finite positive order. If k satisfies* (P3) *(or* (P3^u)*), then k is (uniformly) strongly G-trivial.*

Proof. We will prove this by induction on the order of G. To be precise, our induction hypothesis is that every difference field satisfying (P3) (or (P3^u)) is (uniformly) strongly H-trivial for every almost-simple diagonalizable σ-algebraic group H with $1\leq\operatorname{ord}(H)<\operatorname{ord}(G)$. The base case $\operatorname{ord}(G)=1$ is Lemma 5.24.

For the induction step we have to show that (k,σ^n) is (uniformly) G_n-trivial for every $n\geq 1$. Note that G_n is a diagonalizable σ^n-algebraic group (Lemma 5.15) with $\operatorname{ord}(G_n)=\operatorname{ord}(G)$ (Lemma 3.8). Moreover, (k,σ^n) satisfies (P3) (or (P3^u)) by Lemma 4.4. So if G_n is almost-simple, then the claim follows from Lemma 5.25. We can therefore assume that G_n is not almost-simple. Note that G_n is connected, because G is connected (Lemma 3.7). By Theorem 5.7 there exists a subnormal series $G_n=H_0\supseteq H_1\supseteq\ldots\supseteq H_m=1$ with H_i connected and H_i/H_{i+1} almost-simple for $i=0,\ldots,m-1$. Because the quotients H_i/H_{i+1} are diagonalizable (Proposition 5.13 (iv)) and $\operatorname{ord}(H_i/H_{i+1})<\operatorname{ord}(G_n)=\operatorname{ord}(G)$, it follows from the induction hypothesis that (k,σ^n) is (uniformly) strongly H_i/H_{i+1}-trivial for $i=0,\ldots,m-1$. Therefore Corollary 3.21 shows that (k,σ^n) is (uniformly) strongly G_n-trivial. □

Proposition 5.27. *Let G be a diagonalizable σ-algebraic group of σ-dimension zero. If k satisfies* (P3) *(or* (P3^u)*), then k is (uniformly) strongly G-trivial.*

Proof. If $\mathrm{ord}(G) = 0$, the claim follows from Proposition 5.3. So we may assume $\mathrm{ord}(G) > 0$. Furthermore, we can assume that G is connected (Corollary 5.4). Now the claim follows by combining Theorem 5.7, Lemma 5.26 and Corollary 3.21. □

5.4. **The proof for σ-algebraic vector groups of σ-dimension zero.** In this subsection we show that a σ-field satisfying (P3) (or (P3^u)) is (uniformly) strongly G-trivial for every σ-closed subgroup G of some $\mathbb{G}_a^n$ of σ-dimension zero.

Definition 5.28. *A σ-algebraic group is a* σ-algebraic vector group *if is is isomorphic to a σ-closed subgroup of $\mathbb{G}_a^n$ for some $n \geq 1$.*

In the sequel it will often be helpful to be able to assume that G is σ-reduced. If X is a σ-variety, there exists a unique largest σ-closed σ-subvariety $X_{\sigma\text{-}\mathrm{red}}$ of X that is σ-reduced. It satisfies $k\{X_{\sigma\text{-}\mathrm{red}}\} = k\{X\}_{\sigma\text{-}\mathrm{red}}$. If G is a σ-algebraic group and k is inversive, then $G_{\sigma\text{-}\mathrm{red}}$ is a σ-closed subgroup of G ([Wib21, Cor. 2.9]).

Lemma 5.29. *Let k be an inversive σ-field and let G be a σ-algebraic group over k. If k is (uniformly) $G_{\sigma\text{-}\mathrm{red}}$-trivial, then k is (uniformly) G-trivial.*

Proof. By [Wib21, Cor. 2.8 (ii)] the functor $X \to X_{\sigma\text{-}\mathrm{red}}$ commutes with products. Thus $X_{\sigma\text{-}\mathrm{red}}$ is a $G_{\sigma\text{-}\mathrm{red}}$-torsor. A morphism $k\{X_{\sigma\text{-}\mathrm{red}}\} \to k^{[n]}$ yields a morphism $k\{X\} \to k^{[n]}$ by composing with $k\{X\} \to k\{X_{\sigma\text{-}\mathrm{red}}\}$. □

Lemma 5.30. *Let k be an inversive σ-field and let G be a σ-algebraic group over k. If k is (uniformly) strongly $G_{\sigma\text{-}\mathrm{red}}$-trivial, then k is (uniformly) strongly G-trivial.*

Proof. Let $n \geq 1$. By assumption, for every $(G_{\sigma\text{-}\mathrm{red}})_n$-torsor Y, there exists a $d \geq 1$ such that $Y_d(k, \sigma^{nd}) \neq \emptyset$. Moreover, d does not depend on the choice of Y in the uniform case.

Let X be a G_n-torsor. By [Wib21, Cor. 2.9 (ii)] the functor $X \to X_{\sigma^n\text{-}\mathrm{red}}$ commutes with products. Thus $X_{\sigma^n\text{-}\mathrm{red}}$ is a $(G_n)_{\sigma^n\text{-}\mathrm{red}}$-torsor. Clearly, $\mathbb{I}((G_n)_{\sigma^n\text{-}\mathrm{red}}) = \mathbb{I}((G_{\sigma\text{-}\mathrm{red}})_n)$. So $(G_n)_{\sigma^n\text{-}\mathrm{red}} = (G_{\sigma\text{-}\mathrm{red}})_n$ and by assumption $(X_{\sigma^n\text{-}\mathrm{red}})_d(k, \sigma^{nd}) \neq \emptyset$. So there exists a morphism of k-σ^{nd}-algebras $k\{X_{\sigma^n\text{-}\mathrm{red}}\} \to k$ which we can compose with $k\{X\} \to k\{X_{\sigma^n\text{-}\mathrm{red}}\}$ to obtain a morphism $k\{X\} \to k$ of k-σ^{nd}-algebras. So $X_d(k, \sigma^{nd}) \neq \emptyset$. □

Before tackling general σ-algebraic vectors groups of σ-dimension zero, we treat the σ-closed subgroups of $\mathbb{G}_a$.

Lemma 5.31. *Let G be a σ-closed subgroup of $\mathbb{G}_a$. If k satisfies* (P3) *(or* (P3^u)*), then k is (uniformly) G-trivial.*

Proof. Since k is uniformly $\mathbb{G}_a$-trivial (Lemma 5.1) we may assume that G is a proper σ-closed subgroup of $\mathbb{G}_a$. Moreover, by Lemma 5.29 we may assume that G is σ-reduced. The proper σ-closed subgroups of $\mathbb{G}_a$ are all defined by a linear difference equation ([DVHW17, Cor. A.3].) I.e., there exists a linear σ-equation $\mathcal{L} = \sigma^m(y) + \lambda_{m-1}\sigma^{m-1}(y) + \ldots + \lambda_0 y$ over k such that $G = \{g \in \mathbb{G}_a | \ \mathcal{L}(g) = 0\}$. Because G is σ-reduced (and using that k is inversive (Lemma 4.3)) we see that $\lambda_0 \neq 0$.

By [BW22, Example 5.4] every G-torsor is isomorphic to a G-torsor of the form $X = \{x \in \mathbb{A}^1 | \ \mathcal{L}(x) = a\}$ for some $a \in k$. Consider the linear σ-equation $\sigma(Y) = AY$ where

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ -\lambda_0 & -\lambda_1 & \cdots & -\lambda_{m-1} & a \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \in \mathrm{GL}_{m+1}(k).$$

By assumption (P3) (b) there exists $n \geq 1$ and $Y \in \mathrm{GL}_{m+1}(k^{[n]})$ with $\sigma(Y) = AY$.

Since $Y \in \mathrm{GL}_{m+1}(k^{[n]})$ there exists at least one column

$$y = \begin{bmatrix} y_0 \\ \vdots \\ y_m \end{bmatrix} \in (k^{[n]})^{m+1}$$

of Y with $y_m \neq 0$. As $\sigma(y_m) = y_m$, and the solutions are a $(k^{[n]})^\sigma$-vector space, we can assume $y_m = 1$. For such a y we have $\mathcal{L}(y_0) = a$, i.e., $y_0 \in X(k^{[n]})$. Moreover, if the stronger condition (P3^u) (b) holds, then n does not depend on A and thus it does not depend on the choice of X. □

Proposition 5.32. *Let G be a σ-algebraic vector group of σ-dimension zero. If k satisfies* (P3) *(or* (P3^u)*), then k is (uniformly) strongly G-trivial.*

Proof. We proceed by induction on the order of G. The case $\mathrm{ord}(G) = 0$ is handled by Proposition 5.3. So let us assume that $\mathrm{ord}(G) > 0$. By Corollary 5.4 we may assume that G is connected. Let $n \geq 1$. Then G_n is a σ^n-algebraic vector group (cf. Example 3.4). Say $G_n \leq \mathbb{G}_a^m$ (as σ^n-algebraic groups). As $\mathrm{ord}(G_n) = \mathrm{ord}(G) > 0$ (Lemma 3.8), at least one of the projections $G_n \to \mathbb{G}_a$ has to be non-trivial. So we have an exact sequence $1 \to N \to G_n \to H \to 1$ of σ^n-algebraic groups with H a non-trivial σ^n-closed subgroup of $\mathbb{G}_a$. Thus N is a proper σ^n-closed subgroup of G_n. As G is connected, also G_n is connected (Lemma 3.7) and therefore $\mathrm{ord}(N) < \mathrm{ord}(G_n) = \mathrm{ord}(G)$ (Lemma 5.6). So, by the induction hypothesis and Lemma 4.4 it follows that (k, σ^n) is (uniformly) strongly N-trivial. Moreover, (k, σ^n) is (uniformly) H-trivial by Lemma 5.31 (and Lemma 4.4). So it follows from Proposition 3.20(i) that (k, σ^n) is (uniformly) G_n-trivial as desired. □

5.5. **The proof for Zariski-dense σ-closed subgroups of simple algebraic groups.** Note that (P3) (b) (or (P3^u) (b)) means that k is (uniformly) GL_m^σ-trivial for all $m \geq 1$. The key to showing that this implies that k is (uniformly) G-trivial for any Zariski-dense σ-closed subgroup G of a simple algebraic group, is to first show that it implies that k is (uniformly) $\mathcal{G}^\sigma$-trivial for any closed subgroup $\mathcal{G} \leq \mathrm{GL}_m$ defined over k^σ.

Recall that a σ-ring R is called *σ-simple* if $\{0\}$ and R are the only σ-ideals of R.

Lemma 5.33. *Assume that k is algebraically closed and let R be a σ-simple k-σ-algebra such that R is finitely generated as a k-algebra and integral over k. Then there exists an $r \geq 1$ such that R is isomorphic as a k-σ-algebra to k^r equipped with $\sigma\colon k^r \to k^r, (a_1, \dots, a_r) \mapsto (\sigma(a_r), \sigma(a_1), \dots, \sigma(a_{r-1}))$ and $k \to k^r,\ \lambda \mapsto (\lambda, \dots, \lambda)$.*

Proof. Because R is finitely generated as a k-algebra and integral over k, we see that R is a finite dimensional k-vector space. Furthermore, because the nilradical of R is a σ-ideal, it must be trivial. So R is reduced. Since k is algebraically closed, it follows that R is isomorphic as a k-algebra to k^r for some $r \geq 1$. So we identify R with k^r. Because the kernel of $\sigma\colon k^r \to k^r$ is a σ-ideal, it must be trivial. So $\sigma\colon k^r \to k^r$ is injective and therefore permutes the primitive idempotent elements $e_1, \dots, e_r$ of k^r. Any subset of $e_1, \dots, e_r$ stable under σ generates a σ-ideal. Therefore σ must permute $e_1, \dots, e_r$ as cycle of length r. Without loss of generality we can assume that $\sigma(e_1) = e_2,\ \sigma(e_2) = e_3, \dots, \sigma(e_n) = e_1$. This shows that $\sigma\colon k^r \to k^r$ has the required form. □

As we will use some Galois cohomology in the upcoming proofs, we briefly recall the definitions. (See [Mil17, Section 3, k] or [Ser02] for a fuller treatment). Let k'/k be a Galois field extension with Galois group $\Gamma_{k'/k}$ and let $\mathcal{G}$ be an algebraic group over k. A continuous map $\chi\colon \Gamma_{k'/k} \to \mathcal{G}(k')$, where $\mathcal{G}(k')$ has the discrete topology, is a *cocycle* if $\chi(\gamma_1\gamma_2) = \chi(\gamma_1)\gamma_1(\chi(\gamma_2))$ for all $\gamma_1, \gamma_2 \in \Gamma_{k'/k}$. Two cocycles χ_1, χ_2 are equivalent if there exists a $g \in \mathcal{G}(k')$ such that $\chi_1(\gamma) = g^{-1}\chi_2(\gamma)\gamma(g)$ for all $\gamma \in \Gamma$. The Galois cohomology set $H^1(k'/k, \mathcal{G})$ is the set of equivalence classes of cocycles. It has a distinguished element, the equivalence class consisting of the *principal cocycles*, i.e., the cocycles of the form $\chi(\gamma) = g^{-1}\gamma(g)$ for some $g \in \mathcal{G}(k')$. Let $\Sigma_{k'/k}(\mathcal{G})$ denote the set of isomorphism classes of right $\mathcal{G}$-torsors $\mathcal{X}$ with $\mathcal{X}(k') \neq \emptyset$. For $x \in \mathcal{X}(k')$ and $\gamma \in \Gamma_{k'/k}$ there exists a unique $\chi(\gamma) \in \mathcal{G}(k')$ such that $\gamma(x) = x\chi(\gamma)$. Then $\chi\colon \Gamma_{k'/k} \to \mathcal{G}(k')$ is a cocycle and its equivalence class does not depend on the choice of $x \in \mathcal{X}(k')$. This yields a well-defined map $\Sigma_{k'/k}(\mathcal{G}) \to H^1(k'/k, \mathcal{G})$ which turns out to be a bijection under which the isomorphism class of the trivial $\mathcal{G}$-torsor corresponds to the distinguished element of $H^1(k'/k, \mathcal{G})$.

Lemma 5.34. *Assume that k is algebraically closed and let $\mathcal{G}$ be an algebraic group over k^σ. Then there exists an integer $s \geq 1$ such that for every cocycle $\Gamma_{\overline{k^\sigma}/k^\sigma} \to \mathcal{G}(\overline{k^\sigma})$ the induced cocycle $\Gamma_{\overline{k^\sigma}/k^{\sigma^s}} \to \Gamma_{\overline{k^\sigma}/k^\sigma} \to \mathcal{G}(\overline{k^\sigma})$ is principal.*

Proof. It is well known (Theorem [Lev08, Theorem 2.1.12]) that the algebraic closure $\overline{k^\sigma}$ of k^σ in k coincides with the subfield of all periodic elements of k. It follows that the absolute Galois group $\Gamma_{\overline{k^\sigma}/k^\sigma}$ of k^σ is topologically generated by $\sigma\colon \overline{k^\sigma} \to \overline{k^\sigma}$. Therefore k^σ is a field of type (F) in the sense of [Ser02, Chapter III, Section 4.2] and it follows from [Ser02, Chapter III, Section 4.3, Theorem 4] that $H^1(\overline{k^\sigma}/k^\sigma, \mathcal{G})$ is finite. Thus the set of isomorphism classes of $\mathcal{G}$-torsors is finite and so there exists an extension k^{σ^s}/k^σ such that $\mathcal{X}(k^{\sigma^s}) \neq \emptyset$ for every $\mathcal{G}$-torsor $\mathcal{X}$. The diagram

$$\begin{tikzcd}
\Sigma_{\overline{k^\sigma}/k^\sigma}(\mathcal{G}) \arrow[r] \arrow[d] & \Sigma_{\overline{k^\sigma}/k^{\sigma^s}}(\mathcal{G}_{k^{\sigma^s}}) \arrow[d] \\
H^1(\overline{k^\sigma}/k^\sigma, \mathcal{G}) \arrow[r] & H^1(\overline{k^\sigma}/k^{\sigma^s}, \mathcal{G}_{k^{\sigma^s}})
\end{tikzcd}$$

where the top horizontal arrow is given by base change from k^σ to k^{σ^s} and the bottom horizontal arrow is induced by composing a cocycle with $\Gamma_{\overline{k^\sigma}/k^{\sigma^s}} \to \Gamma_{\overline{k^\sigma}/k^\sigma}$ is commutative. By choice of s, the top horizontal map is trivial. Therefore also the bottom horizontal map is trivial. This implies the claim of the lemma. $\square$

With these two lemmata at hand, we can strengthen conditions (P3)(b) and (P3^u)(b) from solutions in GL_m to solutions in closed subgroups $\mathcal{G} \leq \mathrm{GL}_m$ defined over k^σ:

Proposition 5.35. *If k satisfies* (P3) *then the following stronger version of* (P3)*(b) also holds: For every pair of integers $m, d \geq 1$, every closed subgroup $\mathcal{G} \leq \mathrm{GL}_m$ defined over k^σ and every $A \in \mathcal{G}(k)$, there exists an integer $n \geq 1$ such that the equation $\sigma^d(Y) = AY$ has a solution in $\mathcal{G}(k^{[n]})$. Moreover, if k satisfies* (P3^u)*, then n can be chosen uniformly for all $A \in \mathcal{G}(k)$.*

Proof. Let $m, d \geq 1$ be integers and $\mathcal{G} \leq \mathrm{GL}_m$ a closed subgroup defined over k^σ. If (P3^u)(b) holds, then we use (P3^u)(b$_d$') from Lemma 4.2 and obtain an $l \in \mathbb{N}$ such that for all $A \in \mathcal{G}(k)$ there exists a $Y \in \mathrm{GL}_m(k)$ with $\sigma^{dl}(Y) = \sigma^{(l-1)d}(A) \ldots \sigma^d(A)AY$. If instead (P3) holds, then such an l also exists but it may depend on A. We fix an $A \in \mathcal{G}(k)$ and abbreviate $B = \sigma^{(l-1)d}(A) \ldots \sigma^d(A)A$. Note that $B \in \mathcal{G}(k)$ because $\mathcal{G} \leq \mathrm{GL}_m$ is defined over k^σ. Let $s \geq 1$ be as in the statement of Lemma 5.34 but applied to the difference field (k, σ^{dl}). We claim that there exists a $\hat{Y} \in \mathcal{G}(k)$ with $\sigma^{sdl}(\hat{Y}) = \sigma^{(s-1)dl}(B) \ldots \sigma^{dl}(B)B\hat{Y}$. Note that this implies the claim of the proposition by Lemma 4.1 because $\sigma^{(s-1)dl}(B) \ldots \sigma^{dl}(B)B = \sigma^{(ls-1)d}(A) \ldots \sigma^d(A)A$ and ls is uniform in A if (P3^u) holds.

Define $\tilde{\sigma} = \sigma^{dl}$ and let $T = (T_{ij})$ be the matrix of coordinate functions on GL_m. Consider the coordinate ring $k[\mathrm{GL}_m] = k[T, 1/\det(T)]$ of GL_m over k as a k-$\tilde{\sigma}$-algebra via $\tilde{\sigma}(T) = BT$. Let $\mathbb{I}(\mathcal{G}) \subseteq k[\mathrm{GL}_m]$ be the defining ideal of $\mathcal{G}$ and let $f = f(T) \in \mathbb{I}(\mathcal{G})$ have constant coefficients. Then $\tilde{\sigma}(f(T))(g) = f(\tilde{\sigma}(T))(g) = f(BT)(g) = f(Bg) = 0$ for all $g \in \mathcal{G}(k)$ because $Bg \in \mathcal{G}(k)$. So $\tilde{\sigma}(f) \in \mathbb{I}(\mathcal{G})$. Because $\mathcal{G}$ is defined over k^σ this shows that $\mathbb{I}(\mathcal{G}) \subseteq k[\mathrm{GL}_m]$ is a $\tilde{\sigma}$-ideal.

Thus we can find a maximal $\tilde{\sigma}$-ideal $\mathfrak{m} \subseteq k[\mathrm{GL}_m]$ that contains $\mathbb{I}(\mathcal{G})$. The quotient $R = k[\mathrm{GL}_m]/\mathfrak{m}$ is then a $\tilde{\sigma}$-simple k-$\tilde{\sigma}$-algebra. By construction, the image $\tilde{Y}$ in $\mathrm{GL}_m(R)$ of T is contained in $\mathcal{G}(R)$ and satisfies $\tilde{\sigma}(\tilde{Y}) = B\tilde{Y}$. Recall, from the first paragraph, that we have a $Y \in \mathrm{GL}_m(k)$ with $\tilde{\sigma}(Y) = BY$. Since two solutions matrices only differ by a constant matrix, there exists a $C \in \mathrm{GL}_m(R^{\tilde{\sigma}})$ with $\tilde{Y} = YC$ and we conclude that $R = k[\tilde{Y}, 1/\det(\tilde{Y})] = k[C, 1/\det(C)]$ is generated as a k-algebra by the elements in $R^{\tilde{\sigma}}$. As R is $\tilde{\sigma}$-simple, $R^{\tilde{\sigma}}$ is a field. Moreover, it is an algebraic extension of $k^{\tilde{\sigma}}$. (This is well-known in case $k^{\tilde{\sigma}}$ is algebraically closed [vdPS97, Lemma 1.8] and follows similarly in the general case. It also follows from [Wib12, Prop. 2.11]). Note, however, that $R^{\tilde{\sigma}}$ need not be contained in k because R need not be an integral domain. In any case, R is generated as a k-algebra by elements that are integral over k and therefore R itself is integral over k. By Lemma 5.33 we have $R = k^r$ with $\tilde{\sigma}\colon k^r \to k^r, (a_1, \ldots, a_r) \mapsto (\tilde{\sigma}(a_r), \tilde{\sigma}(a_1), \ldots, \tilde{\sigma}(a_{r-1}))$ for some $r \geq 1$. Then $R^{\tilde{\sigma}} = \{(a, \tilde{\sigma}(a), \ldots, \tilde{\sigma}^{r-1}(a)) \mid a \in k^{\tilde{\sigma}^r}\}$. So there exists a matrix $D \in \mathrm{GL}_m(k^{\tilde{\sigma}^r})$ with $C = (D, \tilde{\sigma}(D), \ldots, \tilde{\sigma}^{r-1}(D))$. Thus $\tilde{Y} \in \mathcal{G}(R)$ can be rewritten as $\tilde{Y} = YC = (YD, Y\tilde{\sigma}(D), \ldots, Y\tilde{\sigma}^{r-1}(D))$. Because $\tilde{Y} \in \mathcal{G}(R)$, we conclude that $Y\tilde{\sigma}^i(D) \in \mathcal{G}(k)$ for $i = 0, \ldots, r-1$. This implies $D^{-1}\tilde{\sigma}^i(D) = (YD)^{-1}Y\tilde{\sigma}^i(D) \in \mathcal{G}(k^{\tilde{\sigma}^r})$.

The Galois group $\Gamma_{k^{\tilde{\sigma}^r}/k^{\tilde{\sigma}}}$ of $k^{\tilde{\sigma}^r}$ over $k^{\tilde{\sigma}}$ is generated by $\tilde{\sigma}\colon k^{\tilde{\sigma}^r} \to k^{\tilde{\sigma}^r}$. (However, the order of $\tilde{\sigma} \in \Gamma_{k^{\tilde{\sigma}^r}/k^{\tilde{\sigma}}}$ could be less than r). In any case, we can define a map $\chi\colon \Gamma_{k^{\tilde{\sigma}^r}/k^{\tilde{\sigma}}} \to \mathcal{G}(k^{\tilde{\sigma}^r})$ by $\chi(\tilde{\sigma}^i) = D^{-1}\tilde{\sigma}^i(D)$ for $i = 0, \ldots, r-1$. It is straight forward to check that χ is a cocycle. Note that χ may not be principal because we don't know if D lies in $\mathcal{G}(k^{\tilde{\sigma}^r})$. By the choice of s, the induced cocycle $\overline{\chi}\colon \Gamma_{\overline{k^{\tilde{\sigma}}}/k^{\tilde{\sigma}}} \to \Gamma_{k^{\tilde{\sigma}^r}/k^{\tilde{\sigma}}} \xrightarrow{\chi} \mathcal{G}(k^{\tilde{\sigma}^r}) \to \mathcal{G}(\overline{k^{\tilde{\sigma}}})$ becomes principal, when restricted to $\Gamma_{\overline{k^{\tilde{\sigma}}}/k^{\tilde{\sigma}^s}} \leq \Gamma_{\overline{k^{\tilde{\sigma}}}/k^{\tilde{\sigma}}}$. In particular, there exists a matrix $E \in \mathcal{G}(\overline{k^{\tilde{\sigma}}})$ such that $E^{-1}\tilde{\sigma}^s(E) = D^{-1}\tilde{\sigma}^s(D)$. But then $\tilde{\sigma}^s(DE^{-1}) = DE^{-1}$ and so $DE^{-1} \in \mathrm{GL}_m(k^{\tilde{\sigma}^s})$. Set $\hat{Y} = YDE^{-1} \in \mathrm{GL}_m(k)$. Because $YD \in \mathcal{G}(k)$ and $E \in \mathcal{G}(k)$ we have $\hat{Y} \in \mathcal{G}(k)$. Since $\tilde{\sigma}(Y) = BY$, we have $\tilde{\sigma}^s(Y) = \tilde{\sigma}^{(s-1)}(B)\ldots\tilde{\sigma}(B)BY$ and because $DE^{-1} \in \mathrm{GL}_m(k^{\tilde{\sigma}^s})$, $\hat{Y}$ must satisfy the same linear $\tilde{\sigma}^s$-equation. So $\hat{Y} \in \mathcal{G}(k)$ and $\tilde{\sigma}^s(\hat{Y}) = \tilde{\sigma}^{(s-1)}(B)\ldots\tilde{\sigma}(B)B\hat{Y}$ as desired. □

Lemma 5.36. *Let $\mathcal{G} \leq \mathrm{GL}_m$ be a closed subgroup defined over k^σ and consider the σ-algebraic group $G = \{g \in \mathcal{G} |\ \sigma(g) = g\}$. If k satisfies* (P3) *(or* (P3^u)*) then k is (uniformly) strongly G-trivial.*

Proof. For $n \geq 1$ the σ^n-algebraic group $G_n = \{g \in \mathcal{G} |\ \sigma^n(g) = g\}$ is of the same form as G. So, using Lemma 4.4, it suffices to show that k is G-trivial.

According to [BW22, Cor. 6.3] (with $d = 1$ and ψ the identity map) every G-torsor is isomorphic to a G-torsor of the form $X' = \{x' \in \mathcal{G} |\ \sigma(x') = x'A'\}$ for some $A' \in \mathcal{G}(k)$, where G is acting by $(g, x) \mapsto gx$. Let $X = \{x \in \mathcal{G} |\ \sigma(x) = Ax\}$ where $A = A'^{-1}$ and G is acting on X by $(g, x) \mapsto xg^{-1}$. Then $X' \to X$, $x' \mapsto x'^{-1}$ is an isomorphism of G-torsors. The stronger versions of assumption (P3) (b) and (P3^u) (b) in Proposition 5.35 (with $d = 1$) imply $X(k^{[n]}) \neq \emptyset$ for some $n \geq 1$. If k satisfies (P3^u), then n can be chosen uniformly for all G-torsors. □

Recall that a non-commutative algebraic group of positive dimension (over an algebraically closed field of characteristic zero) is called *(almost-)simple* if every proper normal closed subgroup is trivial (respectively finite). The simple algebraic groups are sometimes also referred to as the almost-simple algebraic groups of adjoint type.

Proposition 5.37. *Let G be a proper Zariski-dense σ-reduced σ-closed subgroup of a simple algebraic group $\mathcal{G}$. If k satisfies* (P3) *(or* (P3^u)*) then k is (uniformly) strongly G-trivial.*

Proof. The idea of the proof is to show that for some $d \geq 1$ the difference algebraic group G_d is isomorphic to one of the difference algebraic groups treated in Lemma 5.36.

By [DVHW17, Prop. A.19] (Cf. the proof of [CHP02, Prop. 7.10)].) we know that

$$G = \{g \in \mathcal{G} |\ \sigma^n(g) = \varphi(g)\}$$

for some $n \geq 1$ and some isomorphism $\varphi\colon \mathcal{G} \to {}^{\sigma^n}\mathcal{G}$ of algebraic groups over k. Let us fix an embedding of $\mathcal{G}$ into GL_m such that $\mathcal{G}$ is defined over $\mathbb{Q}$ inside GL_m. (This is possible because the simple algebraic groups are defined over $\mathbb{Q}$.) As in the proof of [DVHW17, Theorem A.20] it follows that there exists a matrix $h \in \mathcal{G}(k)$ and an integer $e \geq 1$ such that $\sigma^{ne}(g) = hgh^{-1}$ for all $g \in G$.

Consider the equation $\sigma^{ne}(Y) = hY$. The stronger versions of (P3)(b) and (P3^u)(b) obtained in Proposition 5.35 (applied with $d = ne$) together with Lemma 4.1 both imply that there exists an integer $l \geq 1$ such that the equation $\sigma^{nel}(Y) = \sigma^{(l-1)ne}(h)\ldots\sigma^{ne}(h)hY$ has a solution $u \in \mathcal{G}(k)$. From $\sigma^{ne}(g) = hgh^{-1}$ it follows that $\sigma^{nel}(g) = \sigma^{(l-1)ne}(h)\ldots hg(\sigma^{(l-1)ne}(h)\ldots h)^{-1}$. Therefore $\sigma^{nel}(u^{-1}gu) = u^{-1}gu$ for all $g \in G$. Now $g \mapsto u^{-1}gu$ is an automorphism of $\mathcal{G}$ that maps G isomorphically to a σ-closed subgroup G' of $\mathcal{G}$. Indeed,

$$G' = \{g \in \mathcal{G} |\ \sigma^n(g) = v\varphi(g)v^{-1}\},$$

where $v = \sigma^n(u^{-1})\varphi(u) \in \mathcal{G}(k)$.

Let $T = (T_{ij})$ denote the $m \times m$-matrix of coordinate functions on $\mathcal{G}$. Then the σ-coordinate ring $k\{G'\}$ of G' equals

$$k\{G'\} = k[\mathcal{G}^n] = k[T, 1/\det(T), \sigma(T), 1/\det(\sigma(T)), \ldots, \sigma^{n-1}(T), 1/\det(\sigma^{n-1}(T))]$$

with σ determined by $\sigma(\sigma^{n-1}(T)) = v\varphi(T)v^{-1}$. As $\sigma^{nel}(g) = g$ for all $g \in G'$ we have $\sigma^{nel}(T) = T$. Thus $\sigma^{nel}(\sigma^i(T)) = \sigma^i(T)$ for $i = 0, \ldots, n-1$. This shows that for $d = nel$ the σ^d-algebraic group G'_d

is isomorphic to the σ^d-algebraic group $H = \{h \in \mathcal{G}^n \mid \sigma^d(h) = h\}$. Therefore, also G_d is isomorphic to H. As (k, σ^d) satisfies (P3) or (P3^u), respectively, by Lemma 4.4, we know from Lemma 5.36 that H is (uniformly) strongly (k, σ^d)-trivial. So G_d is (uniformly) strongly (k, σ^d)-trivial, and therefore G is (uniformly) strongly k-trivial (Lemma 3.17). □

5.6. **The proof for σ-algebraic groups of σ-dimension zero.** In this subsection we show that if k satisfies (P3) (or (P3^u)) then k is (uniformly) strongly G-trivial for every σ-algebraic group G with $\sigma\text{-}\dim(G) = 0$. The idea for the proof is to reduce to the three special cases treated in the three previous subsections (diagonalizable σ-algebraic groups, σ-algebraic vector groups and Zariski-dense σ-reduced σ-closed subgroups of simple algebraic groups).

Lemma 5.38. *Assume that k is algebraically closed. Let G be a connected σ-algebraic group of positive order. Then there exists a proper normal σ-closed subgroup N of G such that G/N is isomorphic to a Zariski-dense σ-closed subgroup of $\mathbb{G}_a$, $\mathbb{G}_m$ or a simple algebraic group.*

Proof. First of all, note that if $\mathcal{G}$ is a connected algebraic group of positive dimension, then there exists a proper normal closed subgroup $\mathcal{N}$ of $\mathcal{G}$ such that $\mathcal{G}/\mathcal{N}$ is isomorphic to $\mathbb{G}_a$, $\mathbb{G}_m$ or a simple algebraic group. To see this, simply choose a proper normal closed subgroup $\mathcal{N}'$ of maximal dimension. If $\mathcal{G}/\mathcal{N}'$ is abelian, then it follows from the structure theory of abelian algebraic groups [Mil17, Cor. 16.15] that $\mathcal{G}/\mathcal{N}'$ is isomorphic to $\mathbb{G}_a$ or $\mathbb{G}_m$. If $\mathcal{G}/\mathcal{N}'$ is non-commutative, then $\mathcal{G}' = \mathcal{G}/\mathcal{N}'$ is almost-simple and therefore $\mathcal{G}'/Z(\mathcal{G}')$ is simple.

Now let $\mathcal{G}$ be an algebraic group such that G embeds into $\mathcal{G}$ as a Zariski-dense σ-closed subgroup. Then $\mathcal{G}$ is connected and has positive dimension. As argued above, there exists a proper normal closed subgroup $\mathcal{N}$ of $\mathcal{G}$ such that $\mathcal{G}/\mathcal{N}$ is isomorphic to a simple algebraic group, $\mathbb{G}_a$ or $\mathbb{G}_m$.

Now $N = \mathcal{N} \cap G$ is a normal σ-closed subgroup of G. Suppose $\mathcal{N} \cap G = G$, then $G \subseteq \mathcal{N}$. So $\mathcal{N} = \mathcal{G}$, because $\mathcal{G}$ is Zariski-dense in $\mathcal{G}$. Therefore N is properly contained in G and we have an embedding $G/N \to \mathcal{G}/\mathcal{N}$. As G is Zariski-dense in $\mathcal{G}$, we see that G/N is Zariski-dense in $\mathcal{G}/\mathcal{N}$. □

Proposition 5.39. *Let G be a σ-algebraic group of σ-dimension zero. If k satisfies* (P3) *(or* (P3^u)*) then k is (uniformly) strongly G-trivial.*

Proof. We will prove this by induction on $\mathrm{ord}(G)$. The case when G has order zero is treated in Proposition 5.3. So we can assume $\mathrm{ord}(G) > 0$. By Corollary 5.4 we may assume that G is connected. According to Lemma 5.38 there exists a proper normal σ-closed subgroup N of G such that G/N is isomorphic to a Zariski-dense σ-closed subgroup of $\mathbb{G}_a$, $\mathbb{G}_m$ or a simple algebraic group. As $\mathrm{ord}(N) < \mathrm{ord}(G)$, we can use the induction hypothesis together with Proposition 3.20 (ii) to reduce to the case that G is a Zariski-dense σ-closed subgroup of $\mathbb{G}_a$, $\mathbb{G}_m$ or a simple algebraic group. The case when G is a σ-closed subgroup of $\mathbb{G}_a$ follows from Proposition 5.32 and the case when G is a σ-closed subgroup of $\mathbb{G}_m$ follows from Proposition 5.27. So it only remains to treat the case when G is a Zariski-dense σ-closed subgroup of a simple algebraic group. If $G_{\sigma\text{-}\mathrm{red}}$ is a proper σ-closed subgroup of G, then we can use the induction hypothesis and Lemma 5.30 to conclude. Thus we can assume that $G = G_{\sigma\text{-}\mathrm{red}}$, i.e., G is a proper σ-reduced σ-closed subgroup of a simple algebraic group. This case is treated in Proposition 5.37. □

5.7. **Conclusion.** In this subsection we complete the proof of (P3)⇒(P1) by showing that a σ-field satisfying (P3) is strongly G-trivial for every σ-algebraic group G.

Recall that we defined the meaning of almost-simple for σ-algebraic groups of σ-dimension zero and positive order in Definition 5.5. Following [Wib21, Def. 7.10] we extend the definition to σ-algebraic groups of positive σ-dimension as follows. Assume that k is algebraically closed and inversive. A σ-algebraic group over k of positive σ-dimension is *almost-simple* if it is perfectly σ-reduced and every proper normal σ-closed subgroup has σ-dimension zero.

Lemma 5.40. *Let G be an almost-simple σ-algebraic group with $\sigma\text{-}\dim(G) > 0$. If k satisfies* (P3) *(or* (P3^u)*), then k is (uniformly) strongly G-trivial.*

Proof. By [Wib21, Cor. 8.12], there exists a normal σ-closed subgroup N of G with $\sigma\text{-}\dim(N) = 0$ and an algebraic group $\mathcal{G}$ such that $G/N \cong [\sigma]_k\mathcal{G}$. As k is (uniformly) strongly N-trivial by Proposition 5.39 and also uniformly strongly $[\sigma]_k\mathcal{G}$-trivial by Lemma 5.1, it follows that k is (uniformly) strongly G-trivial by Proposition 3.20(ii). □

Lemma 5.41. *If G is a connected σ-algebraic group, then also $G_{\sigma\text{-}\mathrm{red}}$ is connected.*

Proof. As G is connected, the zero ideal of $k\{G\}$ is prime. Therefore $\mathbb{I}(G_{\sigma\text{-}\mathrm{red}}) = \bigcup_{n\geq 1}\sigma^{-n}(\{0\})$ is a prime ideal. Thus $G_{\sigma\text{-}\mathrm{red}}$ is connected. ☐

Every σ-algebraic group G with $\sigma\text{-}\dim(G) > 0$ contains a unique smallest σ-closed subgroup G^{so} with $\sigma\text{-}\dim(G^{so}) = \sigma\text{-}\dim(G)$ ([Wib21, Lemma 6.18]), the *strong identity component* of G. The σ-algebraic group G is *strongly connected* if $G = G^{so}$, i.e., for every proper σ-closed subgroup H of G we have $\sigma\text{-}\dim(H) < \sigma\text{-}\dim(G)$. Note that G^{so} is strongly connected.

Theorem 5.42. *Let G be a σ-algebraic group. If k satisfies* (P3) *(or* (P3^u)*) then k is (uniformly) strongly G-trivial.*

Proof. By Lemma 5.4 we can assume that G is connected. By Lemmas 5.30 and 5.41 we can also assume that G is σ-reduced. So G is σ-integral and in particular perfectly σ-reduced. Furthermore, by Proposition 5.39 we may assume that $\sigma\text{-}\dim(G) > 0$. As G is perfectly σ-reduced, it follows from [Wib21, Cor. 6.26] that G^{so} is normal in G and we can consider the exact sequence $1 \to G^{so} \to G \to G/G^{so} \to 1$. Because $\sigma\text{-}\dim(G/G^{so}) = 0$, we know from Proposition 5.39 that k is (uniformly) strongly G/G^{so}-trivial. By Proposition 3.20 (ii) we can thus assume that G is strongly connected. Then by [Wib21, Theorem 7.13], there exists a subnormal series

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = 1$$

of strongly connected σ-closed subgroups such that the quotients G_i/G_{i+1} are almost-simple for $i = 0,\ldots,n-1$. So it follows from Lemma 5.40 and Corollary 3.21 that k is (uniformly) strongly G-trivial. ☐

We are finally in a position to complete the proof of our main results (Theorems 1.3) and 1.2) from the introduction.

Proof of Theorems 1.3 and 1.2. Let k be a σ-field (of characteristic zero). The equivalences (P1)$\Leftrightarrow$(P2) and (P1^u)$\Leftrightarrow$(P2^u) are in Proposition 3.19. The implications (P1)$\Rightarrow$(P3) and (P1^u)$\Rightarrow$(P3^u) are in Proposition 4.5. The implications (P3)$\Rightarrow$(P3) and (P3^u)$\Rightarrow$(P1^u) follow from Theorem 5.42. ☐

6. Torsors over σ-closed σ-fields

In this short section, we show that σ-closed σ-fields satisfy condition (P1^u).

Recall that a σ-field k is *σ-closed* if every system of algebraic difference equations over k that has a solution in a σ-field extension of k, already has a solution in k. Note that, due to the basis theorem ([Lev08, Theorem 2.5.11]), the system of algebraic difference equations in this definition can be assumed to be finite. The model theory of σ-closed σ-field has been studied extensively (see e.g., [CH99]). In the model theoretic context, σ-closed σ-fields are usually referred to as models of ACFA. The following simple lemma translates the definition of σ-closed σ-fields into the language of k-σ-algebras.

Lemma 6.1. *A σ-field k is σ-closed if and only if for every finitely σ-generated k-σ-algebra R such that there exists a σ-ideal of R that is prime, there exists a morphism $R \to k$ of k-σ-algebras.*

Proof. First assume that k is σ-closed. Let R be a finitely σ-generated k-σ-algebra R such that there exists a prime σ-ideal $\mathfrak{p}$ of R. Then $\mathfrak{p}^* = \{r \in R| \ \exists\ n \geq 1 : \ \sigma^n(r) \in \mathfrak{p}\}$ is a prime ideal of R with $\sigma^{-1}(\mathfrak{p}) = \mathfrak{p}$. Therefore $R/\mathfrak{p}^*$ is a σ-ring with $\sigma\colon R/\mathfrak{p}^* \to R/\mathfrak{p}^*$ injective. Thus the residue field $k(\mathfrak{p}^*)$ of $\mathfrak{p}^*$ is naturally a σ-field and the canonical map $R \to k(\mathfrak{p})$ is a morphism of k-σ-algebras. Writing $R = k\{y_1,\ldots,y_n\}/I$ for some σ-ideal I of $k\{y_1,\ldots,y_n\}$, we see that the morphism $R \to k(\mathfrak{p}^*)$ corresponds to a solution of I in $k(\mathfrak{p}^*)$. As k is σ-closed, this shows that there exists a solution of I in k. This solution defines a morphism $R = k\{y_1,\ldots,y_n\}/I \to k$ of k-σ-algebras.

Conversely, let $F \subseteq k\{y_1,\ldots,y_n\}$ define a system of algebraic difference equations over k that has a solution in some σ-field extension k' of k. Then $R = k\{y_1,\ldots,y_n\}/[F]$ is a finitely σ-generated k-σ-algebra and the solution of $F = 0$ in k' defines a morphism $R = k\{y_1,\ldots,y_n\}/[F] \to k'$ of k-σ-algebras. The kernel of this morphism is a prime σ-ideal. Thus, by assumption, there exists a morphism $R = k\{y_1,\ldots,y_n\}/[F] \to k$ of k-σ-algebras. The image of the σ-generators defines a solution of $F = 0$ in k. Therefore, k is σ-closed. ☐

As not every finitely σ-generated k-σ-algebra contains a prime σ-ideal, it is crucial that the assumption about the existence of a prime σ-ideal is included in Lemma 6.1.

Lemma 6.2. *If (k,σ) is a σ-closed σ-field, then (k,σ^n) is a σ^n-closed σ^n-field for every $n\geq 1$.*

Proof. This is well-known (Corollary to Lemma 1.12 in [CH99]) and can also quickly be seen using the constructions from Section 3.1: Let R be a finitely σ^n-generated k-σ^n-algebra such that there exists a prime σ^n-ideal of R. As in the proof of Lemma 6.1, the prime σ^n-ideal defines a morphism $R\to k'$ of k-σ^n-algebras into a σ^n-field extension k' of k. Then ${}_1R\to {}_1(k')$ is a morphism of k-σ-algebras and because ${}_1(k')$ is an integral domain (as σ-closed σ-fields are algebraically closed), we see that the kernel is a prime σ-ideal of ${}_1R$. Thus, by Lemma 6.1, there exists a morphism ${}_1R\to k$ of k-σ-algebras. The composition $R\to {}_1R\to k$ then is a morphism of k-σ^n-algebras. So (k,σ^n) is σ^n-closed by Lemma 6.1. $\square$

Proposition 6.3. *Let k be a σ-closed σ-field and G a σ-algebraic group over k. Then there exists an $n\geq 1$ such that $X(k^{[n]})\neq\emptyset$ for every G-torsor X. In other words, a σ-closed σ-field satisfies the equivalent conditions of Theorem 1.3.*

Proof. We first show that k is uniformly strongly G-trivial for every connected σ-algebraic group G. So let $n\geq 1$ and let X be a G_n-torsor. We then have, in particular, an isomorphism $k\{X\}\otimes_k k\{X\}\simeq k\{G\}\otimes_k k\{X\}$ of $k\{X\}$-algebras. Fixing a morphism $k\{X\}\to k'$ of k-algebras into some field extension k' of k, we can base change this isomorphism to obtain an isomorphism $k\{X\}\otimes_k k'\simeq k\{G\}\otimes_k k'$. Because G is connected (and we are in characteristic zero), $k\{G\}$ is an integral domain ([Wib21, Lemma 6.7]). Moreover, $k\{G\}\otimes_k k'$ is an integral domain (e.g., using that k is algebraically closed) and therefore $k\{X\}$ is an integral domain. So the zero ideal of $k\{X\}$ is a prime σ^n-ideal of $k\{X\}$. Because k is σ^n-closed (Lemma 6.2), there exists a morphism $k\{X\}\to k$ of k-σ^n-algebras. Thus X is trivial and k is uniformly strongly G-trivial as claimed.

Because k is algebraically closed and inversive, it follows from Corollary 5.4 that k is uniformly strongly G-trivial for every σ-algebraic group G over k. In particular, k is uniformly G-trivial for every σ-algebraic group G over k as claimed. $\square$

While Proposition 6.3 is a statement about σ-closed σ-fields, we can nevertheless deduce from it a statement about arbitrary σ-fields (of characteristic zero). Note that if K is a σ-field extension of k and $n\geq 1$, then $k^{[n]}=(k,\sigma^n)_1$ is a k-σ-subalgebra of $K_1=(K,\sigma^n)_1$ and K_1 is an n-fold product of field extension of k.

Corollary 6.4. *Let G be a σ-algebraic group. Then there exists a σ-field extension K of k and an integer $n\geq 1$ such that $X(K_1)\neq\emptyset$ for every G-torsor X.*

Proof. Every σ-field can be embedded into a σ-closed σ-field ([CH99, Theorem 1.1]). So let K be a σ-closed σ-field containing k. By Proposition 6.3 there exists an $n\geq 1$ such that $Y(K^{[n]})\neq\emptyset$ for every G_K-torsor Y. As X_K is a G_K-torsor, we have in particular, $X(K_1)=X_K(K^{[n]})\neq\emptyset$. $\square$

One can also show directly that a σ-closed σ-field satisfies (P3^u), which, by Theorem 1.3, is equivalent to (P1^u). In fact, a σ-closed σ-field satisfies (P3^u) (b) and (P3^u) (c) with $n=1$. To see this, it suffices to show that the relevant difference equations have a solution in a σ-field extension of k. For (b), if $A\in\mathrm{GL}_n(k)$ and $k(T_{ij})=k(\mathrm{GL}_n)$ is the function field of GL_n, we can simply define $\sigma\colon k(\mathrm{GL}_n)\to k(\mathrm{GL}_n)$ by $\sigma(T)=AT$. Then clearly T is a solution of $\sigma(Y)=AY$ in some σ-field extension of k. For (c) we can invoke the classical existence theorem from difference algebra ([Lev08, Theorem 7.2.1]) which implies that any non-constant difference polynomial over k has a solution in some σ-field extension of k.

7. An application to Picard-Vessiot theory

Difference algebraic groups arise naturally as Galois groups of linear differential equations depending on a discrete parameter. The solution rings in this context are called σ-Picard-Vessiot rings. They play a role similar to the splitting field in classical Galois theory. Torsors for difference algebraic groups arise when studying isomorphisms between two σ-Picard-Vessiot rings for the same linear differential equation. In this section we apply our main results (Theorems 1.3 and 1.2 to improve the known uniqueness results for σ-Picard-Vessiot rings.

We briefly recall the setup from [DVHW14]. A *$\delta\sigma$-ring* is a commutative ring R together with a derivation $\delta\colon R \to R$ and a ring endomorphism $\sigma\colon R \to R$ such that $\delta(\sigma(r)) = \hbar\sigma(\delta(r))$ for all $r \in R$ for some fixed unit $\hbar \in R^\delta$. If moreover R is a field, it is called a $\delta\sigma$-field. If K is a $\delta\sigma$-field, then a K-algebra R with the structure of a $\delta\sigma$-ring such that $K \to R$ is compatible with δ and σ is called a *K-$\delta\sigma$-algebra*. A *δ-ideal* is an ideal $\mathfrak{a} \subseteq R$ such that $\delta(\mathfrak{a}) \subseteq \mathfrak{a}$. If $\{0\}$ and R are the only δ-ideals of R, the R is called *δ-simple*.

The *δ-constants* of a $\delta\sigma$-ring R are defined as $R^\delta = \{r \in R \mid \delta(r) = 0\}$. Note that R^δ is a σ-ring, and in particular, if K is a $\delta\sigma$-field, then K^δ is a σ-field.

In what follows we work over a $\delta\sigma$-field K of characteristic zero and let $k = K^\delta$ be the σ-field of δ-constants. We consider a linear differential equation $\delta(y) = Ay$ for some matrix $A \in K^{m\times m}$.

Definition 7.1. *A* σ-Picard-Vessiot ring *for $\delta(y) = Ay$ is a K-$\delta\sigma$-algebra R such that*

- *there exists a matrix $Y \in \mathrm{GL}_m(R)$ with $\delta(Y) = AY$ and $R = K\{Y, 1/\det(Y)\}$,*
- *R is δ-simple,*
- *$R^\delta = k$.*

The σ-Galois group G of R/K is defined as the functor from the category of k-σ-algebras to the category of groups given by

$$G(S) = \mathrm{Aut}^{\delta\sigma}(R \otimes_k S/K \otimes_k S)$$

for any k-σ-algebra S, i.e., we consider automorphisms of $R \otimes_k S$ that are the identity on $K \otimes_k S$ and commute with both σ and δ, where $R \otimes_k S$ is considered as a $\delta\sigma$-ring with δ being the trivial derivation on S, i.e., $\delta(s) = 0$ for $s \in S$. It is a σ-algebraic group over k ([DVHW14, Prop. 2.5]).

In general, a σ-Picard-Vessiot ring for a given differential equation $\delta(y) = Ay$ is not unique (up to isomorphism). Under the assumption that the σ-field $k = K^\delta$ is σ-closed, it is known that a σ-Picard Vessiot ring is unique up to powers of σ, i.e., if R_1 and R_2 are σ-Picard Vessiot rings for the same differential equation $\delta(y) = Ay$, then there exists an integer $n \geq 1$ (possibly depending on R_1 and R_2) such that (R_1, δ, σ^n) and (R_2, δ, σ^n) are isomorphic as k-$\delta\sigma^n$-algebras ([DVHW14, Cor. 1.17]). We improve this as follows:

Theorem 7.2. *Let K be a $\delta\sigma$-field of characteristic zero and let $A \in K^{m\times m}$.*

(i) *If $k = K^\delta$ satifies the equivalent conditions of Theorem 1.2, then for any two σ-Picard-Vessiot rings R and R' for $\delta(y) = Ay$, there exists an $n \geq 1$ such that R and R' are isomorphic as K-$\delta\sigma^n$-algebras.*

(ii) *If $k = K^\delta$ satifies the equivalent conditions of Theorem 1.3 (e.g., k is σ-closed), then there exists an $n \geq 1$ such that any two σ-Picard-Vessiot rings for $\delta(y) = Ay$ are isomorphic as K-$\delta\sigma^n$-algebras.*

Proof. Let R and R' be σ-Picard-Vessiot rings for $\delta(y) = Ay$ and let G be the σ-Galois group of R/K. Consider the functor X from the category of k-σ-algebras to the category of sets given by $X(S) = \mathrm{Isom}^{\delta\sigma}_{K\otimes_k S}(R \otimes_k S, R' \otimes_k S)$ for every k-σ-algebra S. So $X(S)$ is the set of $K \otimes_k S$-$\delta\sigma$-isomorphisms from $R \otimes_k S$ to $R' \otimes_k S$, where S is considered as a constant δ-ring. In the first step of the proof of [BW22, Theorem 6.4] is is shown that X is a G-torsor. Thus, if (P1) holds, then there exists an $n \geq 1$ such that $X(k^{[n]}) \neq \emptyset$, i.e., there exists an isomorphism

$$R \otimes_k k^{[n]} \to R' \otimes_k k^{[n]} \tag{8}$$

of $K \otimes_k k^{[n]}$-$\delta\sigma$-algebras. The projection $k^{[n]} \to k$ onto the last factor is a morphism of k-σ^n-algebras. Thus if we base change (8) via $k^{[n]} \to k$ we obtain an isomorphism $R \to R'$ of K-$\delta\sigma^n$-algebras. This proves (i).

If k satisfies (P1^u), then we can find an n that is uniform in X, i.e., independent of R'. The dependence of n on R can then easily be eliminated: Let R_1 and R_2 be two σ-Picard-Vessiot rings for $\delta(y) = Ay$. Then R_1 is isomorphic to R as a K-$\delta\sigma^n$-algebra and R_2 is isomorphic to R as a K-$\delta\sigma^n$-algebra. Thus R_1 and R_2 are isomorphic as K-$\delta\sigma^n$-algebras. ∎

References

[BW22] Annette Bachmayr and Michael Wibmer. Torsors for difference algebraic groups. *Commun. Contemp. Math.*, 24(9):Paper No. 2150068, 34, 2022.

[CH99] Zoé Chatzidakis and Ehud Hrushovski. Model theory of difference fields. *Trans. Amer. Math. Soc.*, 351(8):2997–3071, 1999.

[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.

[CK23] Marcin Chalupnik and Piotr Kowalski. Difference sheaves and torsors. *Fund. Math.*, 260(2):111–161, 2023.

[Coh65] Richard M. Cohn. *Difference algebra*. Interscience Publishers John Wiley & Sons, New York-London-Sydney, 1965.

[CP19] Zoé Chatzidakis and Anand Pillay. Generalized Picard-Vessiot extensions and differential Galois cohomology. *Ann. Fac. Sci. Toulouse Math. (6)*, 28(5):813–830, 2019.

[DVHW14] Lucia Di Vizio, Charlotte Hardouin, and Michael Wibmer. Difference Galois theory of linear differential equations. *Adv. Math.*, 260:1–58, 2014.

[DVHW17] Lucia Di Vizio, Charlotte Hardouin, and Michael Wibmer. Difference algebraic relations among solutions of linear differential equations. *J. Inst. Math. Jussieu*, 16(1):59–119, 2017.

[GHWY17] Xiao-Shan Gao, Zhang Huang, Jie Wang, and Chun-Ming Yuan. Toric difference variety. *J. Syst. Sci. Complex.*, 30(1):173–195, 2017.

[GHY17] Xiao-Shan Gao, Zhang Huang, and Chun-Ming Yuan. Binomial difference ideals. *J. Symbolic Comput.*, 80:665–706, 2017.

[Kol85] E. R. Kolchin. *Differential algebraic groups*, volume 114 of *Pure and Applied Mathematics*. Academic Press Inc., Orlando, FL, 1985.

[KP07] Piotr Kowalski and Anand Pillay. On algebraic σ-groups. *Trans. Amer. Math. Soc.*, 359(3):1325–1337 (electronic), 2007.

[Lev08] Alexander Levin. *Difference algebra*, volume 8 of *Algebra and Applications*. Springer, New York, 2008.

[LSMP24] Omar León Sánchez, David Meretzky, and Anand Pillay. More on Galois cohomology, definability, and differential algebraic groups. *J. Symb. Log.*, 89(2):496–515, 2024.

[Mil17] J. S. Milne. *Algebraic groups*, volume 170 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. The theory of group schemes of finite type over a field.

[MO19] Andrei Minchenko and Alexey Ovchinnikov. Triviality of differential Galois cohomology of linear differential algebraic groups. *Comm. Algebra*, 47(12):5094–5100, 2019.

[MP25] David Meretzky and Anand Pillay. Picard-Vessiot extensions, linear differential algebraic groups, and their torsors. *Comm. Algebra*, 53(1):148–161, 2025.

[Mum99] David Mumford. *The red book of varieties and schemes*, volume 1358 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, expanded edition, 1999. Includes the Michigan lectures (1974) on curves and their Jacobians, With contributions by Enrico Arbarello.

[Pil17] Anand Pillay. The Picard-Vessiot theory, constrained cohomology, and linear differential algebraic groups. *J. Math. Pures Appl. (9)*, 108(6):809–817, 2017.

[Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.

[SP21] Omar León Sánchez and Anand Pillay. Differential Galois cohomology and parameterized Picard-Vessiot extensions. *Commun. Contemp. Math.*, 23(8):Paper No. 2050081, 25, 2021.

[Tom] Ivan Tomašić. A topos-theoretic view of difference algebra. arXiv:2001.09075.

[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.

[Wan18] Jie Wang. Finite basis for radical well-mixed difference ideals generated by binomials. *Comm. Algebra*, 46(6):2589–2599, 2018.

[Wan20] Jie Wang. Toric P-difference varieties. *Sci. China Math.*, 63(4):643–670, 2020.

[Wat79] William C. Waterhouse. *Introduction to affine group schemes*, volume 66 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979.

[Wib12] Michael Wibmer. A Chevalley theorem for difference equations. *Math. Ann.*, 354(4):1369–1396, 2012.

[Wib21] Michael Wibmer. Almost-simple affine difference algebraic groups. *Math. Z.*, 299(1-2):473–526, 2021.

[Wib22] Michael Wibmer. Finiteness properties of affine difference algebraic groups. *Int. Math. Res. Not. IMRN*, (1):506–555, 2022.

[Wib24] Michael Wibmer. Étale difference algebraic groups. *Ann. Inst. Fourier (Grenoble)*, 74(4):1451–1519, 2024.

Michael Wibmer, School of Mathematics, University of Leeds, https://sites.google.com/view/wibmer
Email address: m.wibmer@leeds.ac.uk

Annette Bachmayr, Department of Mathematics, RWTH Aachen University
Email address: bachmayr@mathematik.rwth-aachen.de