EPIGA

Free Proalgebraic Groups

Michael Wibmer

Abstract. Replacing finite groups by linear algebraic groups, we study an algebraic-geometric counterpart of the theory of free profinite groups. In particular, we introduce free proalgebraic groups and characterize them in terms of embedding problems. The main motivation for this endeavor is a differential analog of a conjecture of Shafarevic.

[Français]

Groupes proalgébriques libres

Résumé. En remplaçant les groupes finis par les groupes algébriques linéaires, nous étudions une contrepartie algébro-géométrique de la théorie des groupes profinis libres. En particulier, nous introduisons les groupes proalgébriques libres et nous les caractérisons en termes de problèmes de plongements. Ce travail est principalement motivé par un analogue différentiel d'une conjecture de Shafarevic.

Michael Wibmer
Institute of Analysis and Number Theory, Graz University of Technology, Kopernikusgasse 24/II, 8010 Graz, Austria
e-mail: wibmer@math.tugraz.at

Contents

1. Introduction

Free profinite groups play an important role in the theory of profinite groups and in Galois theory. For example, the Shafarevic conjecture in inverse Galois theory states that the absolute Galois group of the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ is the free profinite group on a countably infinite set. (See e.g., [Har].) A solvable version of Shafarevic's conjecture was established by Iwasawa in [Iwa53] and a geometric version of Shafarevic's conjecture is known to be true:

Theorem 1.1 (Douady, Pop, Harbater). *Let k be an algebraically closed field. Then the absolute Galois group of $K = k(x)$, the field of rational functions over k, is the free profinite group on a set of cardinality $|K|$.*

This was first proved by Douady in characteristic zero ([Dou64]) and then later, independently by Pop ([Pop95]) and Harbater ([Har95]) in positive characteristic.

Differential Galois theory ([vdPS03], [Mag94]) is an extension of classical Galois theory: Instead of polynomials over a field, one considers linear differential equations over a differential field. The differential Galois group of a linear differential equation is a linear algebraic group. Accordingly, the absolute differential Galois group of a differential field is a projective limit of linear algebraic groups, i.e., an affine group scheme or a proalgebraic group.

A basic example of a differential field is the field $k(x)$ with the derivation $\frac{d}{dx}$. No explicit description of the absolute differential Galois group of $k(x)$ is presently known. However, around the turn of the century, Matzat promoted the idea that their should be a differential analog of Theorem 1.1, i.e., a differential version of Shafarevic's conjecture:

Conjecture (Matzat). *Let k be an algebraically closed field of characteristic zero. Then the absolute differential Galois group of $K = k(x)$ is the free proalgebraic group on a set of cardinality $|K|$.*

Matzat's conjecture implies Theorem 1.1 (in characteristic zero) and is a far-reaching generalization of the solution of the inverse problem of differential Galois theory over $k(x)$, which asserts that every linear algebraic group is a differential Galois group over $k(x)$ ([Har05]). For example, Matzat's conjecture implies that for a fixed non-trivial linear algebraic group G, the set of isomorphism classes of Picard-Vessiot extensions with differential Galois group isomorphic to G, has cardinality $|K|$, while the solution of the inverse problem merely asserts that this set is non-empty.

An embedding problem (sometimes also called a lifting problem in the literature) for a profinite group Γ consist of two epimorphisms $G \twoheadrightarrow H$ and $\Gamma \twoheadrightarrow H$ of profinite groups. A solution is an epimorphism $\Gamma \twoheadrightarrow G$ such that

(1)
$$
\begin{array}{ccc}
 & & \Gamma \\
 & \swarrow & \downarrow \\
G & \twoheadrightarrow & H
\end{array}
$$

commutes. The proof of Theorem 1.1 has two main steps:

(1) The Chatzidakis-Melnikov characterization of free profinite groups in terms of embedding problems ([RZ10, Prop. 3.5.11]): A profinite group Γ of infinite rank κ is free on a set of cardinality κ if and only if every non-trivial embedding problem (1) with G a finite group has κ different solutions.

(2) Establishing that the absolute Galois group of $k(x)$ satisfies the above characterization.

Over the last decade, progress towards Matzat's conjecture, along the lines of the above sketch, has been hampered by two aspects: Firstly, there has been no clear definition of what a free proalgebraic group should be, and accordingly, no characterization in terms of embedding problems has been available. Secondly, despite some positive results ([Kov69],[Kov71], [MvdP03],[Obe03],[Har05]), not enough has been known about the solvability of embedding problems for the absolute differential Galois group of $k(x)$.

In this article we introduce free proalgebraic groups and we characterize them in terms of embedding problems. In other words, we complete the first step of the two steps towards Matzat's conjecture. Paired with recent progress ([BHHW18],[BHHP],[BHH18]) on the solvability of differential embedding problems, this yields a special case of Matzat's conjecture that will appear in [BHHW].

Theorem 1.2 ([BHHW, Theorem 3.10]). *Matzat's conjecture is true if the field of constants k is countable and of infinite transcendence degree over $\mathbb{Q}$. In other words, Matzat's conjecture is true for the field $k = \overline{\mathbb{Q}(y_1, y_2, \ldots)}$, the algebraic closure of the field of rational functions in countably many variables over $\mathbb{Q}$.*

The restriction that k is countable enters the picture because over a countable field our characterization of free proalgebraic groups on a countably infinite set is particularly simple. (See Theorem 1.3 below.) However, we do provide a characterization (in fact several equivalent ones) of free proalgebraic groups over fields of arbitrary cardinality. In [BHHW] these equivalent characterizations of free proalgebraic groups in terms of embedding problems are translated to equivalent characterizations of differential fields with a free absolute differential Galois group in terms of differential embedding problems. We hope that this characterization and work in progress on differential embedding problems will lead to a proof of Matzat's conjecture for uncountable fields k, in particular, for the classical case $k = \mathbb{C}$.

In this article we introduce two classes of proalgebraic groups and we answer the question when these two notions coincide. Let us discuss the two classes individually:

Free proalgebraic groups

We introduce free proalgebraic groups through a universal mapping property: The free proalgebraic group on a set X over a field k is a proalgebraic group $\Gamma(X)$ over k together with a map $X \to \Gamma(X)(\bar{k})$ that is universal among all maps satisfying the following property: Every morphism from $\Gamma(X)$ to an algebraic group maps almost all elements of X to the identity. To establish the existence of free proalgebraic groups we use the tannakian machinery ([DM82], [Del90]).

As in the theory of profinite groups, where one considers, e.g., pro-solvable groups or pro-p-groups, it is often convenient or interesting to restrict attention to a certain class $\mathcal{C}$ of linear algebraic groups, for example the class of all reductive algebraic groups, or the class of all unipotent algebraic groups. As long as the class $\mathcal{C}$ satisfies certain closure properties there is a well-behaved notion of a pro-$\mathcal{C}$-group and indeed we introduce free proalgebraic groups in this context, i.e., we define free pro-$\mathcal{C}$-groups.

Our notion of free pro-$\mathcal{C}$-groups encompasses three previously known constructions. Firstly, if $\mathcal{C}$ is a class of finite constant algebraic groups corresponding to a class C of finite groups, then a free pro-$\mathcal{C}$-group can be identified with a profinite group, indeed with a free pro-C-group. In this spirit, most of our results contain familiar results about profinite groups as a special case.

Secondly, the free proalgebraic group on a finite set X is the proalgebraic completion of the (abstract) free group on X.

Thirdly, free prounipotent groups have already been introduced in [LM82], where they were studied in connection with the cohomology of unipotent groups and characterized as the prounipotent groups of cohomological dimension one. Their internal structure has further been investigated in [LM83]. Moreover, in [Mag01], a unipotent version of Matzat's conjecture over $\mathbb{C}$ has been proved: The differential Galois group of the maximal prounipotent Picard-Vessiot extension of $\mathbb{C}(x)$, is a free prounipotent group.

We note that free profinite groups play a distinguished role in the theory of profinite groups ([RZ10], [FJ08]) and that there are several results about free profinite groups that we do not touch upon in this paper that suggest themselves for a generalization to free proalgebraic groups.

Saturated proalgebraic groups

Roughly speaking, saturated proalgebraic groups behave like universal objects in the category of proalgebraic groups. Our defintion of saturated proalgebraic groups gives a precise meaning to the vague idea of forming the projective limit of all linear algebraic groups, or of forming the projective limit of all linear algebraic groups belonging to a certain class $\mathcal{C}$.

Every proalgebraic group Γ can canonically be written as a projective limit of linear algebraic groups. Indeed, $\Gamma = \varprojlim_N \Gamma/N$, where N ranges over all normal closed subgroups of Γ such that Γ/N is algebraic. There is no difficulty in constructing a proalgebraic group Γ such that, up to isomorphism, all linear algebraic groups occur as quotients of Γ. More generally, one may construct a proalgebraic group Γ such that, up to isomorphism, all epimorphisms of linear algebraic groups occur in the canonical projective system for Γ. This property does not determine Γ up to isomorphism. So one may make the stronger requirement, that for every algebraic quotient H of Γ every epimorphism $G \twoheadrightarrow H$ of linear algebraic groups occurs, up to isomorphism, in the canonical projective system for Γ, i.e., we ask that the embedding problem

$$\begin{array}{ccc} & & \Gamma \\ & \swarrow & \downarrow \\ G & \twoheadrightarrow & H \end{array}$$

for Γ has a solution. Even this property does not determine Γ up to isomorphism. However, it turns out that, if k is countable and we require that Γ has countable rank, i.e., Γ is the projective limit of linear algebraic groups, where the projective limit is taken over a countable set, then there exists, up to isomorphism, a

unique such Γ. Moreover, if k has characteristic zero, Γ is isomorphic to the free proalgebraic group on a countably infinite set. To summarize, we have:

Theorem 1.3 (Corollary 3.43). *Let k be a countable field of characteristic zero and Γ a proalgebraic group over k of countable rank. Then Γ is a free proalgebraic group on a countably infinite set if and only if for every epimorphism $G \twoheadrightarrow H$ of linear algebraic groups and every epimorphism $\Gamma \twoheadrightarrow H$ the embedding problem*

$$\begin{array}{ccc} & & \Gamma \\ & \swarrow & \downarrow \\ G & \longrightarrow\!\!\!\!\rightarrow & H \end{array}$$

has a solution.

Theorem 1.3 can be seen as an algebraic-geometric version of Iwasawa's freeness theorem ([Iwa53, Theorem 4], [RZ10, Cor. 3..5.10]) which states that a profinite group of countably infinite rank is free on a countably infinite set if and only if every embedding problem

$$\begin{array}{ccc} & & \Gamma \\ & \swarrow & \downarrow \\ G & \longrightarrow\!\!\!\!\rightarrow & H \end{array}$$

where G is a finite group, is solvable. In fact, we establish a relative version or $\mathcal{C}$-version of Theorem 1.3 so that indeed Iwasawa's result is a special case of ours. Theorem 1.3 is exactly the group theoretic input needed for the proof of the special case of Matzat's conjecture (Theorem 1.2).

However, we do provide a version of Theorem 1.3 that applies for base fields of arbitrary cardinality, that we will discuss now. The rank of a proalgebraic group G can be defined as the smallest cardinal κ such that G is the projective limit of linear algebraic groups, taken over a directed set of cardinality κ. A pro-$\mathcal{C}$-group Γ is saturated if for all epimorphisms $G \twoheadrightarrow H$, $\Gamma \twoheadrightarrow H$ of pro-$\mathcal{C}$-groups with $\operatorname{rank}(H) < \operatorname{rank}(\Gamma)$ and $\operatorname{rank}(G) \leq \operatorname{rank}(\Gamma)$ the embedding problem

$$\begin{array}{ccc} & & \Gamma \\ & \swarrow & \downarrow \\ G & \longrightarrow\!\!\!\!\rightarrow & H \end{array}$$

has a solution. Morally, a proalgebraic group is saturated if it solves as many embedding problems as possible. In Theorem 3.24 we provide several equivalent characterizations of this idea. The general version of Theorem 1.3 states the following:

Theorem 1.4 (Theorem 3.42). *Let k be a field of characteristic zero and let Γ be a pro-$\mathcal{C}$-group whose rank is such that $\operatorname{rank}(\Gamma) = \kappa \geq |k|$. Then Γ is the free pro-$\mathcal{C}$-group on a set of cardinality κ if and only if Γ is saturated.*

We show by example that the assumption $\operatorname{rank}(\Gamma) \geq |k|$ in Theorem 1.4 is necessary.

We conclude this introduction with a brief outline of the article: After introducing some basic terminology and constructions, the existence of free pro-$\mathcal{C}$-groups is established in Section 2 using the tannakian machinery. We also compute some examples of free pro-$\mathcal{C}$-groups. In Section 3 saturated pro-$\mathcal{C}$-groups are introduced and several equivalent characterizations of saturated pro-$\mathcal{C}$-groups are established. We then discuss the questions of existence and uniqueness of saturated pro-$\mathcal{C}$-groups: Saturated pro-$\mathcal{C}$-groups of a fixed rank are unique up to isomorphism. However, their existence can only be guaranteed for a rank at least the cardinality of the base field. We also show that, over a field of characteristic zero, a free pro-$\mathcal{C}$-group Γ on a set of cardinality κ is saturated if $\operatorname{rank}(\Gamma) = \kappa$. Paired with the uniqueness of saturated pro-$\mathcal{C}$-groups, this yields Theorem 1.4.

2. Free pro-$\mathcal{C}$-groups

The main goal of this section is to establish the existence of free pro-$\mathcal{C}$-groups (Definition 2.18). We first need to introduce some terminology.

2.1. Preliminaries and notation

All rings are assumed to be commutative and unital. We work over a fixed base field k throughout. The algebraic closure of k is denoted by $\overline{k}$. We assume some familiarity with the theory of linear algebraic groups and affine group schemes. We recall some basic results and notions that will be used throughout the text below. (See e.g., [Mil17], [DG70] or [Wat79].)

To avoid endless repetitions of the word affine we use the term *algebraic group* to mean affine group scheme of finite type over k. In particular, over a field of positive characteristic, an algebraic group need not be reduced. A *proalgebraic group* is, by definition, an affine group scheme over k. This terminology emphasizes the approach of this paper and is justified by the fact that the proalgebraic groups are precisely the projective limits of algebraic groups. Projective limits are always assumed to be taken over a directed partially ordered set. Projective limits exist in the category of proalgebraic groups and they can indeed be taken pointwise, i.e., $(\varprojlim G_i)(R) = \varprojlim G_i(R)$ for any k-algebra R.

A *closed subgroup* of a proalgebraic group is a closed subgroup scheme. Let G be a proalgebraic group. A closed normal subgroup N of G is called *coalgebraic* if the quotient G/N is algebraic, i.e., of finite type. The isomorphism theorems from the theory of (abstract) groups hold verbatim for proalgebraic groups.

If X is an affine scheme, we write X_{red} for the underlying reduced scheme. Similarly, if R is a ring, we write R_{red} for the quotient of R by its nilradical.

If X is an affine scheme over k, we write $k[X]$ for the k-algebra of global sections of X, so $X = \mathrm{Spec}(k[X])$. If $\phi\colon X \to Y$ is a morphism of affine schemes over k, we denote the scheme-theoretic image of ϕ by $\phi(X)$, i.e., $\phi(X)$ is the smallest closed subscheme of Y such that ϕ factors through the inclusion $\phi(X) \hookrightarrow Y$. In terms of ideals, the defining ideal of $\phi(X)$ is simply the kernel of the dual map $\phi^*\colon k[Y] \to k[X]$. If $\phi\colon G \to H$ is a morphism of proalgebraic groups, then $\phi(G)$ is a closed subgroup of H. For a morphism $\phi\colon G \to H$ of proalgebraic groups the following conditions are equivalent:

- $\phi(G) = H$.
- The dual map $\phi^*\colon k[H] \to k[G]$ is injective.
- There exists a normal closed subgroup N of G such that $H \simeq G/N$ and ϕ identifies with the canonical map $G \to G/N$.
- For every k-algebra R and $h \in H(R)$, there exists a faithfully flat R-algebra S and an element $g \in G(S)$ such that g maps to $h \in H(R) \subseteq G(S)$ under ϕ.

If these conditions are satisfied we call ϕ an *epimorphism* and indicate this by writing $G \twoheadrightarrow H$. If $G \twoheadrightarrow H$ is an epimorphism of algebraic groups, then $G(\overline{k}) \to H(\overline{k})$ is a surjective map. (The converse is true if H is smooth.)

We will often treat a proalgebraic group G as a functor from the category of k-algebras to the category of groups. For a k-algebra R we then often identify $G(R)$ with $\mathrm{Hom}(k[G], R)$, the set of k-algebra homomorphisms from $k[G]$ to R. For a morphism $\phi\colon G \to H$ of proalgebraic groups we denote with $\phi_R\colon G(R) \to H(R)$ the corresponding homomorphism of groups. If confusion is unlikely, we may write $\phi(g)$ instead of $\phi_R(g)$ for $g \in G(R)$.

To define the structure of a proalgebraic group on an affine scheme G over k is equivalent to defining the structure of a Hopf algebra on $k[G]$. The normal closed subgroups of G are in one-to-one correspondence with the Hopf subalgebras of $k[G]$. In more detail, a normal closed subgroup N of G corresponds to the image of $k[G/N] \to k[G]$, the morphism of Hopf algebras, dual to the canonical map $G \to G/N$. We will usually identify $k[G/N]$ with this Hopf subalgebra of $k[G]$. For normal closed subgroups N_1, N_2 of G, we have $k[G/N_1] \cap k[G/N_2] = k[G/N_1 N_2]$ and $k[G/N_1] \cdot k[G/N_2] = k[G/(N_1 \cap N_2)]$.

An algebraic group G is *finite* if $k[G]$ is a finite dimensional vector space over k. The identity component of an algebraic group G is denoted by G^o. This notion extends to proalgebraic groups: If $G = \varprojlim_{i \in I} G_i$ is the projective limit of algebraic groups G_i, then $G^o = \varprojlim_{i \in I} G_i^o$.

For an abelian group M, we denote by $D(M)$ the functor from the category of k-algebras to the category of groups given by

$$D(M)(R) = \operatorname{Hom}(M, R^\times)$$

for any k-algebra R. Here $\operatorname{Hom}(M, R^\times)$ denotes the set of homomorphism of abelian groups from M to $R^\times$. Then $D(M)$ is representable, i.e., a proalgebraic group. Indeed, $D(M)$ is represented by $k[D(M)] = kM$, the group algebra of M over k. A proalgebraic group isomorphic to some $D(M)$ is called *diagonalizable*. The (contravariant) functor $M \rightsquigarrow D(M)$ is exact and fully faithful.

Any finite group G can naturally be interpreted as an algebraic group over k. This algebraic group is often called the *constant* group scheme associated with G, we denote it by G_k. The functor $\mathsf{G} \rightsquigarrow \mathsf{G}_k$ from the category of finite groups to the category of algebaic groups is fully faithful and extends to a fully faithful functor from the category of profinite groups to the category of proalgebraic groups: If $\mathsf{G} = \varprojlim_{i \in I} \mathsf{G}_i$ is a projective limit of finite groups G_i, then $\mathsf{G}_k = \varprojlim_{i \in I} (\mathsf{G}_i)_k$ is a projective limit of finite constant group schemes. The group $\mathsf{G}_k(k)$ can be identified with G itself. All prime ideals of $\operatorname{Spec}(k[\mathsf{G}_k])$ are maximal (and minimal) and the kernel of some morphism $k[\mathsf{G}_k] \to k$ of k-algebras. Thus $\operatorname{Spec}(k[\mathsf{G}_k])$ can also be identified with G. Moreover, the topologies on $\operatorname{Spec}(k[\mathsf{G}_k])$ and G agree. There is a one-to-one correspondence between the closed subgroups of G and the closed subgroups of G_k. Under this correspondence, the normal open (=closed and of finite index) subgroups of G correspond to the coalgebraic subgroups of G_k.

2.2. Formations of algebraic groups

To have a well-behaved notion of pro-$\mathcal{C}$-groups, the class $\mathcal{C}$ of algebraic groups needs to satisfy certain closure properties that we will now discuss.

We always assume that $\mathcal{C}$ is a non-empty class of algebraic groups over k such that any algebraic group isomorphic to an algebraic group in $\mathcal{C}$ also belongs to $\mathcal{C}$. A group that belongs to $\mathcal{C}$ will also be called a $\mathcal{C}$-group. We call $\mathcal{C}$ a *formation* if it satisfies the following two conditions.

(i) $\mathcal{C}$ is closed under taking quotients, i.e., if $G \twoheadrightarrow H$ is an epimorphism of algebraic groups and $G \in \mathcal{C}$, then $H \in \mathcal{C}$.

(ii) $\mathcal{C}$ is closed under subdirect products, i.e., if H is a subdirect product of $G_1, G_2 \in \mathcal{C}$, then $H \in \mathcal{C}$. (Recall that a closed subgroup H of $G_1 \times G_2$ is a subdirect product of G_1 and G_2 if the projections $H \to G_i$ are epimorphisms for $i = 1, 2$.)

Remark 2.1. Condition (ii) above has two equivalent reformulations:

(ii)' If G is a proalgebraic group and $N_1, N_2 \trianglelefteq G$ are normal closed subgroups such that G/N_1 and G/N_2 are in $\mathcal{C}$, then also $G/(N_1 \cap N_2)$ is in $\mathcal{C}$.

(ii)'' If G is an algebraic group and $N_1, N_2 \trianglelefteq G$ are normal closed subgroups such that $N_1 \cap N_2 = 1$ and $G/N_1, G/N_2 \in \mathcal{C}$, then $G \in \mathcal{C}$.

To avoid trivialities we also assume that a formation contains a non-trivial algebraic group.

If C is a formation of (abstract) finite groups ([RZ10, p. 20]), i.e., C is closed under taking quotients and subdirect products, we let $\mathcal{C} = \mathsf{C}_k$ denote the class of all algebraic groups isomorphic to G_k for some G in C. Then $\mathcal{C}$ is a formation of algebraic groups.

As illustrated by the following example, most of the familiar classes of algebraic groups are formations.

Example 2.2. Note that if $\mathcal{C}$ is closed under taking quotients, direct products and closed subgroups, then $\mathcal{C}$ is a formation. Therefore the following classes are formations:

   (i) The class of all algebraic groups,

  (ii) the class of all abelian algebraic groups,

 (iii) the class of all nilpotent algebraic groups,

 (iv) the class of all solvable algebraic groups,

  (v) the class of all unipotent algebraic groups,

 (vi) the class of all étale algebraic groups,

(vii) the class of all diagonalizable algebraic groups,

(viii) the class of all infinitesimal algebraic groups.

   Moreover, over a field of charcteristic zero,

(viii) the class of all semisimple algebraic groups and

 (ix) the class of all reductive linear algebraic groups

are formations. To be precise, here semisimple and reductive groups are required to be smooth but not necessarily connected. Quotients of semisimple (respectively reductive) algebraic groups are semisimple (respectively reductive). See e.g., [Mil17, Lemma 19.14]. Let us show that in characteristic zero the class of semisimple linear algebraic groups is closed under subdirect products. (The argument for reductive algebraic groups is similar.) Let G be an algebraic group and $N_1, N_2 \trianglelefteq G$ closed normal subgroups with $N_1 \cap N_2 = 1$ and $G/N_1, G/N_2$ semi-simple. Let $R(G_{\overline{k}})$ denote the radical of $G_{\overline{k}}$. Since $R(G_{\overline{k}})$ maps into $R((G/N_1)_{\overline{k}}) = 1$, we see that $R(G_{\overline{k}})$ is contained in $(N_1)_{\overline{k}}$. Similarly, $R(G_{\overline{k}}) \subseteq (N_2)_{\overline{k}}$. Thus $R(G_{\overline{k}}) = 1$. Since G is automatically smooth in characteristic zero, it follows that G is semisimple.

The following example shows that over a field of positive characteristic p, the classes of all smooth algebraic groups, all semisimple algebraic groups and all reductive algebraic groups are not formations: The subdirect product $H = \{(g_1, g_2) \in \mathrm{SL}_2 \times \mathrm{SL}_2 \mid \mathrm{Fr}_p(g_1) = \mathrm{Fr}_p(g_2)\}$ of $G_1 = \mathrm{SL}_2$ and $G_2 = \mathrm{SL}_2$ is not smooth. Here, for any 2×2 matrix

$$\mathrm{Fr}_p\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} a^p & b^p \\ c^p & d^p \end{bmatrix}$$

The class of connected algebraic groups is also not a formation as shown by the following: the subdirect product $\{(g_1, g_2) \in \mathbb{G}_m^2 \mid g_1^2 = g_2^4\}$ of $G_1 = G_2 = \mathbb{G}_m$ is not connected.

Let $\mathcal{C}$ be a class of algebraic groups. A proalgebraic group G is called a *pro-$\mathcal{C}$-group* if $G = \varprojlim G_i$ is a projective limit of $\mathcal{C}$-groups G_i, where the transition maps $G_j \to G_i$ ($j \geq i$) are epimorphisms. The following lemma shows that, when $\mathcal{C}$ is a formation, every pro-$\mathcal{C}$-group can canonically be written as a projective limit of $\mathcal{C}$-groups.

Lemma 2.3. *Let $\mathcal{C}$ be a formation of algebraic groups and G a pro-$\mathcal{C}$-group. Then*

   (i) *every algebraic quotient of G belongs to $\mathcal{C}$,*

  (ii) *the canonical map $G \to \varprojlim G/N$ is an isomorphism, where the projective limit is taken over all coalgebraic subgroups N of G and*

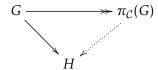 (iii) *every quotient of a pro-$\mathcal{C}$-group is a pro-$\mathcal{C}$-group.*

Proof. Let $G = \varprojlim G_i$ be a projective limit of $\mathcal{C}$-groups G_i, with surjective transition maps $G_j \to G_i$. Then $k[G]$ is the directed union of the $k[G_i]$'s. Let H be an algebraic quotient of G. Since $k[H] \subseteq k[G]$ is finitely generated, $k[H]$ is contained in some $k[G_i]$ and therefore H is a quotient of G_i. As $\mathcal{C}$ is closed under taking quotients, H is a $\mathcal{C}$-group.

Let us prove (ii): The coalgebraic subgroups of G form a directed set under $N \leq N'$ if $N \supseteq N'$ and the transition maps $G/N' \to G/N$ yield a projective system. Since $k[G]$ is the directed union of its finitely generated Hopf subalgebras ([Wat79, Section 3.3]), we see that $G = \varprojlim G/N$.

For a quotient H of G we have $k[H] \subseteq k[G]$. The proalgebraic group H is the projective limit of its algebraic quotients H_i and $k[H_i] \subseteq k[H] \subseteq k[G]$. By (i) the H_i's are $\mathcal{C}$-groups and thus H is a pro-$\mathcal{C}$-group. $\qquad\square$

The following lemma will be useful for constructing free pro-$\mathcal{C}$-groups.

Lemma 2.4. *Let G be a proalgebraic group and $\mathcal{C}$ a formation of algebraic groups. Then G has a maximal pro-$\mathcal{C}$-quotient, i.e., there exists a pro-$\mathcal{C}$-group $\pi_{\mathcal{C}}(G)$ together with an epimorphism $G \twoheadrightarrow \pi_{\mathcal{C}}(G)$ such that for any morphism $\phi\colon G \to H$ of proalgebraic groups with $\phi(G)$ a pro-$\mathcal{C}$-group, there exists a unique morphism $\pi_{\mathcal{C}}(G) \to H$ such that*

$$
\begin{array}{ccc}
G & \longrightarrow & \pi_{\mathcal{C}}(G) \\
& \searrow & \vdots \\
& & H
\end{array}
$$

commutes.

Proof. Let I denote the set of all normal closed subgroups N of G such that $G/N \in \mathcal{C}$. We define a partial order on I by $N_1 \leq N_2$ if $N_1 \supseteq N_2$. Because $\mathcal{C}$ is closed under subdirect products (Remark 2.1) we know that $N_1 \cap N_2 \in \mathcal{C}$ if $N_1, N_2 \in \mathcal{C}$. Thus I is directed. For $N_1 \leq N_2$ we have a canonical epimorphism $G/N_2 \twoheadrightarrow G/N_1$ and the collection of all these maps is a projective system. Let $\pi_{\mathcal{C}}(G)$ denote the corresponding projective limit. Then $\pi_{\mathcal{C}}(G)$ is a pro-$\mathcal{C}$-group and $k[\pi_{\mathcal{C}}(G)] \subseteq k[G]$ is the union of all finitely generated Hopf subalgebras $k[G_i]$ of G such that G_i is a $\mathcal{C}$-group.

If $\phi\colon G \to H$ is a morphism with $\phi(G)$ a pro-$\mathcal{C}$-group, then $k[\phi(G)] \subseteq k[G]$ and since $k[\phi(G)]$ is a union of $k[H_i]$'s with $H_i \in \mathcal{C}$, we see that $k[\phi(G)] \subseteq k[\pi_{\mathcal{C}}(G)]$. So ϕ factors uniquely through $G \twoheadrightarrow \pi_{\mathcal{C}}(G)$. $\qquad\square$

Example 2.5. If G is an algebraic group and $\mathcal{C}$ the class of all étale algebraic groups, then $\pi_{\mathcal{C}}(G)$ agrees with $\pi_0(G) = G/G^o$, the group of connected components of G ([Mil17, Def. 2.38]).

2.3. Coalgebraic subgroups and convergence to one

Let $G = \varprojlim G/N$ be a proalgebraic group, written as the projective limit of the canonical projective system. Then also $G(\overline{k}) = \varprojlim (G/N)(\overline{k})$ and it is possible to topologize $G(\overline{k})$ with the limit topology, where the $(G/N)(\overline{k})$ are considered with the discrete topology (rather than the Zariski topology). Then $\{N(\overline{k})|\ N \leq G \text{ is coalgebraic}\}$ is a neighborhood basis at 1 for $G(\overline{k})$. We have no need to actually use this topology on $G(\overline{k})$, but we will introduce some topological language which is reminiscent of this idea.

Definition 2.6. *Let G be a proalgebraic group. A set $\mathcal{N}$ of coalgebraic subgroups of G is a neighborhood basis at 1 for G, if for every coalgebraic subgroup N of G, there exists $N' \in \mathcal{N}$ with $N' \leq N$.*

Thus a set $\mathcal{N}$ of coalgebraic subgroups of G is a neighborhood basis at 1 for G if and only if

(i) $\mathcal{N}$ is downward directed, i.e., for $N_1, N_2 \in \mathcal{N}$ there exists $N_3 \in \mathcal{N}$ with $N_3 \leq N_1, N_2$.

(ii) $\bigcap_{N \in \mathcal{N}} N = 1$.

From a neighborhood basis $\mathcal{N}$ at 1 for G we obtain a projective system $G/N \twoheadrightarrow G/N'$ ($N, N' \in \mathcal{N}$ and $N \leq N'$) with $G = \varprojlim_{N \in \mathcal{N}} G/N$. Conversely, if $G = \varprojlim_{i \in I} G_i$ is a projective limit of algebraic groups, then the set of all kernels of the morphisms $G \to G_i$ is a neighborhood basis at 1 for G.

Lemma 2.7. *Let G be a proalgebraic group, $H \leq G$ a closed subgroup and $N \leq H$ a coalgebraic subgroup of H. Then there exists a coalgebraic subgroup N' of G such that $H \cap N' \leq N$.*

Proof. Since $k[G]$ is the directed union of its finitely generated Hopf subalgebras and $k[H/N] \subseteq k[H]$ is finitely generated, it follows that there exists a finitely generated Hopf subalgebra of $k[G]$ whose image in $k[H]$ contains $k[H/N]$. This Hopf subalgebra is necessarily of the form $k[G/N']$ for some coalgebraic subgroup N' of G. The image of $k[G/N']$ in $k[H]$ is $k[H/H \cap N']$. Since $k[H/N] \subseteq k[H/H \cap N']$, it follows that $H \cap N' \subseteq N$. $\qquad\square$

From Lemma 2.7 we immediately obtain:

Corollary 2.8. *Let G be a proalgebraic group and $H \leq G$ a closed subgroup. If $\mathcal{N}$ is a neighborhood basis at 1 for G, then $\mathcal{N}(H) = \{N \cap H \mid N \in \mathcal{N}\}$ is a neighborhood basis at 1 for H.*

Corollary 2.9. *Let G be a proalgebraic group and $H \leq G$ a closed subgroup that is algebraic. Then there exists a coalgebraic subgroup N' of G with $N' \cap H = 1$.*

Proof. As H is algebraic we can chose $N = 1$ in Lemma 2.7. $\qquad\square$

Corollary 2.10. *Let $\mathcal{C}$ be a formation of algebraic groups and G a pro-$\mathcal{C}$-group. If $\mathcal{C}$ is closed under taking closed subgroups, then every closed subgroup of G is a pro-$\mathcal{C}$-group.*

Proof. Let H be a closed subgroup of G and let $\mathcal{N}$ be a neighborhood basis at 1 for G. According to Corollary 2.8 the set $\{H \cap N \mid N \in \mathcal{N}\}$ is a neighborhood basis at 1 for H. Thus $H \simeq \varprojlim H/(H \cap N)$. But $H/(H \cap N)$ injects into G/N and is therefore a $\mathcal{C}$-group. $\qquad\square$

The free proalgebraic groups that we want to consider are free on a set X such that the map from X to the proalgebraic group has a certain property which is explained in the following definition.

Definition 2.11. *Let X be a set, G a proalgebraic group and R a k-algebra. A map $\varphi \colon X \to G(R)$ converges to 1 if for every coalgebraic subgroup N of G almost all elements of X map into $N(R)$, i.e., $X \smallsetminus \varphi^{-1}(N(R))$ is finite for every coalgebraic subgroup N of G.*

For $X \subseteq G(R)$, we say that X *converges to* 1 if the inclusion map converges to 1. If G is algebraic, it follows that φ converges to 1 if and only if almost all elements of X map to 1.

Lemma 2.12. *Let $\phi \colon G \to H$ be a morphism of proalgebraic groups, X a set, R a k-algebra and $\varphi \colon X \to G(R)$ a map converging to 1. Then $\phi_R \circ \varphi \colon X \to H(R)$ converges to 1.*

Proof. If N is a coalgebraic subgroup of H, then $\phi^{-1}(N)$ is a coalgebraic subgroup of G. $\qquad\square$

Lemma 2.13. *Let X be a set, G a proalgebraic group, $H \leq G$ a closed subgroup and R a k-algebra. If the map $\varphi \colon X \to G(R)$ converges to 1 and $\varphi(X) \subseteq H(R)$, then $\varphi \colon X \to H(R)$ converges to 1.*

Proof. Let N be a coalgebraic subgroup of H. By Lemma 2.7 there exists a coalgebraic subgroup N' of G with $H \cap N' \leq N$. The kernel of $H(R) \to (G/N')(R)$ is $(H \cap N')(R)$ and almost all elements of X map to 1 in $(G/N')(R)$. Therefore almost all elements of X map into $(H \cap N')(R) \subseteq N(R)$. $\qquad\square$

2.4. Generating proalgebraic groups

Let G be a proalgebraic group, R a k-algebra and $X \subseteq G(R)$. As the intersection of closed subgroups H of G with $X \subseteq H(R)$ also has this property, there exists a smallest closed subgroup $\langle X \rangle$ of G such that $X \subseteq \langle X \rangle(R)$. We call it the *closed subgroup generated by* X. If $\langle X \rangle = G$, we also say that X *generates* G or that X is a generating set of G.

Lemma 2.14. *Let G be a proalgebraic group, R a k-algebra and $X \subseteq G(R)$. If k is perfect and R reduced, then $\langle X \rangle$ is reduced (and therefore geometrically reduced).*

Proof. Since k is perfect, the underlying reduced subscheme G_{red} of a proalgebraic group G is a closed subgroup of G. (See [Mil17, Cor. 1.39] for the algebraic case or [Gro70, Exposé $\mathrm{VI_A}$, Section 0.2] for the general case.) So $\langle X \rangle_{\mathrm{red}}$ is a closed subgroup of G. It therefore suffices to show that $X \subseteq \langle X \rangle_{\mathrm{red}}(R)$.

If H is a closed subgroup of G, an $x \in X \subseteq G(R) = \mathrm{Hom}(k[G], R)$ lies in $H(R)$ if and only if the defining ideal $\mathbb{I}(H) \subseteq k[G]$ is contained in $\ker(x)$. By definition $X \subseteq \langle X \rangle(R)$, so $\mathbb{I}(\langle X \rangle) \subseteq \ker(x)$ for all $x \in X$. Because R is reduced, $\ker(x)$ is a radical ideal and therefore $\mathbb{I}(\langle X \rangle_{\mathrm{red}}) = \sqrt{\mathbb{I}(\langle X \rangle)} \subseteq \ker(x)$ for all $x \in X$. Thus $X \subseteq \langle X \rangle_{\mathrm{red}}(R)$. $\qquad\square$

If R is not reduced, $\langle X \rangle$ need not be reduced, even when k is perfect. For example, if k is a field of characteristic 2, $G = \mathbb{G}_a$, $R = k[\epsilon] = k[t]/(t^2)$ and $X = \{\epsilon\}$, then $\langle X \rangle = \alpha_2 = \{g \in \mathbb{G}_a | \, g^2 = 0\}$. The following example shows that $\langle X \rangle$ need not be reduced if k is not perfect, even when $R = \bar{k}$.

Example 2.15. Let k be a field of characteristic 2 and $a \in k$ such that $a^{\frac{1}{2}} \in \bar{k} \smallsetminus k$. Let $G = \mathbb{G}_a$ and $X = \{0, a^{\frac{1}{2}}\} \leq G(\bar{k})$. We will show that $\langle X \rangle = H = \{g \in \mathbb{G}_a | \, g^2(g^2 - a) = 0\}$. Clearly H is a closed subgroup of G with $X \subseteq H(\bar{k})$. There are only four subschemes of H, their defining equations are

- $x = 0$,
- $x^2 = 0$,
- $x^2 - a = 0$ or
- $x(x^2 - a) = 0$.

These are either not subgroups or do not contain X. Thus $\langle X \rangle = H$.

Lemma 2.16. *Let $\phi \colon G \to H$ be a morphism of proalgebraic groups, R a k-algebra and $X \subseteq G(R)$. Then $\phi(\langle X \rangle) = \langle \phi_R(X) \rangle$. In particular, if $\langle X \rangle = G$ and ϕ is an epimorphism, then $\langle \phi_R(X) \rangle = H$.*

Proof. As $\phi_R(X) \subseteq \phi(\langle X \rangle)(R)$, clearly, $\langle \phi_R(X) \rangle \subseteq \phi(\langle X \rangle)$. On the other hand, $\phi^{-1}(\langle \phi_R(X) \rangle)$ is a closed subgroup of G whose R-points contain X. Thus $\langle X \rangle \subseteq \phi^{-1}(\langle \phi_R(X) \rangle)$ and therefore $\phi(\langle X \rangle) \subseteq \langle \phi_R(X) \rangle$. $\quad\square$

2.5. Existence of free pro-$\mathcal{C}$-groups

We are now prepared to introduce free proalgebraic groups.

Theorem 2.17. *Let X be a set, $\mathcal{C}$ a formation and R a k-algebra. There exists a pro-$\mathcal{C}$-group $\Gamma = \Gamma^{\mathcal{C}}_{R/k}(X)$ and a map $\iota \colon X \to \Gamma(R)$ such that*
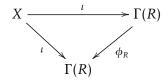
(i) *ι converges to 1 and $\langle \iota(X) \rangle$ is a pro-$\mathcal{C}$-group,*

(ii) *the pair (Γ, ι) is universal, i.e., for every pro-$\mathcal{C}$-group G and every map $\varphi \colon X \to G(R)$ converging to 1 with $\langle \varphi(X) \rangle$ a pro-$\mathcal{C}$-group, there exists a unique morphism $\psi \colon \Gamma \to G$ of proalgebraic groups such that*

(2)
$$
\begin{array}{ccc}
X & \xrightarrow{\quad \iota \quad} & \Gamma(R) \\
& \searrow_{\varphi} \quad \swarrow_{\psi_R} & \\
& G(R) &
\end{array}
$$

commutes.

Moreover, we have $\langle \iota(X) \rangle = \Gamma$.

Proof. We first show that $\langle \iota(X) \rangle = \Gamma$ for any pair (Γ, ι) satisfying (i) and (ii). Let $G = \langle \iota(X) \rangle \leq \Gamma$ and let $\varphi \colon X \to G(R)$ be such that $\varphi(x) = \iota(x)$ for all $x \in X$. Since φ converges to 1 by Lemma 2.13, it follows from (ii) that there exists a morphism $\psi \colon \Gamma \to G$ such that (2) commutes. Then $\phi \colon \Gamma \xrightarrow{\psi} G \to \Gamma$ is such that

$$\begin{array}{ccc} X & \xrightarrow{\ \ \iota\ \ } & \Gamma(R) \\ & {\iota}\searrow & \downarrow{\phi_R} \\ & & \Gamma(R) \end{array}$$

commutes. As also $\mathrm{id} \colon \Gamma \to \Gamma$ has this property, it follows from the uniqueness in (ii) that $\phi = \mathrm{id}$. Therefore $G = \Gamma$ as desired.

We will next construct $\Gamma^{\mathcal{C}}_{R/k}(X)$ for the formation $\mathcal{C}$ of all algebraic groups. Let F_X be the free (abstract) group on X. A *cofinite representation* of F_X (over R) is a pair (V, ϕ), where V is a finite dimensional k-vector space and $\phi \colon F_X \to \mathrm{GL}(V \otimes_k R) = \mathrm{GL}(V)(R)$ is a morphism of groups such that almost all $x \in X$ map to the identity of $\mathrm{GL}(V)(R)$. We may write V instead of (V, ϕ) and $g(a)$ instead of $\phi(g)(a)$ for $g \in F_X$ and $a \in V \otimes_k R$.

A morphism $(V, \phi) \to (V', \phi')$ of cofinite representations is a k-linear map $\eta \colon V \to V'$ such that we have $(\eta \otimes R)(\phi(g)(a)) = \phi'(g)((\eta \otimes R)(a))$ for every $g \in F_X$ and $a \in V \otimes_k R$. Clearly the cofinite representations of F_X are a category. We will show that they indeed are a neutral Tannakian category ([DM82, Del90]) in a natural way.

For two cofinite representations (V, ϕ) and (V', ϕ'), the tensor product $V \otimes_k V'$ becomes a cofinite representation by

$$g(a \otimes b) = g(a) \otimes g(b)$$

for $g \in F_X$ and $a \otimes b \in (V \otimes_k R) \otimes_R (V' \otimes_k R) = (V \otimes_k V') \otimes_k R$. For three cofinite representations V, V', V'', the map $(V \otimes_k V') \otimes_k V'' \to V \otimes_k (V' \otimes_k V'')$ is a morphism of cofinite representations. Therefore the usual associativity constraint on k-vector spaces induces an associativity constraint on the category of cofinite representations. Similarly, we obtain a compatible commutativity constraint. Thus the cofinite representations are a symmetric monoidal category. The identity object $\mathbb{1}$ is given by the one-dimensional k-vector space k, with $\phi \colon F_X \to \mathrm{GL}(k \otimes_k R) = \mathrm{GL}_1(R)$ the trivial map.

For a cofinite representation (V, ϕ) the dual vector space $V^\vee = \mathrm{Hom}_k(V, k)$ is a cofinite representation via $g(f)(a) = f(g^{-1}(a))$ for $g \in F_X$, $f \in V^\vee \otimes_k R = \mathrm{Hom}_R(V \otimes_k R, R)$ and $a \in V \otimes_k R$. The maps $V \otimes_k V^\vee \to \mathbb{1}$ and $\mathbb{1} \to V^\vee \otimes_k V$ are morphisms of cofinite representations. Therefore our category is rigid. (Cf. [Del90, 2.1.2].)

If $\eta \colon V \to V'$ is a morphism of cofinite representations, the kernel $\mathrm{ker}(\eta)$ is naturally a cofinite representation because $\mathrm{ker}(\eta) \otimes_k R = \mathrm{ker}(\eta \otimes R)$. If V is a cofinite representation and $W \leq V$ a subspace such that $W \otimes_k R \subseteq V \otimes_k R$ is stable under F_X, then there is an induced action on $(W \otimes_k R)/(V \otimes_k R) = (W/V) \otimes_k R$ and W/V is a cofinite representation. So we see that if $\eta \colon V \to V'$ is a morphism of cofinite representations, then $\eta(V) \otimes_k R$ is stable under F_X and $V' \to V'/\eta(V)$ is a cokernel of η. So the cofinite representations of F_X are an abelian category.

As k can be identified with the endomorphisms of $\mathbb{1}$, we conclude that the cofinite representations of F_X are a tensor category (in the sense of [Del90, 2.1]).

To conclude the description of our neutral tannakian category we need a fibre functor. We take it to be the forgetful functor ω, that associates the underlying vector space V to a cofinite representations (V, ϕ).

Let $\Gamma = \underline{\mathrm{Aut}}^\otimes(\omega)$ be the fundamental group of this tannakian category. An element of $\Gamma(R)$ is, by definition, a family (λ_V), indexed by all cofinite representations, where $\lambda_V \colon V \otimes_k R \to V \otimes_k R$ is an R-linear

automorphism such that

$$
\begin{array}{ccc}
V \otimes_k R & \xrightarrow{\;\lambda_V\;} & V \otimes_k R \\
{\scriptstyle \eta \otimes R}\downarrow & & \downarrow{\scriptstyle \eta \otimes R} \\
V' \otimes_k R & \xrightarrow{\;\lambda_{V'}\;} & V' \otimes_k R
\end{array}
$$

commutes for every morphism $\eta\colon V \to V'$ of cofinite representations, $\lambda_{V \otimes_k V'} = \lambda_V \otimes \lambda_{V'}$ for all cofinite representations V, V' and $\lambda_{\mathbb{1}}$ is the identity map (on R).

We have a group homomorphism $F_X \to \Gamma(R)$, given by sending $g \in F_X$ to $(\phi(g))_{(V,\phi)}$, where (V,ϕ) ranges over all cofinite representations of F_X. We note that Γ is the projective limit of the algebraic groups $\underline{\mathrm{Aut}}^{\otimes}(\omega|_{\langle(V,\phi)\rangle_{\otimes}})$, where $\langle(V,\phi)\rangle_{\otimes}$ denotes the tensor category generated by the cofinite representation (V,ϕ), and that $\underline{\mathrm{Aut}}^{\otimes}(\omega|_{\langle(V,\phi)\rangle_{\otimes}})$ naturally embeds into $\mathrm{GL}(V)$ as a closed subgroup. The category of cofinite representations of F_X is equivalent (via ω) to the category of (finite dimensional) representations of Γ. Explicitly, a cofinite representation (V,ϕ) corresponds to the canonical projection

$$
\Gamma \to \underline{\mathrm{Aut}}^{\otimes}(\omega|_{\langle(V,\phi)\rangle_{\otimes}}) \subseteq \mathrm{GL}(V).
$$

In particular, the universal element $\mathrm{id}\colon \Gamma \to \Gamma$ corresponds to the group homomorphism $F_X \to \Gamma(R)$.

Let $\iota\colon X \to \Gamma(R)$ be the map induced by restricting $F_X \to \Gamma(R)$ to X. We have to show that ι converges to 1. So let $N \trianglelefteq \Gamma$ be a coalgebraic subgroup. Since the kernel of $\Gamma(R) \to (\Gamma/N)(R)$ is $N(R)$, it suffices to show that almost all elements of X map to 1 under $F_X \to \Gamma(R) \to (\Gamma/N)(R)$.

Let (V,ϕ) be a cofinite representation of F_X that induces a faithful representation of Γ/N. Then the diagram

$$
\begin{array}{ccc}
F_X & \xrightarrow{\;\phi\;} & \mathrm{GL}(V)(R) \\
\downarrow & & \uparrow \\
\Gamma(R) & \longrightarrow & (\Gamma/N)(R)
\end{array}
$$
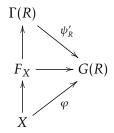
commutes. Because $(\Gamma/N)(R) \to \mathrm{GL}(V)(R)$ is injective and ϕ is cofinite, it follows that almost all elements of X map into $N(R)$. Thus ι converges to 1.

We next establish the universal property: We claim that for every proalgebraic group G and every map $\varphi\colon X \to G(R)$ converging to 1, there exists a unique morphism $\psi\colon \Gamma \to G$ such that (2) commutes.

Note that φ induces a morphism of groups $F_X \to G(R)$. Because φ converges to 1, every (finite dimensional, k-linear) representation of G induces a cofinite representation of F_X. We thus have a tensor functor $F\colon \mathrm{Rep}(G) \to \mathrm{Rep}_{cf}(F_X) = \mathrm{Rep}(\Gamma)$, compatible with the fibre functors, where $\mathrm{Rep}(G)$ denotes the tannakian category of representations of G and $\mathrm{Rep}_{cf}(F_X)$ denotes the category of cofinite representations of F_X. By [DM82, Cor. 2.9], the tensor functor F is induced by a unique morphism $\psi\colon \Gamma \to G$ of proalgebraic groups. By construction, the diagram

$$
\begin{array}{ccc}
& \Gamma(R) & \\
\nearrow & & \searrow{\scriptstyle \psi_R} \\
F_X & \longrightarrow & G(R) \\
\uparrow & & \nearrow \\
& \varphi & \\
X & &
\end{array}
$$

commutes. Moreover, if $\psi'\colon \Gamma \to G$ is another morphism of proalgebraic groups such that

$$
\begin{array}{c}
\Gamma(R) \\
\uparrow \qquad \searrow^{\psi'_R} \\
F_X \longrightarrow G(R) \\
\uparrow \qquad \nearrow_{\varphi} \\
X
\end{array}
$$

commutes, then ψ and ψ' induce the same tensor functor $\mathrm{Rep}(G) \to \mathrm{Rep}_{cf}(F_X)$ and therefore $\psi = \psi'$ (loc. cit.). So the existence of $\Gamma = \Gamma^{\mathcal{C}}_{R/k}(X)$, is established when $\mathcal{C}$ is the formation of all algebraic groups.

Let us now assume that $\mathcal{C}$ is an arbitrary formation and let (Γ, ι) be as above. We know from Lemma 2.4 that Γ has a maximal pro-$\mathcal{C}$-quotient $\Gamma^{\mathcal{C}}_{R/k}(X) = \pi_{\mathcal{C}}(\Gamma)$. Let $\iota_{\mathcal{C}}$ denote the composition

$$
\iota_{\mathcal{C}} \colon X \xrightarrow{\iota} \Gamma(R) \to \pi_{\mathcal{C}}(\Gamma)(R).
$$

By Lemma 2.12 the map $\iota_{\mathcal{C}}$ converges to 1. Since $\langle \iota(X) \rangle = \Gamma$ (as established in the first paragraph) it follows, using Lemma 2.16, that $\langle \iota_{\mathcal{C}}(X) \rangle = \pi_{\mathcal{C}}(\Gamma)$. In particular, $\langle \iota_{\mathcal{C}}(X) \rangle$ is a pro-$\mathcal{C}$-group.

To verify the universal property of $(\pi_{\mathcal{C}}(\Gamma), \iota_{\mathcal{C}})$, let G be a pro-$\mathcal{C}$-group and $\varphi\colon X \to G(R)$ a map converging to 1 such that $\langle \varphi(X) \rangle$ is a pro-$\mathcal{C}$-group. By the universal property of (Γ, ι), there exists a unique morphism $\phi\colon \Gamma \to G$ such that $\varphi = \phi_R \circ \iota$. Using Lemma 2.16, we see that

$$
\phi(\Gamma) = \phi(\langle \iota(X) \rangle) = \langle \phi_R(\iota(X)) \rangle = \langle \varphi(X) \rangle.
$$

Thus $\phi(\Gamma)$ is a pro-$\mathcal{C}$-group and by the universal property of $(\pi_{\mathcal{C}}(\Gamma), \pi)$, there exists a unique morphism $\psi\colon \pi_{\mathcal{C}}(\Gamma) \to G$ such that $\phi = \psi \circ \pi$. The commutativity of

$$
\begin{array}{ccc}
X \xrightarrow{\ \iota\ } \Gamma(R) \xrightarrow{\ \pi_R\ } \pi_{\mathcal{C}}(\Gamma)(R) \\
\ _{\varphi}\searrow \quad \downarrow^{\phi_R} \quad \swarrow_{\psi_R} \\
G(R)
\end{array}
$$

shows that $\varphi = \psi_R \circ \iota_{\mathcal{C}}$ as required. If $\psi'\colon \pi_{\mathcal{C}}(\Gamma) \to G$ is another morphism such that

$$
\varphi = \psi'_R \circ \iota_{\mathcal{C}} = (\psi' \circ \pi)_R \circ \iota,
$$

it follows from the universal property of (Γ, ι) that $\psi' \circ \pi = \phi$. But then the universal property of $(\pi_{\mathcal{C}}(\Gamma), \pi)$ yields $\psi' = \psi$. $\qquad\qquad\square$

Clearly, the pair $(\Gamma^{\mathcal{C}}_{R/k}(X), \iota)$ is uniquely determined (up to isomorphism) by the universal property.

Definition 2.18. *The proalgebraic group $\Gamma^{\mathcal{C}}_{R/k}(X)$ from Theorem 2.17 is called the* free pro-$\mathcal{C}$-group on X/R. *The proalgebraic group $\Gamma^{\mathcal{C}}(X) = \Gamma^{\mathcal{C}}_{k/k}(X)$ is called the* free pro-$\mathcal{C}$-group on X *(over k).*

If $\mathcal{C}$ is a formation of algebraic groups that is closed under taking subgroups, then the conditions $\langle \iota(X) \rangle$ is a pro-$\mathcal{C}$-group in (i) and $\langle \varphi(X) \rangle$ is a pro-$\mathcal{C}$-group in (ii) of Theorem 2.17 can be dropped (Corollary 2.10).

Remark 2.19. For a pro-$\mathcal{C}$-group to be the free pro-$\mathcal{C}$-group on X/R it suffices that it satisfies the mapping property of Theorem 2.17 for any $\mathcal{C}$-group G.

Proof. Let Γ be a pro-$\mathcal{C}$-group and $\iota\colon X \to \Gamma(R)$ be a map converging to 1 with $\langle \iota(X) \rangle$ a pro-$\mathcal{C}$-group such that for every $\mathcal{C}$-group G with a map $\varphi\colon X \to G(R)$ converging to 1 with $\langle \varphi(X) \rangle$ a $\mathcal{C}$-group, there exists a unique morphism $\psi\colon \Gamma \to G$ with $\varphi = \psi_R \circ \iota$.

Let G be a pro-$\mathcal{C}$-group and $\varphi\colon X \to G(R)$ a map converging to 1 with $\langle \varphi(X) \rangle$ a pro-$\mathcal{C}$-group. We may write $G = \varprojlim_{i \in I} G_i$ as a projective limit of $\mathcal{C}$-groups G_i with surjective transition maps $G_i \twoheadrightarrow G_j$ ($i \geq j$).

Then the induced maps $\varphi_i\colon X \xrightarrow{\iota} G(R) \xrightarrow{(\pi_i)_R} G_i(R)$ also converge to 1 (Lemma 2.12) and by Lemma 2.16 $\langle \varphi_i(X) \rangle = \pi_i(\langle \varphi(X) \rangle)$ is a $\mathcal{C}$-group. Thus there exist unique morphisms $\psi_i\colon \Gamma \to G_i$ with $\varphi = (\psi_i)_R \circ \iota$. By uniqueness the ψ_i must be compatible and therefore define a morphism $\psi\colon \Gamma \to G$. This is the unique ψ such that $\varphi = \psi_R \circ \iota$. $\qquad\square$

Remark 2.20. If k is perfect, $\Gamma^{\mathcal{C}}(X)$ is geometrically reduced by Lemma 2.14. If k is not perfect, $\Gamma^{\mathcal{C}}(X)$ need not be reduced. For example, if $\mathcal{C}$ is the formation of all algebraic groups over a field of characteristic 2, the non-reduced group H from Example 2.15 would be a quotient of $\Gamma^{\mathcal{C}}(X)$ and therefore $\Gamma^{\mathcal{C}}(X)$ cannot be reduced.

We next consider some examples of free proalgebraic groups. The first three examples explain how our notion of free proalgebraic groups encompasses previously known constructions.

Example 2.21. Let C be a formation of finite groups and let $\mathcal{C} = \mathsf{C}_k$ be the corresponding formation of algebraic groups over k (Section 2.2). Let X be a set and let $\Gamma^{\mathsf{C}}(X)$ be the free pro-C-group on X ([FJ08, Def. 17.4.1]). Then $\Gamma^{\mathcal{C}}(X) = (\Gamma^{\mathsf{C}}(X))_k$. Since $G(k) = G(L)$ for any field extension L of k and $\mathcal{C}$-group G, one actually has $\Gamma^{\mathcal{C}}_{L/k}(X) = (\Gamma^{\mathsf{C}}(X))_k$ for any field extension L of k.

Example 2.22. Let k be an algebraically closed field, X a finite set and $\mathcal{C}$ the formation of all algebraic groups. Then $\Gamma^{\mathcal{C}}(X)$ is the proalgebraic completion ([BLMM02, Def. 4]) of the (abstract) free group on X. If k has characteristic zero and X has only one element, one can show that $\Gamma^{\mathcal{C}}(X) = \mathbb{G}_a \times D(k^\times)$. See [YZh] or [BLMM02, Example 1].

Example 2.23. Free prounipotent groups over an algebraically closed field of characteristic zero were introduced in [LM82] and further studied in [LM83]. The construction and definition of free prounipotent groups given in [LM82] does not quite agree with ours, however in [LM82, Prop. 2.2] the following mapping property of $U(X)$, the free prounipotent group on a set X (in the sense of [LM82]) is established: for any unipotent algebraic group G, there is a bijection between the set of morphisms $U(X) \to G$ with the set of subsets $\{g_x|\ x \in X\}$ of $G(k)$ where $g_x = 1$ for almost all $x \in X$, such that a morphism $\psi\colon U(X) \to G$ corresponds to $\{\psi(x)|\ x \in X\}$. It is clear from the construction given in [LM82, Section 2] that the map $X \to U(X)$ converges to 1. Thus the mapping property from [LM82, Prop. 2.2] is equivalent to the mapping property of Theorem 2.17 (Remark 2.19). In other words, over an algebraically closed field of characteristic zero, $U(X) = \Gamma^{\mathcal{C}}(X)$, where $\mathcal{C}$ is the class of all unipotent algebraic groups.

If G is a unipotent algebraic group over an algebraically closed field k of characteristic zero and if $x \in G(k) \smallsetminus 1$, then $\langle x \rangle \simeq \mathbb{G}_a$. (Note that $\langle x \rangle$ is abelian and unipotent and therefore isomorphic to $\mathbb{G}_a^n$ for some n, but then necessarily $n = 1$.) It follows that $\Gamma^{\mathcal{C}}(X) = \mathbb{G}_a$ if X is a one element set.

If k is not algebraically closed, $\Gamma^{\mathcal{C}}(X)$ is more complicated. Indeed, if $k = \mathbb{Q}$ and $x = (\sqrt{2}, \sqrt{3}) \in \mathbb{G}_a^2(\bar{k})$, then $\langle x \rangle = \mathbb{G}_a^2$. Thus $\mathbb{G}_a^2$ is a quotient of $\Gamma^{\mathcal{C}}(X)$.

Example 2.24. Let k be a field of characteristic zero and $\mathcal{C}$ the formation of all abelian unipotent algebraic groups. Thus an algebraic group is in $\mathcal{C}$ if and only if it is isomorphic to $\mathbb{G}_a^n$ for some n ([Mil17, Cor. 16.15]). For any set X and k-algebra R we have $\Gamma^{\mathcal{C}}_{R/k}(X) = \prod_Y \mathbb{G}_a$, where Y is a set of cardinality $|X| \cdot \dim_k(R)$.

Proof. Let B be a k-basis of R and set $Y = X \times B$. We define $\iota\colon X \to \prod_Y \mathbb{G}_a(R)$ by

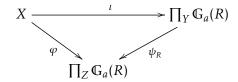$$\iota(x)_y = \begin{cases} b & \text{if } y = (x,b), \\ 0 & \text{otherwise.} \end{cases}$$

The kernels of the projections $\prod_Y \mathbb{G}_a \to \prod_{Y'} \mathbb{G}_a$, where Y' is a finite subset of Y are a neighborhood basis at 1 for $\prod_Y \mathbb{G}_a$. Every such kernel contains almost all elements of $\iota(X)$. Thus ι converges to one.

Let G be a pro-$\mathcal{C}$-group and $\varphi\colon X \to G(R)$ a map converging to 1. Then G is isomorphic to $\prod_Z \mathbb{G}_a$ for some set Z. For $x \in X$ and $z \in Z$ we can write $\varphi(x)_z = \sum_{b \in B} \lambda(b,x,z)b \in R$ for uniquely determined

$\lambda(b,x,z) \in k$. We define $\psi \colon \prod_Y \mathbb{G}_a \to \prod_Z \mathbb{G}_a$ by

$$\psi((s_y)_{y \in Y}) = \left(\sum_{x \in X} \sum_{b \in B} \lambda(b,x,z) s_{(x,b)} \right)_{z \in Z} \in \prod_Z \mathbb{G}_a(S)$$

for any k-algebra S and $(s_y)_{y \in Y} \in \prod_Y \mathbb{G}_a(S)$. The above sum is finite because φ converges to 1. Then ψ is the unique morphism such that

$$
\begin{array}{ccc}
X & \xrightarrow{\ \ \iota\ \ } & \prod_Y \mathbb{G}_a(R) \\
& {\scriptstyle\varphi}\searrow \quad \swarrow{\scriptstyle\psi_R} & \\
& \prod_Z \mathbb{G}_a(R) &
\end{array}
$$

commutes. $\square$

Example 2.25. Let $\mathcal{C}$ be the class of all diagonalizable algebraic groups, R a k-algebra and X a set. Then $\Gamma_{R/k}^{\mathcal{C}}(X) = D(\oplus_X R^\times)$. Here $\oplus_X R^\times$ is the direct sum of $|X|$ copies of the abelian group $R^\times$.

Proof. Let us define $\iota \colon X \to D(\oplus_X R^\times)(R) = \mathrm{Hom}(\oplus_X R^\times, R^\times)$ as the map that sends $x \in X$ to the projection $\pi_x \colon \oplus_X R^\times \to R^\times$ that picks out the x-component. We need to check that ι converges to 1.

In general, if M is an abelian group, the inclusion map $N = D(M') \hookrightarrow D(M)$ of a coalgebraic subgroup into $D(M)$, corresponds to a quotient map $M \twoheadrightarrow M'$ of abelian groups with a finitely generated kernel. So ι converges to 1, because for every finitely generated subgroup A of $\oplus_X R^\times$, $A \subseteq \ker(\pi_x)$ for almost all $x \in X$.

Let $G = D(M)$ be a pro-$\mathcal{C}$-group and $\varphi \colon X \to G(R)$ a map converging to 1. We have to find $\psi \colon D(\oplus_X R^\times) \to G$ such that

(3)
$$
\begin{array}{ccc}
X & \xrightarrow{\ \ \iota\ \ } & D(\oplus_X R^\times)(R) \\
& {\scriptstyle\varphi}\searrow \quad \swarrow{\scriptstyle\psi_R} & \\
& G(R) &
\end{array}
$$

commutes. This corresponds to finding a morphism $\widetilde{\psi} \colon M \to \oplus_X R^\times$ of abelian groups such that

(4)
$$
\begin{array}{ccc}
M & \xrightarrow{\ \ \widetilde{\psi}\ \ } & \oplus_X R^\times \\
& {\scriptstyle\varphi(x)}\searrow \quad \swarrow{\scriptstyle\pi_x} & \\
& R^\times &
\end{array}
$$

commutes for all $x \in X$. Clearly, the unique solution to this problem is given by $\widetilde{\psi}(m) = \oplus_{x \in X} \varphi(x)(m)$ for $m \in M$. Note that this sum is finite because φ converges to 1. $\square$

We would like to warn the reader that the formation of free pro-$\mathcal{C}$-groups is not compatible with extension of the base field in the sense that, for example, the free pro-diagonalizable group over k' on X can be obtained from the free pro-diagonalizable group over k by base extension from k to k'.

We conclude this section with two lemmas that will be needed later. The following lemma is fundamental for showing that certain embedding problems for free pro-$\mathcal{C}$-groups are solvable.

Lemma 2.26. *Let k be field of characteristic zero and let G be an algebraic group. Then there exists a finite subset X of $G(\overline{k})$ such that $G = \langle X \rangle$.*

Proof. A proof, under the additional assumption that k is algebraically closed, can be found in [vdPS03, Lemma 5.13]. But if X generates $G_{\overline{k}}$, then X also generates G. $\square$

The above lemma fails in positive characteristic, even for smooth groups, for example $\mathbb{G}_a$ is not finitely generated in positive characteristic.

Lemma 2.27. *Let k be a field of characteristic zero, X an infinite set and $\mathcal{C}$ a formation. Then $\Gamma^{\mathcal{C}}(X)$ is not an algebraic group.*

Proof. By assumption there exists a non-trivial $\mathcal{C}$-group G. Since k has characteristic zero $G(\overline{k}) \neq 1$ and we can choose $g \in G(\overline{k})$ with $g \neq 1$. Moreover, by Lemma 2.26, we can find $g_1, \ldots, g_n \in G(\overline{k})$ such that $G = \langle g_1, \ldots, g_n \rangle$. Pick $x_1, \ldots, x_n \in X$ and for every finite subset Y of X containing $x_1, \ldots, x_n$ define a map $\varphi_Y \colon X \twoheadrightarrow G(\overline{k})$ by $\varphi_Y(x_i) = g_i$, $(i = 1, \ldots, n)$, $\varphi_Y(y) = g$ for $y \in Y \smallsetminus \{x_1, \ldots, x_n\}$ and $\varphi_Y(x) = 1$ for $x \in X \smallsetminus Y$. Then φ_Y converges to 1 and therefore defines an epimorphism $\phi_Y \colon \Gamma^{\mathcal{C}}(X) \twoheadrightarrow G$.

Let $\{x_1, \ldots, x_n\} \subsetneqq Y_1 \subsetneqq Y_2 \subsetneqq \ldots$ be a strictly ascending chain of finite subsets of X. For $i \geq 1$ set $N_i = \bigcap_{j=1,\ldots,i} \ker(\phi_{Y_i})$. If $y \in Y_{i+1} \smallsetminus Y_i$, then $\iota(y) \notin N_{i+1}(\overline{k})$ but $\iota(y) \in N_i(\overline{k})$. Thus $N_1 \supsetneqq N_2 \supsetneqq \ldots$ is a strictly descending chain of closed subgroups of $\Gamma^{\mathcal{C}}(X)$. Hence $\Gamma^{\mathcal{C}}(X)$ cannot be an algebraic group. $\qquad\square$

3. Saturated pro-$\mathcal{C}$-groups

The main goal of this section is to characterize free pro-$\mathcal{C}$-groups in terms of embedding problems. To achieve this goal we first study certain pro-$\mathcal{C}$-groups that solve "many" embedding problems, we call these groups *saturated*.

3.1. The rank of a proalgebraic group

As we will show, for any formation $\mathcal{C}$ there exists up to isomorphism a unique saturated pro-$\mathcal{C}$-group Γ, once we fix the "size" of Γ and this size is sufficiently big. The goal of this subsection is to make precise this notion of size by introducing the rank of a proalgebraic group.

The rank of a profinite group G can be defined as the smallest cardinal number κ such that G has a set of κ (topological) generators that converges to 1. At first sight, it may seem plausible to define the rank $r(G)$ of a proalgebraic group G, say over an algebraically closed field k, as the smallest cardinal κ such that there exists a subset X of $G(k)$ converging to 1 with $\langle X \rangle = G$. However, this approach has drawbacks and yields pathologies. For example, over a field of positive characteristic, there may not exist such an X. (This is for example the case for $\mathbb{G}_a$.)

Also, for an infinite index set I, $r(\prod_{i \in I} \mathbb{G}_a)$ and $r(\prod_{i \in I} \mathbb{G}_m)$ behave quite differently. If k has characteristic zero, then $r(\prod_{i \in I} \mathbb{G}_a)$ is infinite. On the other hand, if k has transcendence degree greater or equal to $|I|$, then $r(\prod_{i \in I} \mathbb{G}_m) = 1$ since $(g_i)_{i \in I}$ is a generator if $(g_i)_{i \in I}$ are algebraically independent over the prime field.

Below we will define the rank $\mathrm{rank}(G)$ for any proalgebraic group G. It satisfies the following equalities $\mathrm{rank}(\prod_{i \in I} \mathbb{G}_a) = \mathrm{rank}(\prod_{i \in I} \mathbb{G}_m) = |I|$.

Proposition 3.1. *Let G be a proalgebraic group that is not algebraic. Then the following cardinals are equal.*

(i) *The dimension of $k[G]$ as a k-vector space.*

(ii) *The smallest cardinal κ such that $k[G]$ can be generated as a k-algebra by κ elements.*

(iii) *The smallest cardinal κ such that $k[G]$ is the directed union of κ finitely generated Hopf subalgebras.*

(iv) *The smallest cardinal κ such that there exists a neighborhood basis at 1 for G of cardinality κ.*

(v) *The smallest cardinal κ such that there exists a directed set I of cardinality κ and algebraic groups G_i with $G \simeq \varprojlim_{i \in I} G_i$.*

Proof. For $i = 1, \ldots, 5$ let κ_i denote the cardinal defined in point (i) above. Clearly, $\kappa_2 \leq \kappa_1$. On the other hand, if $(f_i)_{i \in I}$ generates $k[G]$ as a k-algebra, then $\bigcup_{J \subseteq I} F_J$ generates $k[G]$ as a k-vector space, where, for

every finite subset J of I the set F_J consists of all monomials in $(f_j)_{j \in J}$. As $\bigcup_{J \subseteq I} F_J$ is the union of $|I|$ countable subsets, we see that $k[G]$ can be generated by $|I|$ elements as a k-vector space. Thus $\kappa_1 \leq \kappa_2$.

Assume that $(f_i)_{i \in I}$ generates $k[G]$ as a k-algebra. For every finite subset J of I let A_J be the smallest Hopf subalgebra of $k[G]$ that contains all the f_j for $j \in J$. Then A_J is finitely generated as a k-algebra ([Wat79, Section 3.3]) and the A_J's form a directed system whose union is $k[G]$. Thus $\kappa_3 \leq \kappa_2$. On the other hand, choosing a finite set of generators for every Hopf subalgebra in a directed system shows that $\kappa_2 \leq \kappa_3$. As finitely generated Hopf subalgebras correspond to coalgebraic subgroups we have $\kappa_3 = \kappa_4$.

If $\mathcal{N}$ is a neighborhood basis at 1 for G, then $G \simeq \varprojlim_{N \in \mathcal{N}} G/N$. Conversely, if $G \simeq \varprojlim_{i \in I} G_i$, and N_i is the kernel of the projection $G \to G_i$, then the N_i are a neighborhood basis at 1 for G. Thus $\kappa_4 = \kappa_5$.   □

We would like to define the *rank* of a proalgebraic group as the quantity characterized in Proposition 3.1. We note that this notion of rank has nothing to do with the classical notion of rank for algebraic groups defined as the dimension of a Cartan subgroup. For an algebraic group G, the quantities defined in (iii), (iv) and (v) of Proposition 3.1 are all equal to 1, but the quantities defined in (i) and (ii) may be distinct and different from 1. For example, for $G = \mathbb{G}_a^2$, the quantity defined in (i) is $|\mathbb{N}|$, whereas the quantity defined in (ii) is 2. The exact definition of the rank of an algebraic group is largely irrelevant for what follows (as long as it is finite). The notationally most convenient choice is to set it equal to 1 for a non-trivial algebraic group and equal to 0 for the trivial group. We therefore make the following definition.

Definition 3.2. *The* rank $\operatorname{rank}(G)$ *of a non-trivial proalgebraic group* G *is the smallest cardinal* κ *such that there exists a neighborhood basis at* 1 *for* G *of cardinality* κ. *The rank of the trivial algebraic group is* 0.

Thus the rank of a proalgebraic group G is finite if and only if G is algebraic. Let G be an infinite profinite group and let $G = \mathsf{G}_k$ denote the corresponding proalgebaic group. The cardinality of a neighborhood basis at 1 for G consisting of open normal subgroups does not depend on the neighborhood basis and agrees with the minimal cardinality of any neighborhood basis at 1 for G (not necessarily consisting of groups). This cardinal number is denoted by $w_0(\mathsf{G})$ in [RZ10]. Since the coalgebraic subgroups of G are in one-to-one correspondence with the open normal subgroups of G, it follows that $\operatorname{rank}(G) = w_0(\mathsf{G})$. In particular, if G is not (topologically) finitely generated, it follows that $\operatorname{rank}(G) = \operatorname{rank}(\mathsf{G})$. (See [RZ10, Cor. 2.6.3] or [FJ08, Prop. 17.1.2].) So the rank for proalgebraic groups generalizes the notion of rank for profinite groups.

Example 3.3. Let $(G_i)_{i \in I}$ be an infinite family of non-trivial algebraic groups and $G = \prod_{i \in I} G_i$. Then $\operatorname{rank}(G) = |I|$. More generally, for an arbitrary set I let $\phi_i \colon G_i \twoheadrightarrow H$ ($i \in I$) be a family of epimorphisms of proalgebraic groups. Let $\prod_{i \in I}(G_i \twoheadrightarrow H)$ denote the functor from the category of k-algebras to the category of groups defined by

$$\left(\prod_{i \in I}(G_i \twoheadrightarrow H) \right)(R) = \{(g_i)_{i \in I} |\ g_i \in G_i(R),\ \phi_i(g_i) = \phi_j(g_j)\ \forall\ i, j \in I\}$$

for any k-algebra R. This functor is representable, i.e., a proalgebraic group. Indeed, it is represented by $\varinjlim k[G_{i_1}] \otimes_{k[H]} \dots \otimes_{k[H]} k[G_{i_n}]$, where the direct limit is taken over all finite subsets $\{i_1, \dots, i_n\}$ of I ordered by inclusion. We call $\prod_{i \in I}(G_i \twoheadrightarrow H)$ the *fibre product* of the ϕ_i. If $H = 1$ this simply reduces to the product. If $I = \{1, 2\}$ one usually writes $G_1 \times_H G_2$ for the corresponding fibre product.

It follows from the above description of the coordinate ring of the fibred product that if κ is an infinite cardinal such that $\operatorname{rank}(G_i) \leq \kappa$ and $|I| \leq \kappa$, then $\operatorname{rank}(\prod_{i \in I}(G_i \twoheadrightarrow H)) \leq \kappa$.

Example 3.4. If M is a non-trivial abelian group, then $\operatorname{rank}(D(M)) = |M|$ unless M is finitely generated, in which case $\operatorname{rank}(D(M)) = 1$.

Lemma 3.5. *Let G be a proalgebraic group. If H is a closed subgroup or a quotient of G, then its rank is such that* $\operatorname{rank}(H) \leq \operatorname{rank}(G)$.

Proof. This is clear if G is algebraic and if G is not algebraic the statement follows from Proposition 3.1, using e.g., characterization (i). □

Lemma 3.6. *Let* $\phi\colon G \twoheadrightarrow H$ *be an epimorphism of proalgebraic groups with algebraic kernel. Then we have* $\mathrm{rank}(G) = \mathrm{rank}(H)$.

Proof. By Lemma 3.5 it suffices to show that $\mathrm{rank}(G) \leq \mathrm{rank}(H)$. By Corollary 2.9 there exists a coalgebraic subgroup M of G such that $M \cap \ker(\phi) = 1$. Let $\mathcal{N}$ be a neighborhood basis at 1 for H. We claim that the set $\mathcal{N}' = \{\phi^{-1}(N) \cap M \mid N \in \mathcal{N}\}$ is a neighborhood basis at 1 for G. First of all, note that $\phi^{-1}(N) \cap M \leq G$ is coalgebraic because $\phi^{-1}(N)$ and M are coalgebraic. Furthermore, $\mathcal{N}'$ is downward directed because $\mathcal{N}$ is and

$$\bigcap_{N\in\mathcal{N}} (\phi^{-1}(N) \cap M) = \phi^{-1}\big(\bigcap_{N\in\mathcal{N}} N\big) \cap M = \ker(\phi) \cap M = 1.$$

Thus $\mathrm{rank}(G) \leq \mathrm{rank}(H)$. □

Lemma 3.7. *Let* G *be a proalgebraic group and* $(N_i)_{i\in I}$ *a family of closed normal subgroups of* G. *If* $\mathrm{rank}(G/N_i) \leq \kappa$ *for all* $i \in I$ *and* $|I| \leq \kappa$, *then* $\mathrm{rank}(G/\cap N_i) \leq \kappa$.

Proof. The statement is clear for finite κ. So let us assume that κ is infinite. We have the inclusions $k[G/N_i] \subseteq k[G/\cap N_i] \subseteq k[G]$ and all the $k[G/N_i]$ generate $k[G/\cap N_i]$ as a k-algebra. Thus joining the generators of the individual $k[G/N_i]$, gives generators for $k[G/\cap N_i]$. Consequently, $k[G/\cap N_i]$ can be generated by $\kappa \cdot \kappa = \kappa$ elements. Thus the claim follows from Proposition 3.1. □

The following proposition shows that the rank can also be understood as the minimal length of a subnormal series satisfying certain conditions.

Proposition 3.8. *Let* G *be a proalgebraic group and* μ *an ordinal number. If there exists a chain*

$$G = N_0 \geq N_1 \geq \ldots \geq N_\lambda \geq \ldots \geq N_\mu = 1$$

of normal closed subgroups N_λ *of* G *($\lambda \leq \mu$) with*

  (i) $N_\lambda/N_{\lambda+1}$ *algebraic for all* $\lambda < \mu$ *and*

  (ii) $N_\lambda = \bigcap_{\lambda'<\lambda} N_{\lambda'}$ *if* λ *is a limit ordinal,*

then $\mathrm{rank}(G) \leq |\mu|$. *Moreover, there exists an ordinal number* μ *with* $|\mu| = \mathrm{rank}(G)$ *and a chain as above satisfying (i) and (ii). In particular,* $\mathrm{rank}(G) = \min |\mu|$, *where* μ *ranges over all ordinals for which there exists such a chain.*

Proof. We will show by transfinite induction that $\mathrm{rank}(G/N_\lambda) \leq |\lambda|$ for every $\lambda \leq \mu$. The initial case $\lambda = 0$ is true by definition. If $\lambda = \lambda' + 1$ is a successor ordinal, then $G/N_{\lambda'+1} \twoheadrightarrow G/N_{\lambda'}$ has kernel $N_{\lambda'}/N_{\lambda'+1}$. Thus $\mathrm{rank}(G/N_\lambda) = \mathrm{rank}(G/N_{\lambda'}) \leq |\lambda'| \leq |\lambda|$ by Lemma 3.6. If λ is a limit ordinal, then $\mathrm{rank}(G/N_\lambda) \leq |\lambda|$ by Lemma 3.7.

Let us now show that there exists a chain with $|\mu| = \mathrm{rank}(G)$. Let $\mathcal{N}$ be a neighborhood basis at 1 for G with $|\mathcal{N}| = \mathrm{rank}(G)$ and let μ be an ordinal number with $|\mu| = |\mathcal{N}|$. So we may write $\mathcal{N} = \{U_\lambda \mid \lambda < \mu\}$. For $\lambda \leq \mu$ we set $N_\lambda = \bigcap_{\lambda'<\lambda} U_\lambda$. Clearly the N_λ's form a descending chain of normal closed subgroups of G such that $N_0 = N$ and $N_\mu = 1$. Moreover $N_\lambda/N_{\lambda+1} = N_\lambda/(N_\lambda \cap U_{\lambda+1}) = U_{\lambda+1}N_\lambda/U_{\lambda+1}$ is algebraic, because $U_{\lambda+1}N_\lambda/U_{\lambda+1}$ embeds into $N/U_{\lambda+1}$. Clearly (ii) is satisfied. □

Our next goal is to determine the rank of a free pro-$\mathcal{C}$-group. The following lemma yields a lower bound.

Lemma 3.9. *Let* G *be a proalgebraic group that is not algebraic and let* R *be a* k-*algebra. If* $X \subseteq G(R)$ *converges to 1, then* $|X| \leq \mathrm{rank}(G)$.

Proof. Let $\mathcal{N}$ be a neighborhood basis at 1 for G. We have $X = \bigcup_{N\in\mathcal{N}}(X \smallsetminus N(R))$ (assuming w.l.o.g. $1 \notin X$) with $X \smallsetminus N(R)$ finite. So $|X| \leq |\mathcal{N}|$. □

The next lemma yields an upper bound for the rank of free pro-$\mathcal{C}$-groups.

Lemma 3.10. *Let $\mathcal{C}$ be a formation and let X be a set. Then $\Gamma^{\mathcal{C}}(X)$ has at most $|\overline{k}||X|$ coalgebraic subgroups.*

Proof. Let $\mathcal{N}$ denote the set of all coalgebraic subgroups of $\Gamma^{\mathcal{C}}(X)$. These all arise as kernels of some epimorphism $\phi\colon \Gamma^{\mathcal{C}}(X) \twoheadrightarrow H$ for some $\mathcal{C}$-group H. Such a ϕ is determined by choosing a finite subset $\{x_1,\dots,x_n\}$ of X and the images $\phi_{\overline{k}}(x_1),\dots,\phi_{\overline{k}}(x_n) \in H(\overline{k})$. For a fixed H, there are $|X||H(\overline{k})|$ choices. There are, up to isomorphism, at most $|\overline{k}|$ algebraic groups over k. Thus, also allowing H to vary, we see that there are at most $|\overline{k}||X|$ coalgebraic subgroups. $\qquad\square$

Combining the previous two lemmas we obtain:

Corollary 3.11. *Let $\mathcal{C}$ be a formation and let X be a set such that $\Gamma^{\mathcal{C}}(X)$ is not algebraic. Then*

$$(5) \qquad\qquad\qquad |X| \leq \operatorname{rank}(\Gamma^{\mathcal{C}}(X)) \leq |\overline{k}||X|.$$

In particular, if $|X| \geq |\overline{k}|$, then $\operatorname{rank}(\Gamma^{\mathcal{C}}(X)) = |X|$. $\qquad\square$

Both extreme cases of inequality (5) may occur: If X is an infinite set and $\mathcal{C}$ is the formation of all abelian unipotent groups over an algebraically closed field of characteristic zero, then $\operatorname{rank}(\Gamma^{\mathcal{C}}(X)) = |X|$ by Example 2.24. On the other hand, if $\mathcal{C}$ is the formation of all diagonalizable algebraic groups, then $\operatorname{rank}(\Gamma^{\mathcal{C}}(X)) = |\overline{k}||X|$ by Example 2.25.

In some rare cases $\Gamma^{\mathcal{C}}(X)$ can indeed be an algebraic group and then the inequality $|X| \leq \operatorname{rank}(\Gamma^{\mathcal{C}}(X))$ from Corollary 3.11 may not hold. For example, if k is an algebraically closed field of characteristic zero, X a finite set and $\mathcal{C}$ the formation of all abelian unipotent groups, then $\Gamma^{\mathcal{C}}(X) = \mathbb{G}_a^n$, where $n = |X|$, by Example 2.24. Also, if k is a field of positive characteristic and $\mathcal{C}$ is the formation of all infinitesimal algebraic groups, then $\Gamma^{\mathcal{C}}(X) = 1$ for any set X (since $G(\overline{k}) = 1$ for any infinitesimal algebraic group G). However, if k has characteristic zero and X is infinite, then $\Gamma^{\mathcal{C}}(X)$ is not algebraic by Lemma 2.27. We thus obtain from Corollary 3.11:

Corollary 3.12. *Let k be a field of characteristic zero, $\mathcal{C}$ a formation and X a set with $|X| \geq |k|$. Then $\operatorname{rank}(\Gamma^{\mathcal{C}}(X)) = |X|$.* $\qquad\square$

We record one more lemma for later use.

Lemma 3.13. *Let $\mathcal{C}$ be a formation and let X be an infinite set. If $\phi\colon \Gamma^{\mathcal{C}}(X) \twoheadrightarrow H$ is an epimorphism such that $\operatorname{rank}(H) < |X|$, then $|X|$ many elements of X map into $\ker(\phi)(\overline{k})$.*

Proof. If $\operatorname{rank}(H)$ is finite the statement is obvious, so let us assume that $\operatorname{rank}(H)$ is infinite.

Let $\mathcal{N}$ be a neighborhood basis at 1 for H with $|\mathcal{N}| = \operatorname{rank}(H)$. Since $\ker(\phi) = \bigcap_{N \in \mathcal{N}} \phi^{-1}(N)$, we have

$$X \smallsetminus \iota^{-1}(\ker(\phi)(\overline{k})) = \bigcup_{N \in \mathcal{N}} (X \smallsetminus \iota^{-1}(\phi^{-1}(N)(\overline{k}))),$$

where $\iota\colon X \to \Gamma^{\mathcal{C}}(X)(\overline{k})$ is the map from Theorem 2.17. The right hand side has cardinality bounded by $|\mathcal{N}| = \operatorname{rank}(H) < |X|$. Thus $|X \cap \iota^{-1}(\ker(\phi)(\overline{k}))| = |X|$. $\qquad\square$

3.2. The dimension of a proalgebraic group

For our characterization of saturated pro-$\mathcal{C}$-groups we will also need another measure for the size of a proalgebraic group that is different from the rank. Let G be a proalgebraic group. Then the nilradical $\mathfrak{a}$ of $k[G^o]$ is a prime ideal and we can define the dimension $\dim(G)$ of G as the transcendence degree over k of the field of fractions of $k[G^o]_{\mathrm{red}} = k[G^o]/\mathfrak{a} = k[(G^o)_{\mathrm{red}}]$. If G is an algebraic group this is simply the usual dimension of G.

Lemma 3.14. *Let G be a proalgebraic group. If H is a closed subgroup or a quotient of G, then we have* $\dim(H) \le \dim(G)$.

Proof. Let us first consider an epimorphism $G \twoheadrightarrow H$. Then we have an induced epimorphism $G^o \twoheadrightarrow H^o$. We therefore get inclusions $k[H^o] \subseteq k[G^o]$ and $k[H^o]_{\mathrm{red}} \subseteq k[G^o]_{\mathrm{red}}$. Thus $\dim(G) \ge \dim(H)$.

If H is a closed subgroup of G, then H^o is a closed subgroup of G^o. We therefore have a surjection $k[G^o] \twoheadrightarrow k[H^o]$ that induces a surjection $k[G^o]_{\mathrm{red}} \twoheadrightarrow k[H^o]_{\mathrm{red}}$. Thus $\dim(H) \le \dim(G)$. $\qquad\square$

Lemma 3.15. *Let $\phi\colon G \twoheadrightarrow H$ be an epimorphism of proalgebraic groups with $\dim(\ker(\phi)) = 0$. Then we have* $\dim(G) = \dim(H)$.

Proof. By Lemma 3.14 the kernel of the induced epimorphism $G^o \twoheadrightarrow H^o$ also has dimension zero. We can thus assume that G and H are connected. It suffices to show that every element of $k[G]_{\mathrm{red}}$ is algebraic over the field of fractions of $k[H]_{\mathrm{red}}$. Let $f \in k[G]$. Then $f \in k[G/N]$ for some coalgebraic subgroup N of G. The kernel $\ker(\phi)N/N = \ker(\phi)/(\ker(\phi) \cap N)$ of the epimorphism $G/N \twoheadrightarrow H/\phi(N)$ of algebraic groups has dimension zero by Lemma 3.14. So G/N and $H/\phi(N)$ have the same dimension. Therefore every element in $k[G/N]_{\mathrm{red}}$ is algebraic over the field of fractions of $k[H/\phi(N)]_{\mathrm{red}}$. In particular, the image of f in $k[G/N]_{\mathrm{red}} \subseteq k[G]_{\mathrm{red}}$ is algebraic over the field of fractions of $k[H]_{\mathrm{red}}$. $\qquad\square$

Lemma 3.16. *Let G be a proalgebraic group that is not algebraic. Then $\dim(G) \le \mathrm{rank}(G)$.*

Proof. As $\dim(G) = \dim(G^o)$ and $\mathrm{rank}(G^o) \le \mathrm{rank}(G)$ we may assume that G is connected. We can choose a transcendence basis for the fraction field of $k[G]_{\mathrm{red}}$ that lies inside $k[G]_{\mathrm{red}}$ and lift it to a subset of $k[G]$. This subset is k-linearly independent and therefore the k-dimension of $k[G]$ is at least the dimension of G. $\qquad\square$

Lemma 3.17. *Let G be a proalgebraic group and $(N_i)_{i \in I}$ a family of normal closed subgroup such that $G/\cap N_i$ has positive dimension. Then there exist an $i \in I$ such that G/N_i has positive dimension.*

Proof. Since $(G/\cap N_i)^o = G^o/\cap(G^o \cap N_i)$ we may assume that G is connected. As $k[G/\cap N_i]$ is generated by the subalgebras $k[G/N_i]$, the same property holds after modding out by the nilradical. Thus $\dim(G/N_i) > 0$ for some $i \in I$. $\qquad\square$

Lemma 3.18. *Let $\alpha\colon G \twoheadrightarrow H$ be an epimorphism of algebraic groups such that $\dim(\ker(\alpha)) > 0$ and let I be a set. Then $\dim(\prod_I(G \twoheadrightarrow H)) \ge |I|$.*

Proof. Since $\prod_I(G \twoheadrightarrow H)$ contains the closed subgroup $\prod_I \ker(\alpha)$ it suffices to see that $\dim(\prod_I \ker(\alpha)) \ge |I|$. But this follows rather directly from the definition. $\qquad\square$

3.3. Embedding problems

We are now prepared to make precise the idea of a proalgebraic group that solves many embedding problems.

Definition 3.19. *An* embedding problem *for a proalgebraic group Γ consists of two epimorphisms $\alpha\colon G \twoheadrightarrow H$ and $\beta\colon \Gamma \twoheadrightarrow H$ of proalgebraic groups. A* solution *is an epimorphism $\phi\colon \Gamma \twoheadrightarrow G$ such that $\beta = \alpha\phi$, i.e.,*

(6)

$$
\begin{array}{ccc}
& \Gamma & \\
& \downarrow \searrow^{\beta} & \\
G & \xrightarrow{\ \alpha\ } & H
\end{array}
$$

commutes. A morphism $\phi\colon \Gamma \to G$ (that is not necessarily an epimorphism) such that $\beta = \alpha\phi$ is called a weak solution. *We also refer to diagram (6) as the embedding problem. If there exists a solution the embedding problem is called* solvable. *The kernel of (6) is $\ker(\alpha)$. If the kernel of (6) is trivial, (6) is called a* trivial embedding

problem. *(In this case, $\alpha^{-1}\beta$ is the unique solution.) The embedding problem (6) is algebraic if G (and therefore also H) are algebraic groups.*

Let $\mathcal{C}$ be a formation and assume that Γ is a pro-$\mathcal{C}$-group. Then (6) is a pro-$\mathcal{C}$-embedding problem if G is a pro-$\mathcal{C}$-group. If G is in $\mathcal{C}$, then (6) is a $\mathcal{C}$-embedding problem.

It is instructive to reformulate (6) in terms of Hopf algebras. Given the two inclusions $k[H] \subseteq k[G]$ and $k[H] \subseteq k[\Gamma]$, we would like to find an embedding of $k[G]$ into $k[\Gamma]$ over $k[H]$.

Roughly speaking, we are interested in pro-$\mathcal{C}$-groups that solve as many pro-$\mathcal{C}$-embedding problems as possible. There does not exist a pro-$\mathcal{C}$-group Γ such that all pro-$\mathcal{C}$-embedding problems (6) for Γ are solvable. For example, if $H = \Gamma$, β is the identity map and (6) is non-trivial, then (6) does not have a solution. Also, if $\mathrm{rank}(G) > \mathrm{rank}(\Gamma)$, there cannot exist an epimorphism $\Gamma \to G$ (Lemma 3.5). It turns out that imposing the restrictions $\mathrm{rank}(H) < \mathrm{rank}(\Gamma)$ and $\mathrm{rank}(G) \le \mathrm{rank}(\Gamma)$ is sufficient to allow for the existence of a pro-$\mathcal{C}$-group that solves all such pro-$\mathcal{C}$-embedding problems. Moreover, for every cardinal number $\kappa \ge |\bar{k}|$, there exists a unique such pro-$\mathcal{C}$-group Γ with $\mathrm{rank}(\Gamma) = \kappa$ (Theorems 3.37 and 3.38).

The following theorem summarizes several well-known characterizations of profinite groups that solve many embedding problems. See [RZ10, Section 3.5] or [FJ08, Section 25.1].

Theorem 3.20. *Let C be a formation of finite groups and Γ a pro-C-group of infinite rank. We consider non-trivial pro-C-embedding problems*

(7)

$$
\begin{array}{ccc}
 & & \Gamma \\
 & & \Big\downarrow {\scriptstyle\beta} \\
\mathsf{G} & \xrightarrow{\ \alpha\ } & \mathsf{H}
\end{array}
$$

for Γ. The following statements are equivalent:

(i) *Every pro-C-embedding problem (7) with $\mathrm{rank}(\mathsf{H}) < \mathrm{rank}(\Gamma)$ and $\mathrm{rank}(\mathsf{G}) \le \mathrm{rank}(\Gamma)$ has a solution.*

(ii) *Every pro-C-embedding problem (7) with $\mathrm{rank}(\mathsf{H}) < \mathrm{rank}(\Gamma)$ and finite kernel has a solution.*

(iii) *Every pro-C-embedding problem (7) with $\mathrm{rank}(\mathsf{H}) < \mathrm{rank}(\Gamma)$ such that $\ker(\alpha)$ is a finite minimal normal subgroup of G has a solution.*

(iv) *Every C-embedding problem (7) has $\mathrm{rank}(\Gamma)$ solutions.*

To state our generalization of Theorem 3.20 we need two more definitions.

Definition 3.21. *Let $N \ne 1$ be a normal closed subgroup of a proalgebraic group G such that N is an algebraic group. If N is finite, N is an almost minimal normal subgroup of G if for every normal closed subgroup N' of G with $N' \subseteq N$ either $N' = N$ or $N' = 1$. If N is not finite, N is an almost minimal normal subgroup of G if for every normal closed subgroup N' of G with $N' \subseteq N$ either $N' = N$ or N' is finite.*

An embedding problem (6) has almost minimal kernel, if its kernel is an almost minimal normal subgroup of G.

Definition 3.22. *A family $(\phi_i)_{i \in I}$ of solutions of (6) is called independent if the induced morphism $\prod_{i \in I} \phi_i \colon \Gamma \to \prod_{i \in I}(G \twoheadrightarrow H)$ is an epimorphism.*

Remark 3.23. Since the coordinate ring of $\prod_{i \in I}(G \twoheadrightarrow H)$ is the union (direct limit) of tensor products $k[G] \otimes_{k[H]} \dots \otimes_{k[H]} k[G]$, we see that the family $(\phi_i)_{i \in I}$ is independent if and only if for every finite subset $\{i_1, \dots, i_n\}$ of I the morphism $k[G] \otimes_{k[H]} \dots \otimes_{k[H]} k[G] \to k[\Gamma]$, $a_1 \otimes \dots \otimes a_n \mapsto \phi_{i_1}^*(a_1) \cdots \phi_{i_n}^*(a_n)$ is injective. Thus, independence of the ϕ_i, corresponds to linear independence (over $k[H] = k[\Gamma/\ker(\beta)]$) of the $k[\Gamma/\ker(\phi_i)]$ inside $k[\Gamma]$.

The main goal of this section is to prove the following theorem, which generalizes Theorem 3.20 from finite groups to algebraic groups.
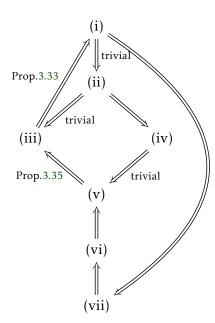
Theorem 3.24. *Let C be a formation and Γ a pro-C-group of infinite rank. We consider non-trivial pro-C-embedding problems*

(8)
$$
\begin{array}{ccc}
 & & \Gamma \\
 & \swarrow & \downarrow \beta \\
G & \xrightarrow{\alpha} & H
\end{array}
$$

for Γ. The following statements are equivalent:

  (i) *Every pro-C-embedding problem (8) with $\operatorname{rank}(H) < \operatorname{rank}(\Gamma)$ and $\operatorname{rank}(G) \leq \operatorname{rank}(\Gamma)$ has a solution.*

 (ii) *Every pro-C-embedding problem (8) with $\operatorname{rank}(H) < \operatorname{rank}(\Gamma)$ and algebraic kernel has a solution.*

(iii) *Every pro-C-embedding problem (8) with $\operatorname{rank}(H) < \operatorname{rank}(\Gamma)$ and almost minimal kernel has a solution.*

 (iv) *For every C-embedding problem (8) and every normal closed subgroup N of Γ with $\operatorname{rank}(\Gamma/N) < \operatorname{rank}(\Gamma)$ and $N \subseteq \ker(\beta)$, there exists a solution ϕ such that $\phi(N) = \ker(\alpha)$.*

  (v) *For every C-embedding problem (8) and every normal closed subgroup N of Γ with $\operatorname{rank}(\Gamma/N) < \operatorname{rank}(\Gamma)$ and $N \subseteq \ker(\beta)$, there exists a solution ϕ such that $\phi(N) \neq 1$ if $\ker(\alpha)$ is finite and $\dim(\phi(N)) > 0$ if $\dim(\ker(\alpha)) > 0$.*

 (vi) *For every C-embedding problem (8) we have $\operatorname{rank}(\Gamma/N) = \operatorname{rank}(\Gamma)$ if $\ker(\alpha)$ is finite and we have $\dim(\Gamma/N) = \operatorname{rank}(\Gamma)$ if $\dim(\ker(\alpha)) > 0$, where N denotes the intersection of all kernels of all solutions to (8).*

(vii) *For every C-embedding problem (8) there exist $\operatorname{rank}(\Gamma)$ independent solutions.*

The proof of Theorem 3.24 will be given at the end of this subsection. It consists of the following implications:

In [BHHW, Theorem 3.7] we translate the conditions from Theorem 3.24 to differential embedding problems. The reader may find it instructive to look at the meaning of the above conditions in this context.

Definition 3.25. *Let C be a formation. A pro-C-group of infinite rank satisfying the equivalent characterizations of Theorem 3.24 is called* saturated.

Remark 3.26. A non-trivial pro-$\mathcal{C}$-group Γ of finite rank, i.e., a non-trivial $\mathcal{C}$-group, cannot satisfy all conditions (i)-(vii) of Theorem 3.24. For example, condition (i) (with $H = 1$) implies that for any $G \in \mathcal{C}$ and $n \geq 1$, the algebraic group G^n is an epimorphic image of Γ. Thus the rank of Γ must be infinite.

It turns out that in characteristic zero, saturated pro-$\mathcal{C}$-groups with rank not less than $|k|$ are free pro-$\mathcal{C}$-groups in disguise (Theorem 3.42). The following remark explains why we chose the expression "saturated".

Remark 3.27. Let C be a formation of finite groups. There exists a certain first order theory T such that models of T correspond to the class of profinite groups having a certain property (called the Iwasawa property in [Cha98] and [CvdM82] and the embedding property in [FJ08]). Moreover, a pro-C-group satisfies the equivalent conditions of Theorem 3.20 if and only if it corresponds to a saturated model of T. See [Cha98] and [CvdM82]. It seems conceivable that there is some first order theory T such that saturated pro-$\mathcal{C}$-groups correspond to saturated models of T. In any case, the abelian groups M, such that $D(M)$ is a saturated pro-diagonalizable group, are exactly the saturated models of a certain first order theory (namely, the theory of divisible abelian groups with infinite p-torsion for every prime p). See Example 3.40.

Remark 3.28. Let (8) be a pro-$\mathcal{C}$-embedding problem for Γ and N a normal closed subgroup of Γ with $N \subseteq \ker(\beta)$. If ϕ is a solution to (8), then $\phi(N) \subseteq \ker(\alpha)$ and $N \ker(\phi) \subseteq \ker(\beta)$. Moreover, for a solution ϕ, the following statements are equivalent:

(i) The induced map $\Gamma \to G \times_H \Gamma/N$ is an epimorphism.

(ii) $\phi(N) = \ker(\alpha)$.

(iii) $N \ker(\phi) = \ker(\beta)$.

Proof. (i)$\Rightarrow$(ii): Let R be a k-algebra and $g \in \ker(\alpha)(R) \leq G(R)$. Then

$$(g, 1) \in (G \times_H \Gamma/N)(R) = G(R) \times_{H(R)} (\Gamma/N)(R).$$

Since $\Gamma \to G \times_H \Gamma/N$ is an epimorphism, there exists a faithfully flat R-algebra S and a $\gamma \in \Gamma(S)$ such that $(\phi(\gamma), \overline{\gamma}) = (g, 1)$. But then $\gamma \in N(S)$ and $\phi(\gamma) = g$. So $\phi(N) = \ker(\alpha)$ as desired.

(ii)$\Rightarrow$(i): Let R be a k-algebra and $(g, h) \in (G \times_H \Gamma/N)(R)$. Then there exists a faithfully flat R-algebra S and $\gamma \in \Gamma(S)$ such that γ maps to h, i.e., $h = \overline{\gamma}$. We have $\alpha(g) = \beta(\gamma)$ and so $\alpha(\phi(\gamma)) = \beta(\gamma) = \alpha(g)$. Therefore $\phi(\gamma)^{-1} g \in \ker(\alpha)(S)$. As $\ker(\alpha) = \phi(N)$, there exists a faithfully flat S-algebra S' and $n \in N(S')$ with $\phi(\gamma)^{-1} g = \phi(n)$. But then γn maps to (g, h) under $\Gamma \to G \times_H \Gamma/N$.

(iii)$\Rightarrow$(ii): If $N \ker(\phi) = \ker(\beta)$, then $\phi(N) = \phi(N \ker(\phi)) = \phi(\ker(\beta)) = \ker(\alpha)$.

(ii)$\Rightarrow$(iii): If $\phi(N) = \ker(\alpha)$, then $\phi(N \ker(\phi)) = \phi(N) = \ker(\alpha)$ and also $\phi(\ker(\beta)) = \ker(\alpha)$. Since both, $N \ker(\phi)$ and $\ker(\beta)$, contain $\ker(\phi)$, this implies $N \ker(\phi) = \ker(\beta)$. $\square$

Remark 3.29. While there is a clear correspondence between (i), (ii) and (iii) of Theorem 3.20 and Theorem 3.24, the other characterizations in Theorem 3.24 (with maybe the exception of (vii)) do not look like (iv) of Theorem 3.20 on the face of it. However, it is not hard to see that (vi) of Theorem 3.24 corresponds to (iv) of Theorem 3.20 in the case when $\mathcal{C} = \mathsf{C}_k$ is a formation of finite constant algebraic groups obtained from a formation C of finite groups.

Indeed, we will show that (vi) of Theorem 3.24 holds for a C_k-embedding problem (8) if and only if it has $\mathrm{rank}(\Gamma)$ solutions:

We first note that two solutions of (8) that have the same kernel, only differ by an automorphism of G. Since there are only finitely many such automorphisms, the number of kernels of solutions equals $\mathrm{rank}(\Gamma)$ if and only if there are $\mathrm{rank}(\Gamma)$ solutions. Moreover, if N is the intersection of all solutions to (8), then the finite intersections of kernels of solutions yield a neighborhood basis at 1 for Γ/N. Now in an infinite profinite group the cardinality of a neighborhood basis at 1 consisting of normal open ($\simeq$coalgebraic) subgroups equals the cardinality of all open subgroups (since there are only finitely many

subgroups containing a given open normal subgroup). It follows that $\mathrm{rank}(\Gamma/N) = \mathrm{rank}(\Gamma)$ if and only if (8) has $\mathrm{rank}(\Gamma)$ solutions.

The following three lemmas are a preparation for the proof of (iii)$\Rightarrow$(i) in Theorem 3.24. For a finite affine scheme X over k, let us write $|X|$ for the vector space dimension $\dim_k(k[X])$ of the coordinate ring of X, i.e., the number of points of X counted with multiplicities. For clarity of exposition we separated the following lemma from the proof of Lemma 3.31.

Lemma 3.30. *Let G be an algebraic group. Then $|G/N|$ is bounded, as N varies over all normal closed subgroups of G with $\dim(N) = \dim(G)$.*

Proof. In characteristic zero $|G/G^o|$ is a bound. In positive characteristic, if $N \subseteq G$ with $\dim(N) = \dim(G)$, we can only conclude that $(G^o)_{\mathrm{red}}$ is contained in N. So $|G/N| = |G_{\overline{k}}/N_{\overline{k}}| \leq |G_{\overline{k}}/(G_{\overline{k}}^o)_{\mathrm{red}}|$. Here we passed to $\overline{k}$ to guarantee that the underlying reduced subscheme of a subgroup is a subgroup. Also note that $G_{\overline{k}}/(G_{\overline{k}}^o)_{\mathrm{red}}$ is a zero dimensional algebraic scheme and therefore is finite. $\square$

Lemma 3.31. *Let G be a proalgebraic group and $N, \widetilde{N}$ normal closed subgroups of G with $\widetilde{N} \subseteq N$ and such that $N/\widetilde{N}$ is algebraic. Then there exists a finite chain*

$$N = N_0 \geq N_1 \geq \ldots \geq N_n = \widetilde{N}$$

of normal closed subgroups of G such that N_i/N_{i+1} is an almost minimal normal subgroup of G/N_{i+1} for $i = 0, \ldots, n-1$.

Proof. Assume first that $N/\widetilde{N}$ is finite. If there is no normal closed subgroup N' of G that strictly contains $\widetilde{N}$ and is strictly contained in N, then $N/\widetilde{N}$ is an almost minimal normal subgroup of $G/\widetilde{N}$ and we can choose $n = 1$. So let us assume that such an N' exists. In this case, we may choose an N' such that $|N'/\widetilde{N}|$ is maximal (i.e., $|N/N'|$ is minimal) and call it N_1. Then N/N_1 is an almost minimal normal subgroup of G/N_1. Since $|N_1/\widetilde{N}| < |N/\widetilde{N}|$ we may conclude by induction on $|N/\widetilde{N}|$.

Let us now consider the general case. We proceed by induction on $\dim(N/\widetilde{N})$. The base case $\dim(N/\widetilde{N}) = 0$ was just handled above. So we may assume that $\dim(N/\widetilde{N}) > 0$. As above, if there is no normal closed subgroup of G that strictly contains $\widetilde{N}$ and is strictly contained in N we may choose $n = 1$. Otherwise, among all normal closed subgroups N' of G that are strictly contained in N and strictly contain $\widetilde{N}$, choose one such that $\dim(N'/\widetilde{N})$ is maximal (i.e., $\dim(N/N')$ minimal) and call it N_1. If $\dim(N/N_1) > 0$, then N/N_1 is not finite and an almost minimal normal subgroup of G/N_1, because a normal closed subgroup of G/N_1 that is strictly contained in N/N_1 must have dimension zero and is therefore a finite subgroup. As $\dim(N_1/\widetilde{N}) < \dim(N/\widetilde{N})$ we conclude by induction on $\dim(N/\widetilde{N})$.

If $\dim(N/N_1) = 0$ we proceed as follows: Since $|N/N'|$ is bounded, as N' varies over all normal closed subgroups of G with $N \supseteq N' \supseteq \widetilde{N}$ and $\dim(N/N') = 0$ (Lemma 3.30 applied to $G = N/\widetilde{N}$), we may choose one such that $|N/N'|$ is maximal. Let us call this group $\overline{N}$. Since $N/\overline{N}$ is finite, we know from the first part of this proof that there exists a sequence

$$N = N_0 \geq N_1 \geq \ldots \geq N_m = \overline{N}$$

as in the statement of the lemma. Now if N' is a normal closed subgroup of G strictly contained in $\overline{N}$ and containing $\widetilde{N}$, then $\dim(N') < \dim(\overline{N})$ since otherwise the maximality of $|N/\overline{N}|$ would be contradicted. Considering the normal closed subgroups $\overline{N} \supseteq \widetilde{N}$ of G we may conclude by induction since this case was already treated above. $\square$

It is not possible to strengthen "almost minimal" to "minimal" in the above lemma. For example, consider $G = \mathbb{G}_m = N$ and $\widetilde{N} = 1$.

Lemma 3.32. *Let G be a proalgebraic group and N a normal closed subgroup. Then there exists an ordinal number μ and a chain*

$$N = N_0 \geq N_1 \geq \ldots \geq N_\lambda \geq \ldots \geq N_\mu = 1$$

of normal closed subgroups N_λ ($\lambda \leq \mu$) of G such that

(i) *$N_{\lambda+1} = N_\lambda$ or $N_\lambda/N_{\lambda+1}$ is an almost minimal normal closed subgroup of $G/N_{\lambda+1}$ for $\lambda < \mu$,*

(ii) *$N_\lambda = \bigcap_{\lambda' < \lambda} N_{\lambda'}$ if λ is a limit ordinal and*

(iii) *if G has infinite rank and $\mathrm{rank}(G/N) < \mathrm{rank}(G)$, then $\mathrm{rank}(G/N_\lambda) < \mathrm{rank}(G)$ for $\lambda < \mu$.*

Proof. If N is algebraic, the claim follows from Lemma 3.31. So let us assume that N is not algebraic. Let $\mathcal{N}$ denote a neighborhood basis at 1 of G with $|\mathcal{N}| = \mathrm{rank}(G)$. According to Corollary 2.8 the set $\mathcal{N}(N) = \{N \cap N' |\ N' \in \mathcal{N}\}$ is a neighborhood basis at 1 for N. Let μ be the smallest ordinal number such that $|\mu| = |\mathcal{N}(N)|$. So we may write $\mathcal{N}(N) = \{U_\lambda |\ \lambda < \mu\}$. We set $N_0 = N$ and for $1 \leq \lambda \leq \mu$ we set $N_\lambda = \bigcap_{\lambda' < \lambda} U_\lambda$. Clearly the N_λ's form a descending chain of normal closed subgroups of G such that $N_0 = N$ and $N_\mu = 1$. Moreover $N_\lambda/N_{\lambda+1} = N_\lambda/(N_\lambda \cap U_{\lambda+1}) = U_{\lambda+1}N_\lambda/U_{\lambda+1}$ is algebraic, because $U_{\lambda+1}N_\lambda/U_{\lambda+1}$ embeds into $N/U_{\lambda+1}$. If $N_\lambda/N_{\lambda+1}$ is not an almost minimal normal closed subgroup of $G/N_{\lambda+1}$, we can use Lemma 3.31 to insert finitely many subgroups between N_λ and $N_{\lambda+1}$ to achieve (i). On the other hand, (ii) is satisfied by construction.

If G is algebraic statement (iii) is void. So let us assume that G is not algebraic, i.e., $\mathrm{rank}(G)$ is infinite. By Proposition 3.8 (applied to G/N) there exists a chain

$$G = M_0 \geq M_1 \geq \ldots \geq M_\xi \geq \ldots \geq M_\nu = N$$

of normal closed subgroups M_ξ of G such that

(i) *$M_\xi/M_{\xi+1}$ algebraic for all $\xi < \nu$,*

(ii) *$N_\xi = \bigcap_{\xi' < \xi} N_{\xi'}$ if ξ is a limit ordinal*

and $|\nu| = \mathrm{rank}(G/N)$. Assume $\mathrm{rank}(G/N) < \mathrm{rank}(G)$ and fix $\lambda < \mu$. Proposition 3.8 applied to the chain

$$M_0 \geq M_1 \geq \ldots \geq M_\nu = N = N_0 \geq N_1 \geq \ldots \geq N_\lambda$$

shows that $\mathrm{rank}(G/N_\lambda) \leq |\nu + \lambda| = |\nu| + |\lambda|$. But $|\nu| = \mathrm{rank}(G/N) < \mathrm{rank}(G)$ and $|\lambda| < |\mu| = \mathrm{rank}(G)$ by choice of μ. $\qquad\square$

We are now prepared to prove the implication (iii)$\Rightarrow$(i) in Theorem 3.24.

Proposition 3.33. *Let $\mathcal{C}$ be a formation and Γ a pro-$\mathcal{C}$-group of infinite rank. We consider pro-$\mathcal{C}$-embedding problems*

(9)

$$
\begin{array}{ccc}
 & & \Gamma \\
 & \swarrow & \downarrow \\
G & \longrightarrow & H
\end{array}
$$

for Γ. If every pro-$\mathcal{C}$-embedding problem with $\mathrm{rank}(H) < \mathrm{rank}(\Gamma)$ and almost minimal algebraic kernel has a solution, then every pro-$\mathcal{C}$-embedding problem with $\mathrm{rank}(H) < \mathrm{rank}(\Gamma)$ and $\mathrm{rank}(G) \leq \mathrm{rank}(\Gamma)$ has a solution.

Proof. Assume that an embedding problem (9) with $\mathrm{rank}(H) < \mathrm{rank}(\Gamma)$ and $\mathrm{rank}(G) \leq \mathrm{rank}(\Gamma)$ is given. Let N be the kernel of this embedding problem. According to Lemma 3.32 there exists an ordinal number μ and a chain

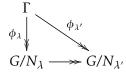$$N = N_0 \geq N_1 \geq \ldots \geq N_\lambda \geq \ldots \geq N_\mu = 1$$

of normal closed subgroups N_λ ($\lambda \leq \mu$) of G such that

(i) *$N_{\lambda+1} = N_\lambda$ or $N_\lambda/N_{\lambda+1}$ is an almost minimal normal closed subgroup of $G/N_{\lambda+1}$ for $\lambda < \mu$ and*

(ii) *$N_\lambda = \bigcap_{\lambda' < \lambda} N_{\lambda'}$ if λ is a limit ordinal and*

(iii) if G has infinite rank and $\operatorname{rank}(H) < \operatorname{rank}(G)$, then $\operatorname{rank}(G/N_\lambda) < \operatorname{rank}(G)$ for $\lambda < \mu$.

We will show by (transfinite) induction that for each $\lambda \leq \mu$ there exists an epimorphism $\phi_\lambda\colon \Gamma \twoheadrightarrow G/N_\lambda$ such that the diagram

$$
\begin{array}{ccc}
 & \Gamma & \\
{\scriptstyle \phi_\lambda}\downarrow & & \searrow{\scriptstyle \phi_{\lambda'}} \\
G/N_\lambda & \longrightarrow\!\!\!\!\rightarrow & G/N_{\lambda'}
\end{array}
$$

commutes for $\lambda' \leq \lambda$. We let $\phi_0\colon \Gamma \twoheadrightarrow G/N_0 = H$ be the epimorphism of the given embedding problem. Assume now that $\phi_{\lambda'}$ has been constructed for each $\lambda' < \lambda$. We have to distinguish two cases: If λ is a limit ordinal, then $N_\lambda = \bigcap_{\lambda'<\lambda} N_{\lambda'}$. So $G/N_\lambda = \varprojlim_{\lambda'} G/N_{\lambda'}$ and we set $\phi_\lambda = \varprojlim_{\lambda'} \phi_{\lambda'}$.

If λ is a successor ordinal, say $\lambda = \nu + 1$, we would like to define ϕ_λ as a solution to the embedding problem

(10)
$$
\begin{array}{ccc}
 & \Gamma & \\
{\scriptstyle}\vdots & & \searrow{\scriptstyle \phi_\nu} \\
\downarrow & & \\
G/N_\lambda & \longrightarrow\!\!\!\!\rightarrow & G/N_\nu
\end{array}
\qquad .
$$

If $N_\lambda = N_\nu$, we may choose $\phi_\lambda = \phi_\nu$. Otherwise, (10) has an almost minimal algebraic kernel $N_\nu/N_{\nu+1}$. So to establish the existence of ϕ_λ, it suffices to verify that $\operatorname{rank}(G/N_\nu) < \operatorname{rank}(\Gamma)$. If $\operatorname{rank}(G)$ is finite, this follows from the assumption that $\operatorname{rank}(\Gamma)$ is infinite. So we may assume that $\operatorname{rank}(G)$ is infinite. If $\operatorname{rank}(H) = \operatorname{rank}(G)$, then $\operatorname{rank}(G/N_\nu) \leq \operatorname{rank}(G) = \operatorname{rank}(H) < \operatorname{rank}(\Gamma)$. If $\operatorname{rank}(H) < \operatorname{rank}(G)$, then $\operatorname{rank}(G/N_\nu) < \operatorname{rank}(G) \leq \operatorname{rank}(\Gamma)$ by (iii). By construction, the epimorphism $\phi_\mu\colon \Gamma \twoheadrightarrow G$ is a solution to (9). $\qquad\square$

We now work towards a proof of (v)$\Rightarrow$(iii) in Theorem 3.24.

Lemma 3.34. *Let $\alpha\colon G \twoheadrightarrow H$ be an epimorphism of proalgebraic groups such that $\ker(\alpha)$ is algebraic. Then there exist algebraic groups H' and H'' and epimorphisms $H \twoheadrightarrow H''$, $H' \twoheadrightarrow H''$ such that $G \simeq H' \times_{H''} H$ and α can be identified with the projection onto the second factor. Moreover, if $\ker(\alpha)$ is an almost minimal normal subgroup of G, then the kernel of $H' \to H''$ is an almost minimal normal subgroup of H'.*

Proof. If N_1, N_2 are normal closed subgroups of a proalgebraic group G, it follows from the universal properties that $G/N_1 \times_{G/N_1N_2} G/N_2 \simeq G/(N_1 \cap N_2)$. In particular, $G/N_1 \times_{G/N_1N_2} G/N_2 \simeq G$ if $N_1 \cap N_2 = 1$.

According to Corollary 2.9, there exists a coalgebraic subgroup N of G with $N \cap \ker(\alpha) = 1$. So $G \simeq G/N \times_{G/N\ker(\alpha)} G/\ker(\alpha) = H' \times_{H''} H$.

Note that $\ker(\alpha)$ is isomorphic to $\ker(H' \to H'')$. If N' is a normal closed subgroup of H' contained in $\ker(H' \to H'')$. Then $N' \simeq N' \times_{H''} 1$ corresponds to a normal closed subgroup of G contained in $\ker(\alpha)$. $\qquad\square$

The following proposition proves (v)$\Rightarrow$(iii) of Theorem 3.24.

Proposition 3.35. *Let $\mathcal{C}$ be a formation and Γ a pro-$\mathcal{C}$-group of infinite rank. We consider non-trivial pro-$\mathcal{C}$-embedding problems*

(11)
$$
\begin{array}{ccc}
 & \Gamma & \\
{\scriptstyle}\vdots & & \searrow{\scriptstyle \beta} \\
\downarrow & & \\
G & \xrightarrow{\;\alpha\;}\!\!\!\!\rightarrow & H
\end{array}
$$

for Γ. Assume that for every $\mathcal{C}$-embedding problem (11) and every normal closed subgroup N of Γ with $N \subseteq \ker(\beta)$ and $\operatorname{rank}(\Gamma/N) < \operatorname{rank}(\Gamma)$, there exists a solution ϕ such that $\phi(N) \neq 1$ if $\ker(\alpha)$ is finite and $\dim(\phi(N)) > 0$

if $\dim(\ker(\alpha)) > 0$. *Then every pro-$\mathcal{C}$-embedding problem (11) with* $\mathrm{rank}(H) < \mathrm{rank}(\Gamma)$ *and almost minimal kernel has a solution.*

Proof. Assume that a pro-$\mathcal{C}$-embedding problem (11) with $\mathrm{rank}(H) < \mathrm{rank}(\Gamma)$ and almost minimal kernel is given. According to Lemma 3.34, the epimorphism $G \twoheadrightarrow H$ can be written as $H' \times_{H''} H \to H$, where $H' \twoheadrightarrow H''$ is an epimorphism of algebraic groups with almost minimal kernel and $H \twoheadrightarrow H''$. Let N be the kernel of $\beta \colon \Gamma \twoheadrightarrow H$. Then $\mathrm{rank}(\Gamma/N) = \mathrm{rank}(H) < \mathrm{rank}(\Gamma)$. Since N lies in the kernel of $\Gamma \to H''$, it follows from the assumption, that the $\mathcal{C}$-embedding problem

(12)
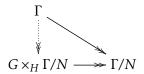$$\begin{array}{ccc} & & \Gamma \\ & \swarrow & \downarrow \\ H' & \longrightarrow & H'' \end{array}$$

has a solution $\phi \colon \Gamma \twoheadrightarrow H'$ such that

- if $\ker(H' \to H'')$ is finite, then $\phi(N) \neq 1$ and

- if $\dim(\ker(H' \to H'')) > 0$, then $\dim(\phi(N)) > 0$.

Clearly, the induced map $\psi = (\phi, \beta) \colon \Gamma \to H' \times_{H''} H$ is a weak solution of the given embedding problem (11). We will show that ψ actually is a solution, i.e., an epimorphism. Since N lies in the kernel of $\Gamma \to H''$ and ϕ is a solution of (12) we have $\phi(N) \subseteq \ker(H' \to H'')$. As $\phi \colon \Gamma \to H'$ is an epimorphism, $\phi(N)$ is a normal closed subgroup of H'. Since $\ker(H' \to H'')$ is almost minimal, we see that $\phi(N) = \ker(H' \to H'')$. It thus follows from Remark 3.28 that $\psi \colon \Gamma \to H' \times_{H''} H = G$ is an epimorphism. So ψ is the desired solution of (11). $\qquad\square$

Finally, we can put all pieces together for the proof of Theorem 3.24:

Proof of Theorem 3.24: Clearly, (i)$\Rightarrow$(ii)$\Rightarrow$(iii). By Proposition 3.33 (iii)$\Rightarrow$(i). So (i), (ii) and (iii) are equivalent.

Let us show (ii)$\Rightarrow$(iv): So let (8) be a $\mathcal{C}$-embedding problem and N a normal closed subgroup of Γ with $N \subseteq \ker(\beta)$ and $\mathrm{rank}(\Gamma/N) < \mathrm{rank}(\Gamma)$. By assumption, the embedding problem

$$\begin{array}{ccc} & & \Gamma \\ & \swarrow & \downarrow \\ G \times_H \Gamma/N & \longrightarrow & \Gamma/N \end{array}$$

has a solution $\phi' \colon \Gamma \twoheadrightarrow G \times_H \Gamma/N$. Let $\phi = \pi_G \circ \phi'$, where $\pi_G \colon G \times_H \Gamma/N \to G$ denotes the projection onto the first factor. Then ϕ is a solution to (8). According to Remark 3.28 we have $\phi(N) = \ker(\alpha)$.

Now (iv)$\Rightarrow$(v) is obvious and (v)$\Rightarrow$(iii) by Proposition 3.35. So we already know that the first five conditions of Theorem 3.24 are equivalent.

Let us show (vi)$\Rightarrow$(v): So we assume that a $\mathcal{C}$-embedding problem (8) is given, together with a normal closed subgroup of N of Γ with $N \subseteq \ker(\beta)$ and $\mathrm{rank}(\Gamma/N) < \mathrm{rank}(\Gamma)$. Let $N_{\alpha,\beta}$ denote the intersection of all kernels of all solutions to (8).

Let us first assume that $\ker(\alpha)$ is finite. By assumption we have $\mathrm{rank}(\Gamma/N_{\alpha,\beta}) = \mathrm{rank}(\Gamma)$. On the other hand, $\mathrm{rank}(\Gamma/N_{\alpha,\beta}N) \leq \mathrm{rank}(\Gamma/N) < \mathrm{rank}(\Gamma)$. This shows that the kernel $N_{\alpha,\beta}N/N_{\alpha,\beta} = N/(N \cap N_{\alpha,\beta})$ of the epimorphism $\Gamma/N_{\alpha,\beta} \twoheadrightarrow \Gamma/N_{\alpha,\beta}N$ must be non-trivial. In other words, N is not contained in $N_{\alpha,\beta}$. Thus there exists a solution ϕ of (8) such that N is not contained in $\ker(\phi)$, i.e., $\phi(N) \neq 1$ as desired.

Let us now assume that $\dim(\ker(\alpha)) > 0$. By assumption, $\dim(\Gamma/N_{\alpha,\beta}) = \mathrm{rank}(\Gamma)$. On the other hand, $\dim(\Gamma/N_{\alpha,\beta}N) \leq \dim(\Gamma/N) \leq \mathrm{rank}(\Gamma/N) < \mathrm{rank}(\Gamma)$, using Lemmas 3.14 and 3.16. Applying Lemma 3.15 to the epimorphism $\Gamma/N_{\alpha,\beta} \twoheadrightarrow \Gamma/N_{\alpha,\beta}N$ shows that its kernel $N_{\alpha,\beta}N/N_{\alpha,\beta} = N/(N \cap N_{\alpha,\beta})$ has positive dimension. Using Lemma 3.17 we see that $N/(N \cap \ker(\phi))$ has positive dimension for some solution ϕ of (8). Thus $\phi(N) \simeq N/(N \cap \ker(\phi))$ has positive dimension as desired.

We next show that (i)⇒(vii): So we assume that a $\mathcal{C}$-embedding problem (8) is given. Let I be a set of cardinality $\mathrm{rank}(\Gamma)$ and set $G' = \prod_I (G \twoheadrightarrow H)$. Then $\mathrm{rank}(G') \leq \mathrm{rank}(\Gamma)$. By assumption the embedding problem

$$
\begin{array}{ccc}
 & & \Gamma \\
 & \swarrow\!\!\!\!\!\!\!\!\!\downarrow & \downarrow \\
G' & \longrightarrow\!\!\!\!\!\!\!\!\rightarrow & H
\end{array}
$$

has a solution $\phi\colon \Gamma \twoheadrightarrow G'$. For every $i \in I$ we can compose ϕ with the projection $\pi_i\colon G' \to G$ that picks out the i-th component, to obtain a solution $\phi_i\colon \Gamma \twoheadrightarrow G$ of (8). By construction these solutions are independent.

Finally, we show (vii)⇒(vi): So we assume that a $\mathcal{C}$-embedding problem (8) is given together with independent solutions $(\phi_i)_{i\in I}$, where $|I| = \mathrm{rank}(\Gamma)$. The intersection N of all kernels of all solution to (8) is contained in $\bigcap_{i\in I} \ker(\phi_i)$. So the isomorphism $\Gamma/\bigcap_{i\in I}\ker(\phi_i) \to \prod_{i\in I}(G \twoheadrightarrow H)$ yields an epimorphism $\Gamma/N \twoheadrightarrow \prod_{i\in I}(G \twoheadrightarrow H)$. By Lemma 3.5 we have
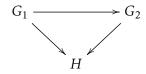
$$
\mathrm{rank}(\Gamma/N) \geq \mathrm{rank}(\prod_{i\in I}(G \twoheadrightarrow H)) \geq \mathrm{rank}(\prod_{i\in I}\ker(\alpha)) = |I| = \mathrm{rank}(\Gamma).
$$

Moreover, if $\dim(\ker(\alpha)) > 0$ we have $\dim(\Gamma/N) \geq \dim(\prod_{i\in I}(G \twoheadrightarrow H)) \geq |I| = \mathrm{rank}(\Gamma)$ by Lemmas 3.14 and 3.18. But then necessarily $\dim(\Gamma/N) = \mathrm{rank}(\Gamma)$, because $\dim(\Gamma/N) \leq \dim(\Gamma) \leq \mathrm{rank}(\Gamma)$ (Lemmas 3.14 and 3.16). □

3.4. Existence of saturated pro-$\mathcal{C}$-groups

We next discuss the question, for which infinite cardinals κ there exists a saturated pro-$\mathcal{C}$-group of rank κ. We will show that the answer is always positive for $\kappa \geq |\bar{k}|$.

We will need some preparatory results. Two epimorphisms $G_1 \twoheadrightarrow H$, $G_2 \twoheadrightarrow H$ of proalgebraic groups are said to be *isomorphic* if there exists an isomorphism $G_1 \to G_2$ such that

$$
\begin{array}{ccc}
G_1 & \longrightarrow & G_2 \\
 & \searrow \quad \swarrow & \\
 & H &
\end{array}
$$

commutes. This definition also applies for $G_1 = G_2$.

For a formation $\mathcal{C}$ we denote by $|\mathcal{C}|$ the cardinality of the set of all isomorphism classes of $\mathcal{C}$-groups.

Lemma 3.36. *Let κ be an infinite cardinal and let $\mathcal{C}$ be a formation such that*

(i) *$|\mathcal{C}| \leq \kappa$,*

(ii) *every $\mathcal{C}$-group has at most κ normal closed subgroups and*

(iii) *there are, up to isomorphism, at most κ distinct epimorphisms between any two $\mathcal{C}$-groups.*

Let H be a pro-$\mathcal{C}$-group with $\mathrm{rank}(H) \leq \kappa$. Then the set of isomorphism classes of epimorphisms $G \twoheadrightarrow H$ of pro-$\mathcal{C}$-groups with algebraic kernel, has cardinality less or equal to κ.

Proof. We start by showing that H has at most κ coalgebraic subgroups. Let $\mathcal{M}$ denote the set of coalgebraic subgroups of H and let $\mathcal{N}$ be a neighborhood basis at 1 for H with $|\mathcal{N}| \leq \kappa$. For every $M \in \mathcal{M}$ there exists an $N \in \mathcal{N}$ with $N \subseteq M$. On the other hand, for a fixed N, there are at most κ many $M \in \mathcal{M}$ with $N \subseteq M$ by (ii). Thus

$$
|\mathcal{M}| = \left| \bigcup_{N\in\mathcal{N}} \{M \in \mathcal{M} |\ N \subseteq M\} \right| \leq |\mathcal{N}| \cdot \kappa \leq \kappa.
$$

For a fixed coalgebraic subgroup N of H, there are at most κ epimorphisms $H' \twoheadrightarrow H/N = H''$ (up to isomorphism) of $\mathcal{C}$-groups by (i) and (iii).

Such an epimorphism $H' \twoheadrightarrow H''$ gives rise to an epimorphism $H' \times_{H''} H \twoheadrightarrow H$ of pro-$\mathcal{C}$-groups with algebraic kernel. Moreover, by Lemma 3.34, every epimorphism $G \twoheadrightarrow H$ of pro-$\mathcal{C}$-groups with algebraic kernel is of this form. Thus there are, up to isomorphism, at most $\kappa \cdot \kappa = \kappa$ epimorphisms $G \twoheadrightarrow H$ of pro-$\mathcal{C}$-groups with algebraic kernel. $\qquad\square$

Theorem 3.37. *Let κ be an infinite cardinal. If $\mathcal{C}$ is a formation such that*

  (i) *$|\mathcal{C}| \leq \kappa$,*

  (ii) *every $\mathcal{C}$-group has at most κ normal closed subgroups and*

  (iii) *there are, up to isomorphism, at most κ distinct epimorphisms between any two $\mathcal{C}$-groups,*

then there exists a saturated pro-$\mathcal{C}$-group of rank κ. In particular, if $\kappa \geq |\bar{k}|$, there exists a saturated pro-$\mathcal{C}$-group of rank κ for any formation $\mathcal{C}$.

Proof. Let $\Gamma_0 = \prod_i G_i$ be a product of $\mathcal{C}$-groups such that every $\mathcal{C}$-isomorphism class occurs exactly κ many times in this product. By (i) and Example 3.3 we have $\mathrm{rank}(\Gamma_0) = \kappa$. According to Lemma 3.36 there are at most κ isomorphism classes of epimorphisms $G \twoheadrightarrow \Gamma_0$ of pro-$\mathcal{C}$-groups with algebraic kernel. Let $\Gamma_1 = \prod_i (G_i \twoheadrightarrow \Gamma_0)$ be a fibred product of epimorphisms of pro-$\mathcal{C}$-groups with algebraic kernel, where every isomorphism class of such epimorphisms occurs exactly κ times. By Lemma 3.36 this fibred product is formed over an index set of cardinality κ. According to Example 3.3 we have $\mathrm{rank}(\Gamma_1) \leq \kappa$. Since Γ_0 is a quotient of Γ_1 we actually have $\mathrm{rank}(\Gamma_1) = \kappa$. We now keep iterating this construction. So Γ_2 would be a fibred product of epimorphisms $G_i \twoheadrightarrow \Gamma_1$ and so on. Let $\Gamma = \varprojlim_{i \in \mathbb{N}} \Gamma_i$ be the projective limit of the Γ_i's. Then Γ is a pro-$\mathcal{C}$-group of rank κ.

We will show that Γ is saturated. To do this we will use condition (vii) of Theorem 3.24. So let

(13)
$$
\begin{array}{ccc}
\Gamma & & \\
\vdots & \searrow^{\beta} & \\
\downarrow & & \\
G & \xrightarrow{\alpha} & H
\end{array}
$$

be a non-trivial $\mathcal{C}$-embedding problem. Since H is algebraic, there exists an $i \in \mathbb{N}$ such that H is a quotient of Γ_i (i.e., $k[H]$ is contained in $k[\Gamma_i] \subseteq k[\Gamma]$). Then $G \times_H \Gamma_i \twoheadrightarrow \Gamma_i$ is an epimorphism of pro-$\mathcal{C}$-groups with algebraic kernel. By construction of Γ, there is an epimorphism $\Gamma \twoheadrightarrow \prod_J (G \times_H \Gamma_i \twoheadrightarrow \Gamma_i)$, where the product is taken over an index set J of cardinality κ. For $j \in J$ let $\phi_j \colon \Gamma \twoheadrightarrow G$ be the composition

$$
\Gamma \twoheadrightarrow \prod_J (G \times_H \Gamma_i \twoheadrightarrow \Gamma_i) \twoheadrightarrow G \times_H \Gamma_i \twoheadrightarrow G,
$$

where the map in the middle is the projection onto the j-th factor. Then ϕ_j is a solution to (13) for every $j \in J$. In fact, since

$$
\prod_J (G \times_H \Gamma_i \twoheadrightarrow \Gamma_i) = \left(\prod_J (G \twoheadrightarrow H) \right) \times_H \Gamma_i,
$$

the family $(\phi_j)_{j \in J}$ of solutions is independent.

Finally, a counting argument shows that

  (i) Up to isomorphism there are at most $|\bar{k}|$ algebraic groups.

  (ii) An algebraic group has at most $|\bar{k}|$ normal closed subgroups.

  (iii) There are at most $|\bar{k}|$ epimorphisms between any two algebraic groups.

Thus conditions (i), (ii) and (iii) are satisfied for any $\mathcal{C}$ if $\kappa \geq |\bar{k}|$. $\qquad\square$

We note that the conditions of Theorem 3.37 are satisfied for any infinite κ if $\mathcal{C} = \mathsf{C}_k$ is a formation of algebraic groups coming from a formation C of finite groups. The conditions are also met for any infinite κ for the class $\mathcal{C}$ of all diagonalizable algebraic groups.

3.5. Uniqueness of saturated pro-$\mathcal{C}$-groups

The uniqueness of saturated pro-$\mathcal{C}$-groups of a fixed rank follows by a rather standard back and forth argument.

Theorem 3.38. *Let $\mathcal{C}$ be a formation and let Γ and Γ' be saturated pro-$\mathcal{C}$-groups with $\mathrm{rank}(\Gamma) = \mathrm{rank}(\Gamma')$. Then Γ and Γ' are isomorphic.*

Proof. Let $\kappa = \mathrm{rank}(\Gamma) = \mathrm{rank}(\Gamma)$. We choose $\mathcal{N}$ and $\mathcal{N}'$, neighborhood bases at 1 of cardinality κ for Γ and Γ' respectively and we well-order them: $\mathcal{N} = \{N_\mu | \ \mu < \kappa\}$, $\mathcal{N}' = \{N'_\mu | \ \mu < \kappa\}$ with $N_0 = \Gamma$ and $N'_0 = \Gamma'$.

We will use transfinite induction to construct descending chains of closed normal subgroups $\{M_\mu | \ \mu < \kappa\}$ and $\{M'_\mu | \ \mu < \kappa\}$ of Γ and Γ' respectively, and isomorphisms $\phi_\mu \colon \Gamma/M_\mu \to \Gamma'/M'_\mu$ such that the following properties are satisfied for every $\mu < \kappa$:

(i) The diagram

$$
\begin{array}{ccc}
\Gamma/M_\mu & \xrightarrow{\ \phi_\mu\ } & \Gamma'/M'_\mu \\
\downarrow & & \downarrow \\
\Gamma/M_\lambda & \xrightarrow{\ \phi_\lambda\ } & \Gamma'/M'_\lambda
\end{array}
$$

commutes for $\lambda < \mu$.

(ii) $\mathrm{rank}(\Gamma/M_\mu) \le \mu$.

(iii) $M_\lambda \le N_\mu$ and $M'_\lambda \le N'_\mu$ for $\lambda < \mu$.

For $\mu = 0$, we set $M_0 = N_0 = \Gamma$ and $M'_0 = N'_0 = \Gamma'$. We also let $\phi_0 \colon \Gamma/M_0 = 1 \to \Gamma'/M'_0$ be the trivial map.

Now fix a $\mu < \kappa$ and assume that M_λ, M'_λ and θ_λ have been constructed for all $\lambda < \mu$ such that (i), (ii) and (iii) holds for $\lambda < \mu$. We have to consider two cases:

Case 1: $\mu = \lambda + 1$ is a successor ordinal: Set $P_\mu = N_\lambda \cap M_\lambda$. The kernel of $\Gamma/P_\mu \to \Gamma/M_\lambda$ is $M_\lambda/(N_\lambda \cap M_\lambda) \simeq M_\lambda N_\lambda/N_\lambda \hookrightarrow \Gamma/N_\lambda$. Because Γ/N_λ is algebraic, also the kernel of $\Gamma/P_\mu \to \Gamma/M_\lambda$ is algebraic. Since Γ' is saturated, the pro-$\mathcal{C}$-embedding problem $\Gamma/P_\mu \to \Gamma/M_\lambda$, $\Gamma' \to \Gamma'/M'_\lambda \xrightarrow{\phi_\lambda^{-1}} \Gamma/M_\lambda$ has a solution, i.e., we can find an epimorphism $\phi' \colon \Gamma' \twoheadrightarrow \Gamma/P_\mu$ such that

$$
\begin{array}{c}
\Gamma' \\
{\scriptstyle \phi'}\downarrow \ \ \searrow \\
\Gamma/P_\mu \longrightarrow\!\!\!\!\rightarrow \Gamma/M_\lambda
\end{array}
$$

commutes. For $P'_\mu = \ker(\phi')$, this induces an isomorphism $\overline{\phi'} \colon \Gamma'/P'_\mu \to \Gamma/P_\mu$ such that

$$
\begin{array}{ccc}
\Gamma/P_\mu & \xleftarrow{\ \overline{\phi'}\ } & \Gamma'/P'_\mu \\
\downarrow & & \downarrow \\
\Gamma/M_\lambda & \xleftarrow{\ \phi_\lambda^{-1}\ } & \Gamma'/M'_\lambda
\end{array}
$$

commutes. Set $M'_\mu = P'_\mu \cap N'_\lambda \le M'_\lambda$. As noted above, the kernel of $\Gamma/P_\mu \to \Gamma/M_\lambda$ is algebraic. Therefore, by Lemma 3.6, $\mathrm{rank}(\Gamma/P_\mu) = \mathrm{rank}(\Gamma/M_\lambda) \le \lambda$. If λ is finite, $\mathrm{rank}(\Gamma/P_\mu) \le 1 \le \mu$. If λ is infinite, $|\lambda| = |\mu|$ (because $\mu = \lambda + 1$). So in either case, $\mathrm{rank}(\Gamma/P_\mu) \le \mu$. We consider the pro-$\mathcal{C}$-embedding problem

$$
\Gamma'/M'_\mu \twoheadrightarrow \Gamma'/P'_\mu, \ \Gamma \to \Gamma/P_\mu \xrightarrow{\overline{\phi'}^{-1}} \Gamma'/P'_\mu
$$

for Γ. We have $\operatorname{rank}(\Gamma'/P'_\mu) = \operatorname{rank}(\Gamma/P_\mu) \leq \mu < \operatorname{rank}(\Gamma)$. As Γ is saturated, we can find a solution $\phi\colon \Gamma \twoheadrightarrow \Gamma'/M'_\mu$ to the above embedding problem. Set $M_\mu = \ker(\phi) \leq P_\mu = N_\lambda \cap M_\lambda$. Then we have a commutative diagram

$$
\begin{array}{ccc}
\Gamma/M_\mu & \xrightarrow{\ \phi_\mu\ } & \Gamma'/M'_\mu \\
\downarrow & & \downarrow \\
\Gamma/P_\mu & \xrightarrow{\ \overline{\phi'}^{-1}\ } & \Gamma'/P'_\mu
\end{array}
$$

where $\phi_\mu = \overline{\phi}$ is induced from ϕ. Stacking the above two diagrams on top of each other, we find that

$$
\begin{array}{ccc}
\Gamma/M_\mu & \xrightarrow{\ \phi_\mu\ } & \Gamma'/M'_\mu \\
\downarrow & & \downarrow \\
\Gamma/M_\lambda & \xrightarrow{\ \phi_\lambda\ } & \Gamma'/M'_\lambda
\end{array}
$$

commutes. As the kernel of $\Gamma'/M'_\mu \twoheadrightarrow \Gamma'/P'_\mu$ is algebraic, it follows from Lemma 3.6 that

$$\operatorname{rank}(\Gamma/M_\mu) = \operatorname{rank}(\Gamma'/M'_\mu) = \operatorname{rank}(\Gamma'/P'_\mu) \leq \mu.$$

So conditions (i), (ii) and (iii) are satisfied for μ.

Case 2: μ is a limit ordinal: Set $M_\mu = \bigcap_{\lambda < \mu} M_\lambda$ and $M'_\mu = \bigcap_{\lambda < \mu} M'_\lambda$. Then the ϕ_λ for $\lambda < \mu$ induce an isomorphism $\phi_\mu\colon \Gamma/M_\mu \to \Gamma'/M'_\mu$. Clearly, conditions (i) and (iii) are satisfied.

For $\lambda < \mu$ we have $\operatorname{rank}(\Gamma/M_\lambda) \leq |\lambda| \leq |\mu|$. Therefore condition (ii) is satisfied by Lemma 3.7. This concludes the construction of the M_μ, M'_μ and the isomorphisms ϕ_μ for $\mu < \kappa = \operatorname{rank}(\Gamma)$.

It follows from condition (iii) that $\bigcap_{\mu < \kappa} M_\mu = 1$ and $\bigcap_{\mu < \kappa} M'_\mu = 1$. Therefore the ϕ_μ for $\mu < \kappa$ induce an isomorphism $\Gamma \to \Gamma'$. $\qquad\square$

We continue with two examples of saturated pro-$\mathcal{C}$-groups.

Example 3.39. Let k be a field of characteristic zero and $\mathcal{C}$ the formation of all abelian unipotent algebraic groups. (Cf. Example 2.24.) We claim that for any infinite cardinal κ, the proalgebraic group $\prod_\kappa \mathbb{G}_a$ is the saturated pro-$\mathcal{C}$-group of rank κ.

Proof. It suffices to show that $\prod_\kappa \mathbb{G}_a$ is saturated. Maybe the clearest way to see this it to observe that the functor $V \rightsquigarrow G(V)$ with $G(V)(R) = \operatorname{Hom}_k(V, R)$ for any k-algebra R, is a (contravariant) equivalence of categories from the category of k-vector spaces to the category of pro-$\mathcal{C}$-groups. We note that $G(V)$ is represented by the symmetric algebra on V and that an epimorphism $G(V) \twoheadrightarrow G(W)$ of pro-$\mathcal{C}$-groups corresponds to an injection $W \hookrightarrow V$ of k-vector spaces. Moreover, for an infinite dimensional k-vector space V, we have $\operatorname{rank}(G(V)) = \dim_k(V)$. Thus the claim reduces to the following obvious statement: If V is a vector space of dimension κ, V_1 a subspace of V with $\dim_k(V_1) < \kappa$ and $V_1 \hookrightarrow V_2$ an embedding of vector spaces with $\dim_k(V_2) \leq \kappa$, then V_2 can be embedded into V over V_1. $\qquad\square$

We next determine the saturated pro-diagonalizable groups.

Example 3.40. Let $\mathcal{C}$ be the formation of all diagonalizable algebraic groups and let κ be an infinite cardinal. According to Theorems 3.37 and 3.38 there exist a unique saturated pro-$\mathcal{C}$-group Γ of rank κ. This group Γ is of the form $\Gamma = D(M)$ for some abelian group M. We would like to determine M. According to Theorem 3.24 and Theorem 3.38 the group M is uniquely characterized by the following properties:

(i) $|M| = \kappa$ and

(ii) for every subgroup M_1 of M with $|M_1| < |M|$ and embedding of abelian groups $M_1 \hookrightarrow M_2$ with $|M_2| \leq |M|$, there exists an embedding of M_2 over M_1 into M.

To be precise, if $\kappa = \aleph_0$, the statement $|M_1| < |M|$ in (ii) should be replaced by M_1 is finitely generated. This unique abelian group is $M = \bigoplus_\kappa \mathbb{Q} \oplus \bigoplus_\kappa \mathbb{Q}/\mathbb{Z}$.

Proof. Let us first show that M is divisible: Let $a \in M$ and $n \geq 1$, we have to show that there exists $b \in M$ with $nb = a$. Let $M_1 = \langle a \rangle$ denote the cyclic subgroup of M generated by a. Then M_1 is contained in a cyclic abelian group M_2 such that $nM_2 = M_1$. (If a has infinite order consider the inclusion $\mathbb{Z}n \subseteq \mathbb{Z}$ and if a has finite order m, consider the inclusion image $\mathbb{Z}n/\mathbb{Z}mn \subseteq \mathbb{Z}/\mathbb{Z}mn$.) Since M_2 embeds into M over M_1 it follows that M is divisible.

Any divisible group is of the form $\bigoplus_{\kappa_0} \mathbb{Q} \bigoplus_{p \in \mathbb{P}} \oplus_{\kappa_p} \mathbb{Z}(p^\infty)$, where $\mathbb{P}$ denotes the set of all prime numbers and $\mathbb{Z}(p^\infty)$ the p-Prüfer group. (See e.g., [Kap54, Theorem 4].) The cardinal numbers κ_0 and κ_p are uniquely determined. The groups $\bigoplus_\kappa \mathbb{Q}$ and $\bigoplus_\kappa \mathbb{Z}(p^\infty)$ have cardinality κ and so embed into M by (ii). It follows that $M = \bigoplus_\kappa \mathbb{Q} \bigoplus_{p \in \mathbb{P}} \oplus_\kappa \mathbb{Z}(p^\infty)$. As $\bigoplus_{p \in \mathbb{P}} \mathbb{Z}(p^\infty) = \mathbb{Q}/\mathbb{Z}$ the claim follows. $\quad\square$

3.6. Free pro-$\mathcal{C}$-groups and saturation

Having discussed free pro-$\mathcal{C}$-groups and saturated pro-$\mathcal{C}$-groups, we now address the question under which circumstances these notions coincide. Given the uniqueness of saturated pro-$\mathcal{C}$-groups of a fixed rank (Theorem 3.38) the question boils down to, whether or not a free pro-$\mathcal{C}$-group is saturated.

Proposition 3.41. *Let $\mathcal{C}$ be a formation and let X be an infinite set. Let*

(14)
$$
\begin{array}{ccc}
\Gamma^{\mathcal{C}}(X) & & \\
\Big\downarrow\kern-0.6em\raisebox{-0.3em}{} & \searrow^{\beta} & \\
G & \xrightarrow{\ \alpha\ } & H
\end{array}
$$

be a pro-$\mathcal{C}$-embedding problem for $\Gamma^{\mathcal{C}}(X)$ with algebraic kernel and $\mathrm{rank}(H) < |X|$. *Assume that there exists a finite set $B \subseteq \ker(\alpha)(\bar{k})$ with $\ker(\alpha) = \langle B \rangle$. Then (14) is solvable.*

Proof. According to Lemma 3.34 there exist algebraic groups H', H'' and epimorphisms $H' \twoheadrightarrow H''$ and $H \twoheadrightarrow H''$ such that $G = H' \times_{H''} H$.

We will define a map $\varphi \colon X \to G(\bar{k})$. Let us first define $\varphi(x)$ for $\iota(x) \notin \ker(\beta)(\bar{k})$. If x maps to the identity under $\Gamma^{\mathcal{C}}(X) \twoheadrightarrow H \twoheadrightarrow H''$, we set $\varphi(x) = (1, \beta(\iota(x))) \in (H' \times_{H''} H)(\bar{k})$. There are only finitely many elements, say $x_1, \ldots, x_n$, of X that do not map to the identity under $\Gamma^{\mathcal{C}}(X) \twoheadrightarrow H''$. For these we can choose $h'_i \in H'(\bar{k})$ such that the image of h'_i in $H''(\bar{k})$ agrees with the image of x_i in $H''(\bar{k})$. We set $\varphi(x_i) = (h'_i, \beta(\iota(x_i))) \in (H' \times_{H''} H)(\bar{k})$ for $i = 1, \ldots, n$.

Now let us define $\varphi(x)$ for $\iota(x) \in \ker(\beta)(\bar{k})$. By assumption there exists a finite subset $B = \{b_1, \ldots, b_m\}$ of $\ker(\alpha)(\bar{k})$ with $\ker(\alpha) = \langle B \rangle$. It follows from Lemma 3.13 that $X \cap \iota^{-1}(\ker(\beta)(\bar{k}))$ is infinite. So we can find distinct elements $x'_1, \ldots, x'_m \in X \cap \ker(\beta)(\bar{k})$. We set $\varphi(x'_i) = b_i$ for $i = 1, \ldots, m$. For $x \notin \{x'_1, \ldots, x'_m\}$ we set $\varphi(x) = 1$. This concludes the definition of φ. Note that by construction $\alpha \circ \varphi = \beta \circ \iota$ on X. We claim that $\varphi \colon X \to G(\bar{k})$ converges to 1.

If N is a coalgebraic subgroup of H contained in $\ker(H \twoheadrightarrow H'')$, then $1 \times_{H''} N$ is a coalgebraic subgroup of $G = H' \times_{H''} H$. Moreover, every coalgebraic subgroup N' of G contains a coalgebraic subgroup of this form. (Namely, the intersection of N' with the kernel of the projection $H' \times_{H''} H \twoheadrightarrow H'$.) So it suffices to see that φ maps almost all elements of X into $(1 \times_{H''} N)(\bar{k})$, where N is a coalgebraic subgroup of H contained in $\ker(H \twoheadrightarrow H'')$. This however, is clear from the definition of φ.

We next show that $\langle \varphi(X) \rangle = G$. Using Lemma 2.16 we see that $\alpha(\langle \varphi(X) \rangle) = \langle \alpha(\varphi(X)) \rangle = \langle \beta(\iota(X)) \rangle = H$. Since $\ker(\alpha) \subseteq \langle \varphi(X) \rangle$, this implies $\langle \varphi(X) \rangle = G$.

Thus φ induces an epimorphism $\phi \colon \Gamma^{\mathcal{C}}(X) \to G$. Clearly ϕ is a solution of (14). $\quad\square$

Theorem 3.42. *Let k be a field of characteristic zero, $\mathcal{C}$ a formation and Γ a pro-$\mathcal{C}$-group with $\mathrm{rank}(\Gamma) \geq |k|$. Then Γ is isomorphic to a free pro-$\mathcal{C}$-group on a set of cardinality $\mathrm{rank}(\Gamma)$ if and only if Γ is saturated.*

Proof. Let X be a set with $|X| = \text{rank}(\Gamma)$. Assume first that $\Gamma \simeq \Gamma^{\mathcal{C}}(X)$. Then $\text{rank}(\Gamma^{\mathcal{C}}(X)) = |X|$ and because in characteristic zero any algebraic group is finitely generated (Lemma 2.26), it follows from Proposition 3.41 that $\Gamma \simeq \Gamma^{\mathcal{C}}(X)$ is saturated.

Conversely, assume Γ is saturated. We know from Corollary 3.12 that $\text{rank}(\Gamma^{\mathcal{C}}(X)) = |X|$. So, as above, it follows from Proposition 3.41 that $\Gamma^{\mathcal{C}}(X)$ is saturated. Since $\text{rank}(\Gamma^{\mathcal{C}}(X)) = \text{rank}(\Gamma)$ we can conclude that $\Gamma^{\mathcal{C}}(X)$ and Γ are isomorphic by Theorem 3.38. □

Corollary 3.43. *Let k be a countable field of characteristic zero and let $\mathcal{C}$ be a formation. Moreover, let X be a countably infinite set and Γ a pro-$\mathcal{C}$-group of countable rank. Then Γ is isomorphic to the free pro-$\mathcal{C}$-group $\Gamma^{\mathcal{C}}(X)$ if and only if every $\mathcal{C}$-embedding problem for Γ is solvable.*

Proof. By Corollary 3.12 the free pro-$\mathcal{C}$-group $\Gamma^{\mathcal{C}}(X)$ has rank $|X|$. By Theorem 3.42 $\Gamma \simeq \Gamma^{\mathcal{C}}(X)$ is saturated. Since $\text{rank}(\Gamma)$ is countable, condition (ii) of Theorem 3.24 reduces to the statement that all $\mathcal{C}$-embedding problems are solvable.

Conversely, if every $\mathcal{C}$-embedding problem for Γ is solvable, then $\text{rank}(\Gamma)$ has to be infinite. Since $\text{rank}(\Gamma)$ is countable, we see that Γ is saturated. Thus $\Gamma \simeq \Gamma^{\mathcal{C}}(X)$ by Theorem 3.42. □

Theorem 3.42 is not true in positive characteristic. The corresponding statement in positive characteristic fails for two reasons. Firstly, a free proalgebaic group over a perfect field is always reduced (Remark 2.20) while a saturated pro-$\mathcal{C}$-group need not be reduced. Indeed, if $\mathcal{C}$ contains at least one algebraic group that is not reduced, then a saturated pro-$\mathcal{C}$-group is not reduced.

Secondly, and maybe more fundamentally, not all algebraic groups in positive characteristic are finitely generated, so, if $\mathcal{C}$ contains an algebraic group that is not finitely generated, then it cannot be a quotient of a free pro-$\mathcal{C}$-group and therefore the free pro-$\mathcal{C}$-group cannot be saturated.

We conclude this section with two examples that illustrate Theorem 3.42. These examples also show that Theorem 3.42 is not true without the assumption that $\text{rank}(\Gamma) \geq |k|$.

Example 3.44. Let k be a field of characteristic zero, $\mathcal{C}$ the formation of all abelian unipotent groups and κ an infinite cardinal. According to Examples 3.39 and 2.24, the saturated pro-$\mathcal{C}$-group of rank κ is $\prod_{\kappa} \mathbb{G}_a$, while the free pro-$\mathcal{C}$-group on a set of cardinality κ is $\prod_{Y} \mathbb{G}_a$, where $|Y| = \kappa \cdot \dim_k(\overline{k})$. These groups are isomorphic if and only if $\dim_k(\overline{k}) \leq \kappa$. As predicted by Theorem 3.42, this is the case if $\kappa \geq |k|$.

Example 3.45. Let $\mathcal{C}$ be the formation of all diagonalizable algebraic groups and let X be an infinite set. We saw in Example 2.25 that $\Gamma^{\mathcal{C}}(X) = D(\bigoplus_X \overline{k}^{\times})$. On the other hand, we saw in Example 3.40 that the saturated pro $\mathcal{C}$-group of rank $|X|$ is given by $D(\bigoplus_X \mathbb{Q} \oplus \bigoplus_X \mathbb{Q}/\mathbb{Z})$. In positive characteristic p these groups are not isomorphic since $\bigoplus_X \overline{k}^{\times}$ has no p-torsion, whereas $\bigoplus_X \mathbb{Q} \oplus \bigoplus_X \mathbb{Q}/\mathbb{Z}$ does. So let us assume that k has characteristic zero. The group $\bigoplus_X \mathbb{Q} \oplus \bigoplus_X \mathbb{Q}/\mathbb{Z}$ has cardinality $|X|$, whereas the group $\bigoplus_X \overline{k}^{\times}$ has cardinality $|X| \cdot |k|$. Thus if $|X| < |k|$, the groups are not isomorphic. On the other hand, if $|X| \geq |k|$, the groups must be isomorphic by Theorem 3.42. An explicit (non-canonical) isomorphism between the two groups can be constructed by observing that $\overline{k}^{\times} \simeq \mathbb{Q}/\mathbb{Z} \oplus_{\kappa} \mathbb{Q}$ for some cardinal $\kappa \leq |k|$.

References

[BHH18] A. Bachmayr, D. Harbater, and J. Hartmann, *Differential embedding problems over Laurent series fields*, J. Algebra **513** (2018), 99–112.

[BHHP] A. Bachmayr, D. Harbater, J. Hartmann, and F. Pop, *Large fields in differential Galois theory*, preprint 2017. arXiv:1710.03183

[BHHW] A. Bachmayr, D. Harbater, J. Hartmann, and M. Wibmer, *Free differential Galois groups*, preprint 2019. arXiv:1904.07806

[BHHW18] A. Bachmayr, D. Harbater, J. Hartmann, and M. Wibmer, *Differential embedding problems over complex function fields*, Doc. Math. **23** (2018), 241–291.

[BLMM02] H. Bass, A. Lubotzky, A. R. Magid, and S. Mozes, *The proalgebraic completion of rigid groups.* In: Proceedings of the Conference on Geometric and Combinatorial Group Theory, Part II (Haifa, 2000), pp. 19–58, Geom. Dedicata, **95** (2002).

[Cha98] Z. Chatzidakis. *Model theory of profinite groups having the Iwasawa property*, Illinois J. Math. **42** (1998), no. 1, 70–96.

[CvdDM82] G. Cherlin, L. van den Dries, and A. Macintyre, *The elementary theory of regularly closed fields*, preprint 1982.

[Del90] P. Deligne, *Catégories tannakiennes.* In: The Grothendieck Festschrift, Vol. II, pp. 111–195, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990.

[DG70] M. Demazure and P. Gabriel, *Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs.* Avec un appendice *Corps de classes local* par Michiel Hazewinkel. Masson & Cie, Éditeur, Paris; North-Holland Publishing Co., Amsterdam, 1970.

[DM82] P. Deligne and J. S. Milne, *Tannakian categories.* In: Hodge cycles, motives, and Shimura varieties, pp. 101–228, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin, 1982.

[Dou64] A. Douady, *Détermination d'un groupe de Galois*, C. R. Acad. Sci. Paris **258** (1964), 5305–5308.

[FJ08] M. D. Fried and M. Jarden, *Field arithmetic*, third edition. Revised by Jarden. Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics, vol. 11, Springer-Verlag, Berlin, 2008.

[Gro70] *Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Schémas en groupes. I: Propriétés générales des schémas en groupes.* Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, vol. 151. Springer-Verlag, Berlin, 1970.

[Har] D. Harbater, *Shafarevich conjecture*, Encyclopedia of Mathematics. http://www.encyclopediaofmath.org/index.php?title=Shafarevich_conjecture&oldid=39969.

[Har95] D. Harbater, *Fundamental groups and embedding problems in characteristic p*. In: Recent developments in the inverse Galois problem (Seattle, WA, 1993), pp. 353–369, Contemp. Math., vol. 186, Amer. Math. Soc., Providence, RI, 1995.

[Har05] J. Hartmann, *On the inverse problem in differential Galois theory*, J. Reine Angew. Math. **586** (2005), 21–44.

[Iwa53] K. Iwasawa, *On solvable extensions of algebraic number fields*, Ann. of Math (2) **58** (1953), 548–572.

[Kap54] I. Kaplansky, *Infinite abelian groups*, University of Michigan Press, Ann Arbor, 1954.

[Kov69] J. Kovacic, *The inverse problem in the Galois theory of differential fields*, Ann. of Math. (2) **89** (1969), 583–608.

[Kov71] J. Kovacic, *On the inverse problem in the Galois theory of differential fields. II.* Ann. of Math. (2) **93** (1971), 269–284.

[LM82] A. Lubotzky and A. Magid, *Cohomology of unipotent and prounipotent groups*, J. Algebra **74** (1982), no. 1, 76–95.

[LM83] A. Lubotzky and A. R. Magid, *Free prounipotent groups*, J. Algebra **80** (1983), no. 2, 323–349.

[Mag94] A. R. Magid, *Lectures on differential Galois theory*, University Lecture Series, vol. 7, American Mathematical Society, Providence, RI, 1994.

[Mag01]   A. R. Magid, *The Picard-Vessiot antiderivative closure*, J. Algebra **244** (2001), no. 1, 1–18.

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

[MvdP03] B. H. Matzat and M. van der Put, *Constructive differential Galois theory.* In: Galois groups and fundamental groups, pp. 425–467, Math. Sci. Res. Inst. Publ., vol. 41, Cambridge Univ. Press, Cambridge, 2003.

[Obe03]   T. Oberlies, *Einbettungsprobleme in der Differentialgaloistheorie.* Dissertation, 2003. Available at http://www.ub.uni-heidelberg.de/archiv/4550

[Pop95]   F. Pop, *Étale Galois covers of affine smooth curves. The geometric case of a conjecture of Shafarevich. On Abhyankar's conjecture.* Invent. Math. **120** (1995), no. 3, 555–578.

[RZ10]   L. Ribes and P. Zalesskii, *Profinite groups*, second edition, Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics, vol. 40, Springer-Verlag, Berlin, 2010.

[vdPS03] M. van der Put and M. F. Singer, *Galois theory of linear differential equations*, Fundamental Principles of Mathematical Sciences, vol. 328, Springer-Verlag, Berlin, 2003.

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

[YZh]   YZhou, *Is there a "free abelian group of rank 1" in the category of affine group schemes?* MathOverflow, https://mathoverflow.net/q/211379 (version: 2015-07-13).