Profinite structures interpretable in fields

Krzysztof Krupiński*

Abstract

We investigate profinite structures in the sense of Newelski interpretable in fields. We show that profinite structures interpretable in separably closed fields are the same as profinite structures weakly interpretable in ACF_p. We also find a strong connection with the inverse Galois problem.

We give field theoretic constructions of profinite structures weakly interpretable in ACF_p and satisfying some model theoretic properties, like smallness, m-normality, non-triviality, being $\mathcal{M}$-rank 1. For example we interpret in this way the profinite structure consisting of the profinite group $\mathbb{Z}_p^\omega$ together with a distiguished Sylow p-subgroup of its standard structural group.

0 Introduction

A profinite structure is a profinite topological space X with a distinguished structural group $Aut^*(X)$ which is a closed subgroup of the group of all homeomorphisms of X respecting the appropriate inverse system. A profinite group in this context is an inverse limit of finite groups (so it is a profinite group in the usual sense, see [RZ]) with the structural group preserving the group action. Precise definitions are given in Preliminaries.

In this paper we consider profinite structures which are inverse limits of countable systems. So w.l.o.g. they have a form

$$\lim_{\longleftarrow} X_i$$

for inverse systems $X_0 \longleftarrow X_1 \longleftarrow \dots$ of finite discrete spaces X_i, $i \in \omega$. We say that the structural group $Aut^*(X)$ of a profinite structure [group] X is standard if it is the group of all homeomorphisms [topological automorphisms] of X respecting the appropriate inverse system. We say that X is small if for every natural number $n > 0$, on the set $X^n = X \times \dots \times X$ there are countably many orbits under the action of $Aut^*(X)$. Profinite structures, in particular profinite groups regarded as profinite

*Research supported by KBN grant 2 P03A 016 24
Key words: profinite structures, separably closed fields, algebraically closed fields

structures, have been introduced in [N1] and [N2]. Small profinite groups occur naturally in model theory as profinite groups interpretable in small theories [N1]. Newelski has developed the model theory of small profinite structures. Many results from stable model theory have been proven in this context. The model theoretic notions of m-normality, m-stability and $\mathcal{M}$-rank (see Definitions 4.1 and 4.2) play prominent role in all these considerations.

The simplest examples of profinite groups are products of countably many finite groups. Let $X = \prod_{i<\omega} X_i$ be such a product. We consider it as the inverse limit of finite groups $X \restriction n = \prod_{i<n} X_i$, $n > 0$, with the natural projections. The standard structural group consists here of these automorphisms of X which induce automorphisms of each $X \restriction n$ for $n > 0$. Any other structural group of X can be chosen as a closed subgroup of the standard one.

The main example of small, m-normal and m-stable profinite groups are products of countably many finite abelian groups of bounded exponent [Kr1]. More precisely, a product $X = \prod_{i<\omega} X_i$ of finite groups (with the standard structural group) is small iff almost all groups X_i are abelian and X has finite exponent. In this case X is also m-normal and m-stable. More generally, each abelian profinite group of finite exponent, being the inverse limit of a system indexed by ω and considered with the standard structural group, is small, m-normal and m-stable [Kr2].

There are several open questions about the existence of small profinite structures and groups with some model theoretic properties [N1], [N2]. Some of them are the following:

($*$) Does there exist a profinite structure which is small but not m-normal?

($**$) Does there exist a small profinite structure X containing an orbit o such that $\omega \leq \mathcal{M}(o) < \infty$?

Wagner [W] gave a negative answer to ($**$) for small profinite groups.

Trying to answer positively such kind of questions we need new explicit examples (and methods of constructing them) of small profinite structures. Except for abelian profinite groups with the standard structural group and with some other structural groups (see [Kr1], [Kr2]) there are no examples of small profinite structures. Profinite structures interpretable in classical algebraic theories (see Definitions 1.1.5 and 1.1.6) have not been considered so far.

Our main goal in this paper is to find examples (and methods of constructing them) of profinite structures interpretable in separably and algebraically closed fields and satisfying various model theoretic properties.

Besides the standard definition of profinite structure interpretable in a first order theory (Definition 1.1.5) we also consider the notion of weak interpretability (Definition 1.1.6).

We could have started from profinite structures interpretable in ACF_p. However, by ω-stability, we get that every such structure is countable with finite orbits under the action of the structural group, so it is small, m-normal, m-stable with $\mathcal{M}$-rank 0. That is why we turn to profinite structures interpretable in $SCF_{p,e}$, where e is the Ershov invariant (∞ or finite $\neq 0$).

We consider profinite structures interpretable in $SCF_{p,e}$ over a countable field F. Showing finite elimination of imaginaries (Definition 1.1.3) in $SCF_{p,\infty}$ and using some model theory of $SCF_{p,e}$ we get (under natural assumptions on F) that profinite structures interpretable in $SCF_{p,e}$ (e is arbitrary $\neq 0$) over F are the same as those weakly interpretable in ACF_p over F. The situation becomes interesting because:

- we are able to obtain explicit examples of profinite structures weakly interpretable in ACF_p with various model theoretic properties;

- there is a strong connection between weak interpretability in ACF_p and the inverse Galois problem.

Let us recall here that for a fixed field F the inverse Galois problem asks:

($***$) Which groups do appear as Galois groups of Galois extensions of F?

We show (see Theorem 3.1) that a profinite structure is weakly interpretable in ACF_p over a fixed field F iff its structural group appears as the Galois group of a Galois extension of F.

This theorem marks out two directions for further considerations. The first one uses Galois theory to obtain new profinite structures weakly interpretable in ACF_p, which could give the positive answer to the questions like ($*$) and ($**$). The second one is a new approach to the inverse Galois problem. Namely, instead of asking if a profinite group is the Galois group of some Galois extension of F, we could consider this group as the structural group of some profinite structure X and ask if X is weakly interpretable in ACF_p over F. Maybe some model theoretic assumptions on X could give the positive answer to this question yielding new examples of Galois groups.

In this paper we concentrate on the first direction. At the beginning of Section 4 we describe two methods for obtaining profinite structures weakly interpretable in ACF_p over a fixed field.

Method 1 Direct field theoretic construction.

Method 2 Applying Theorem 3.1 and some more advanced Galois theory.

Using them we get several examples of profinite structures weakly interpretable in ACF_p over the field of rational functions (or more generally, over any Hilbertian field) which are respectively:

- not m-normal, not m-stable, not small;

- of $\mathcal{M}$-rank 1, m-normal, not small, non-trivial;

- of $\mathcal{M}$-rank 1, m-normal, small, trivial;

- of $\mathcal{M}$-rank n (for arbitrary $n \in \omega$), m-normal, small, non-trivial for $n = 1$.

In fact in the last item we obtain small profinite groups $(\mathbb{Z}^{\omega}_{p^n}, Aut^*(\mathbb{Z}^{\omega}_{p^n}))$, where $Aut^*(\mathbb{Z}^{\omega}_{p^n})$ is the standard structural group of $\mathbb{Z}^{\omega}_{p^n}$.

At the end we would like to say that we assume that the reader is familiar with basic model theory. We use the notions of a countable first order theory, its monster model $\mathfrak{C}$, types, algebraic and definable closure (acl, dcl), imaginary extension $\mathfrak{C}^{eq}$, definable and type-definable sets in $\mathfrak{C}$ (see [Ba], [Bu], [M], [Pi], [S]).

We would like to draw the reader's attention to the fact that sometimes we use model theoretic notions in classical model theoretic context and sometimes in the context of profinite structures.

1 Preliminaries

1.1 Profinite structures

We present here all the necessary definitions and basic facts on profinite structures and groups in the sense of Newelski. For the proofs and more details about profinite structures and groups see [N1], [N2] and [W].

We start from the general definition of a profinite structure. A profinite space X is the inverse limit of an inverse system $(X_i, f_{ij})_{i,j\in I}$ of finite discrete spaces X_i, $i \in I$, with topology inherited from the product of all these finite spaces. We say that a homeomorphism f of X respects the inverse system if for any $i \in I$ and for any two elements $a, b \in X$ with the same i-th coordinate, the images $f(a)$ and $f(b)$ have also the same i-th coordinate. The homeomorphisms of X respecting the inverse system form a topological group $Homeo^*(X)$ with topology inherited from the Tychonov product topology on the space X^X.

Definition 1.1.1 *A profinite structure is a profinite topological space X with a distinguished structural group $Aut^*(X)$, which is a closed subgroup of $Homeo^*(X)$.*

We call $Homeo^*(X)$ the standard structural group of X.

W.l.o.g. we assume from now on that all the connecting maps are surjections. So, a homeomorphism f of X belongs to $Homeo^*(X)$ iff f is induced by an automorphism of the inverse system, e.g. for $I = \omega$, f arises from a sequence $f_0, f_1, \ldots$ of automorphisms of $X_0, X_1, \ldots$, respectively, defining an automorphism of the inverse system (Fig. 0).

$$\begin{tikzcd}
X_0 \arrow[d, "f_0"'] & X_1 \arrow[l, "f_{10}"'] \arrow[d, "f_1"'] & X_2 \arrow[l, "f_{21}"'] \arrow[d, "f_2"'] & \cdots \arrow[l, "f_{32}"'] & X \arrow[d, "f"'] \\
X_0 & X_1 \arrow[l, "f_{10}"'] & X_2 \arrow[l, "f_{21}"'] & \cdots \arrow[l, "f_{32}"'] & X
\end{tikzcd}$$

Figure 0

As we mentioned in the introduction we consider only inverse limits of countable systems, w.l.o.g. of the form

$$\varprojlim X_i$$

for inverse systems $X_0 \longleftarrow X_1 \longleftarrow \ldots$ of finite discrete spaces X_i, $i \in \omega$. More precisely, the inverse limit of a countable system can be regarded as the inverse limit of a subsystem indexed by ω. However, the standard structural group in the first case is a closed subgroup (sometimes proper) of the standard structural group in the second case.

It turns out that $Homeo^*(X)$ and $Aut^*(X)$ are profinite groups. Namely, they are inverse limits of systems of some groups of permutations of spaces X_i, $i \in \omega$. Moreover, they act continuously on X.

Assume X is a profinite group, that is, the inverse limit of a system of finite groups X_i, $i \in \omega$. In this paper we will consider X as a profinite structure in the sense of Definition 1.1.1, with the structural group $Aut^*(X)$ being a closed subgroup of $Homeo^*(X)$, consisting of group automorphisms of X. Sometimes $Aut^*(X)$ will consist of all group automorphisms of X respecting the inverse system. Then $Aut^*(X)$ will be called standard.

We denote a profinite structure by $(X, Aut^*(X))$. When it is clear what the structural group is we just write X.

Let X be a profinite structure, e.g. a profinite group. Let $A \subseteq X$ be finite. By $Aut^*(X/A)$ we denote the set of elements of $Aut^*(X)$ fixing A pointwise. We say that $V \subseteq X$ is A-invariant if $f[V] = V$ for every $f \in Aut^*(X/A)$. If V is additionally closed, then we say that V is A-definable.

For $a \in X^n$ and $A \subseteq X$ we define

$$o(a/A) = \{f(a) : f \in Aut^*(X/A)\},$$

the orbit of a over A. Let $O_n(A) = \{o(a/A) : a \in X^n\}$. Usually $A, B, \ldots$ denote finite subsets of X and $a, b, \ldots$ denote elements or finite tuples of elements of X.

A profinite structure $(X, Aut^*(X))$ is called homogeneous if any two elements of X lie in the same orbit under the action of $Aut^*(X)$. We say that a profinite structure X is small if $|O_n(\emptyset)| \leq \omega$ for every natural number $n > 0$ (see [N1], [N2]). Equivalently, $O_1(A)$ is countable for every finite set $A \subseteq X$.

As we mentioned in the introduction, the main examples of small profinite groups are abelian profinite groups of finite exponent being the inverse limits of systems indexed by ω and considered with the standard structural group.

Two profinite structures $(X, Aut^*(X))$ and $(Y, Aut^*(Y))$ are isomorphic if there is a homeomorphism $f : X \to Y$ such that the pullback function f^* maps $Aut^*(Y)$ onto $Aut^*(X)$. Equivalently, there is a homeomorphism $f : X \to Y$ and a topological isomorphism $\Phi : Aut^*(X) \to Aut^*(Y)$ such that $f(g(x)) = \Phi(g)(f(x))$ for all $x \in X$ and $g \in Aut^*(X)$.

A degenerate example of a profinite structure is a finite permutational structure, i.e. a pair (X, G), where X is a finite set and G is a group of permutations of X. An isomorphism between two finite permutational structures is an isomorphism of profinite structures. In other words, (X, G) and (Y, H) are isomorphic iff there is a bijection $f : X \to Y$ and a group isomorphism $\Phi : G \to H$ such that $f(gx) = \Phi(g)f(x)$ for all $x \in X$ and $g \in G$. The following easy remark will be useful in the proof of Theorem 3.1.

Remark 1.1.2 *Let (X, G) be a finite permutational structure and $\{x_1, \dots, x_n\}$ be a selector of the set of all orbits on X under the action of G. Let $H_i = Stab(x_i) < G$, $i = 1, \dots, n$. Then $(G/H_1 \cupdot \dots \cupdot G/H_n, G) \cong (X, G)$, where the action of G on the disjoint union $G/H_1 \cupdot \dots \cupdot G/H_n$ is given by the left multiplication, a bijection $f : G/H_1 \cupdot \dots \cupdot G/H_n \to X$ is defined by $f(gH_i) = gx_i$ and an isomorphism $\Phi : G \to G$ is the identity.*

We will need a weaker version of elimination of imaginaries.

Definition 1.1.3 *We say that a complete theory T has finite elimination of imaginaries if for every subset F of a monster model of T and for every finite equivalence relation E definable over F each class of E is interdefinable over F with some real element from $acl(F)$.*

One can check that T has finite elimination of imaginaries iff for every F and $a \in acl^{eq}(F)$ the element a is interdefinable over F with some real element from $acl(F)$.

For finite elimination of imaginaries we have the following proposition, which corresponds to the similar fact for full elimination of imaginaries [MMP].

Proposition 1.1.4 *Suppose T has finite elimination of imaginaries. Let M be a monster model of T and E be a finite equivalence relation on M^n definable over a subset F of M such that $|dcl(F)| \geq 2$. Then there is an F-definable function $f : M^n \to M^m$ such that $xEy \iff f(x) = f(y)$.*

Proof. Let $o_1, \dots, o_k$ be the orbits on M^n/E under the action of $Aut(M/F)$. Take any representatives $a_1/E \in o_1, \dots, a_k/E \in o_k$. By finite elimination of imaginaries we can find tuples $b_i \in M^{m_i}$, $i \leq k$, such that for all $i \leq k$, b_i is interdefinable over F with a_i/E. Using the fact that $|dcl(F)| \geq 2$ we can assume that all m_i are equal to the same natural number m'. Take two elements $\alpha \neq \beta$ from $dcl(F)$.

Now we can define our function $f : M^n \to M^m$, where $m = m' + k$. Fix an $a \in M^n$. We have a unique $i \leq k$ such that $a/E \in o_i$. We take an arbitrary $g \in Aut(M/F)$ with $g(a_i/E) = a/E$. Finally we define

$$f(a) = g(b_i)^\frown \epsilon_i \in M^{m'+k},$$

where $\epsilon_i \in M^k$ has α on the i-th coordinate and β on the remaining coordinates. One can verify that f satisfies our demands. ■

Now we turn to the notions of interpretability. First we recall the definition of interpretability from [N1] and [N2]. Then we introduce a notion of weak interpretability.

Let T be a first order countable complete theory T with a monster model $\mathfrak{C}$ and $F \subseteq \mathfrak{C}$ be a countable (w.l.o.g. dcl-closed) set. In the definition below Y is an arbitrary F-type-definable subset of $\mathfrak{C}^{eq}$ and $E_1 \supseteq E_2 \supseteq \dots$ is an arbitrary descending sequence of finite F-definable equivalence relations on Y.

Definition 1.1.5 *We say that a profinite structure is interpretable in T over F if it is isomorphic to the inverse limit of spaces Y/E_i with the structural group induced by $Aut(\mathfrak{C}/F)$.*

So $(X, Aut^*(X))$ is interpretable in T over F iff it is isomorphic to

$$\{\langle a/E_1, a/E_2, \dots\rangle : a \in Y\}$$

with the structural group induced by $Aut(\mathfrak{C}/F)$.

Definition 1.1.6 *We say that a profinite structure is weakly interpretable in T over F if it is isomorphic to an F-type-definable subset of $acl^{eq}(F)^\omega$ with the structural group induced by $Aut(\mathfrak{C}/F)$.*

In the above definition we treat X as the inverse limit of the inverse system of projections of X on the first i coordinates, $i \in \omega$ (all these projections are of course finite). For theories with elimination of imaginaries or even with finite elimination of imaginaries Definition 1.1.6 can be simplified as follows.

Proposition 1.1.7 *If T has finite elimination of imaginaries and $|dcl(F)| \geq 2$, then every profinite structure weakly interpretable in T over F is isomorphic to an F-type-definable subset of $acl(F)^\omega$ with the structural group induced by $Aut(\mathfrak{C}/F)$.*

Proof. We can assume that our profinite structure $(X, Aut^*(X))$ weakly interpretable in T over F is just an F-type-definable subset of $acl^{eq}(F)^\omega$ with the structural group induced by $Aut(\mathfrak{C}/F)$. The idea of the proof is to replace imaginary coordinates of elements of X by the real ones.

We have that X is an F-type-definable subset of $\mathfrak{C}^{n_1}/E_1 \times \mathfrak{C}^{n_2}/E_2 \times \dots$, for some 0-definable equivalence relations E_i, $i \in \omega$. Fix an $i \in \omega$. Then the projection $\pi_i[X]$ of X on the i-th coordinate is a finite F-definable subset of $\mathfrak{C}^{n_i}/E_i$. So the set $X_i = \{c \in \mathfrak{C}^{n_i} : c/E_i \in \pi_i[X]\}$ is F-definable. Hence we can find a finite F-definable equivalence relation E_i' on $\mathfrak{C}^{n_i}$ which coincides with E_i on X_i. Finally we see that X is an F-type-definable subset of $\mathfrak{C}^{n_1}/E_1' \times \mathfrak{C}^{n_2}/E_2' \times \dots$ (in fact we work here in the language expanded by constants from F).

Now Proposition 1.1.4 yields a collection of F-definable functions $f_i' : \mathfrak{C}^{n_i} \to \mathfrak{C}^{m_i}$ such that $xE_i'y \iff f_i'(x) = f_i'(y)$ for all $i \in \omega$. Hence we get F-definable injections $f_i : \mathfrak{C}/E_i' \to \mathfrak{C}^{m_i}$ for $i \in \omega$. Consider an F-type-definable injection

$$f : X \to \prod_{i\in\omega} \mathfrak{C}^{m_i},$$

defined by

$$f(\langle x_i/E_i' : i \in \omega\rangle) = \langle f_i(x_i/E_i') : i \in \omega\rangle.$$

Let $Y = f[X]$. Then Y is an F-type-definable subset of $acl(F)^\omega$. It is easy to check that f defines an isomorphism between $(X, Aut(\mathfrak{C}/F) \restriction X)$ and $(Y, Aut(\mathfrak{C}/F) \restriction Y)$. ■

Now we look at the relationship between two notions of interpretability.

Proposition 1.1.8 *A profinite structure $(X, Aut^*(X))$ is interpretable in T over F iff there is an F-type-definable set $Y \subseteq \mathfrak{C}^{eq}$ and F-definable functions $f_i : Y \to acl^{eq}(F)$, $i \in \omega$, such that $(X, Aut^*(X))$ is isomorphic to the F-type-definable set*

$$\{\langle f_0(a), f_1(a), \ldots\rangle \in acl^{eq}(F)^\omega : a \in Y\} \subseteq acl^{eq}(F)^\omega,$$

with the structural group induced by $Aut(\mathfrak{C}/F)$.

Proof. ($\leftarrow$) Assume $(X, Aut^*(X))$ is isomorphic to an F-type-definable set

$$\{\langle f_0(a), f_1(a), \ldots\rangle \in acl^{eq}(F)^\omega : a \in Y\} \subseteq acl^{eq}(F)^\omega,$$

with the structural group induced by $Aut(\mathfrak{C}/F)$. Define relations E_i, $i \in \omega$, on Y in the following way

$$E_i(x, y) \iff \bigwedge_{j \leq i} f_j(x) = f_j(y).$$

We easily see that $E_0 \supseteq E_1 \supseteq \ldots$ are finite F-definable equivalence relations on Y and that $(X, Aut^*(X))$ is isomorphic to the inverse limit of finite spaces Y/E_i, $i \in \omega$, with the structural group induced by $Aut(\mathfrak{C}/F)$.

($\rightarrow$) Assume X is the inverse limit of a system Y/E_i, $i \in \omega$, and $Aut^*(X)$ is induced by $Aut(\mathfrak{C}/F)$, for an F-type-definable set Y and finite F-definiable equivalence relations E_i, $i \in \omega$, on Y. Then for each $i \in \omega$, there is an F-definable equivalence relation E'_i defined on the appropriate sort of $\mathfrak{C}$ which coincides with E_i on Y. Let $E'_i(x, y, b_i)$ be a formula over $b_i \subseteq F$ defining E'_i. By compactness there is a formula $\phi(z) \in tp(b_i)$ such that for each $b \models \phi$ the formula $E'_i(x, y, b)$ defines an equivalence relation on $\mathfrak{C}$. We define new 0-definable equivalence relations on $\mathfrak{C}$ as follows:

$$E''_i((x, z), (y, t)) \iff (x = y \wedge z = t) \vee (\phi(z) \wedge z = t \wedge E'_i(x, y, z)).$$

Now we can define the desired functions $f_i : Y \to acl^{eq}(F)$. Namely, for each $a \in Y$ we put

$$f_i(a) = (a, b_i)/E''_i.$$

Let $Z = \{\langle f_0(a), f_1(a), \ldots\rangle \in acl^{eq}(F)^\omega : a \in Y\}$ and $Aut^*(Z)$ be induced by $Aut(\mathfrak{C}/F)$. To finish the proof notice that a function $f : X \to Z$ defined by

$$f(\langle a/E_i : i \in \omega\rangle) = \langle (a, b_i)/E''_i : i \in \omega\rangle,\ a \in Y$$

yields an isomorphism of profinite structures $(X, Aut^*(X))$ and $(Z, Aut^*(Z))$. ■

Corollary 1.1.9 *Each profinite structure interpretable in T over F is also weakly interpretable in T over F.*

We also see that a profinite structure interpretable in T over F is isomorphic to a very special F-type-definable subset of $acl^{eq}(F)$. In fact in many cases the class of profinite structures interpretable in T over F is much smaller than the class of profinite structures weakly interpretable in T over F (e.g for $T = ACF_p$).

The main examples of profinite structures interpretable in T over F are traces of complete types over F. More precisely, for $p \in S(F)$ we consider $(Tr(p), Aut^*(Tr(p)))$, where

$$Tr(p) = \{q \in S(acl^{eq}(F)) : p \subseteq q\}$$

and $Aut^*(Tr(p))$ is induced by $Aut(\mathfrak{C}/F)$. We treat $Tr(p)$ as the inverse limit of the system of all spaces $p(\mathfrak{C})/E$, with E ranging over finite equivalence relations on $\mathfrak{C}$ definable over F. So $Tr(p)$ is a profinite structure homogeneous under the action of $Aut^*(Tr(p))$. We racall that the elements of $S(acl^{eq}(F))$ are called strong types over F. For $a \in \mathfrak{C}$ we will use the notation $stp(a/F) = tp(a/acl^{eq}(F))$.

Throughout the paper $\overline{F}$ [$\overline{F}^{sep}$, respectively] denotes the algebraic [separable] closure of a given field F.

Let F be a field of characteristic p. The main examples of profinite structures weakly interpretable in ACF_p over a field F are of the form

$$(T_\eta, Gal(T_\eta/F)),$$

where for $\eta \in (\overline{F}^{sep})^\omega$ we define T_η as the orbit of η under the action of $Gal(\overline{F}^{sep}/F)$ and $Gal(T_\eta/F)$ as the group of permutations of T_η induced by $Gal(\overline{F}^{sep}/F)$. We treat T_η as the inverse limit of finite spaces $T_{\eta\restriction i}$, $i \geq 1$, where $T_{\eta\restriction i}$ is defined as the orbit of the finite tuple $\eta \restriction i$ under the action of $Gal(\overline{F}^{sep}/F)$. Similar example also works for an arbitrary complete theory T. However, in this paper we will use it only in the case $T = ACF_p$.

Let F be a field. Throughout the paper, when we have a set Y contained in $\overline{F}$ or in $\overline{F}^\omega$ invariant on $Gal(\overline{F}/F)$, then $Gal(Y/F)$ denotes the group of permutations of Y induced by $Gal(\overline{F}/F)$.

1.2 Fields

In this subsection we recall basic facts on separably closed fields [MMP], [D], [CCSSW], [CW].

Let K be a field of characteristic p and $x_0, \ldots, x_{n-1} \in K$. We say that $x_0, \ldots, x_{n-1}$ are p-independent if the set of monomials $x_0^{i(0)} \ldots x_{n-1}^{i(n-1)}$, $i \in p^n$, is linearly independent over K^p (here p^n denotes the set of n-tuples $i = \langle i(0), \ldots, i(n-1)\rangle$, where $i(j) \in \{0, \ldots, p-1\}$, but sometimes in the paper it denotes just the number). A maximal p-independent subset of K is called a Ershov basis (or a p-basis) of K. The number $p^e = [K : K^p]$, which may be ∞, is called the imperfect degree of K and e the Ershov invariant (or the imperfect exponent) of K (see [FJ], [MMP]).

Classically $SCF_{p,e}$ denotes the theory of separably closed fields of characteristic p and Ershov invariant e in the language $\mathcal{L}$ of field theory. We assume that $e > 0$. Adding to the language names $b_0, \ldots, b_{e-1}$ for elements of an Ershov basis in the case $e < \infty$, or relations $Q_n(x_1, \ldots, x_n)$, $n \in \omega$ (telling that $x_1, \ldots, x_n$ are p-independent) in the case $e = \infty$, we obtain the theory $SCF'_{p,e}$. Finally, by adding to the language the so-called λ-functions, we get the theory $SCF_{p,e,\lambda}$ in the expanded language denoted by $\mathcal{L}_\lambda$, where:

1. For $e < \infty$ the λ-functions λ_i, $i \in p^e$, are defined by equality
$$x = \sum_{i \in p^e} \lambda_i(x)^p b_0^{i(0)} \dots b_{e-1}^{i(e-1)}.$$

2. For $e = \infty$ the λ-functions $\lambda_{i,n}$, $n \in \omega, i \in p^n$, are defined as follows.
For n-tuple $\overline{y}$ and element x we have $\lambda_{i,n}(\overline{y}, x) = 0$, when $\overline{y}$ is p-dependent or $(n+1)$-tuple $\overline{y}, x$ is p-independent, else
$$x = \sum_{i \in p^n} \lambda_{i,n}(\overline{y}, x)^p y_0^{i(0)} \dots y_{n-1}^{i(n-1)}.$$

When $e < \infty$ and $\eta = (i_0, \dots, i_{t-1}) \in (p^e)^t$, then we define λ_η as the composition $\lambda_{i_{t-1}} \circ \dots \circ \lambda_{i_0}$. For an $\eta \in (p^e)^{<\omega}$ and an element x of a model of $SCF_{p,e,\lambda}$ we put $x_\eta = \lambda_\eta(x)$. The elements x_η, $\eta \in (p^e)^{<\omega}$, form the so-called tree of coordinates of x (Fig. 1).

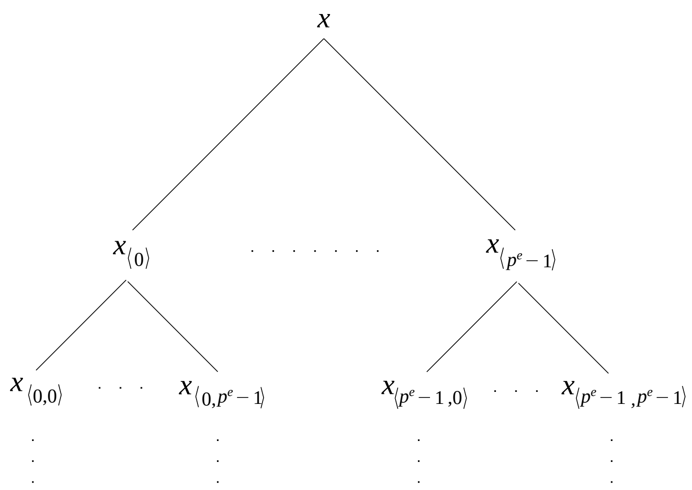


Figure 1

When $e = \infty$, $\mathcal{B}$ is a p-independent subset (maybe infinite) of a model K of $SCF_{p,e,\lambda}$ and an element $x \in K$ satisfies $x \in K^{p^n}(\mathcal{B})$ for all $n \in \omega$, then, similarly as above, we define the tree of coordinates of x with respect to $\mathcal{B}$

The next fact is a collection of well-known results about separably closed fields. For the proofs see [D] and *"Some model theory of separably closed fields"* by M. Messmer in [MMP]. These results are also collected in [CW]. We skip here the index p in $SCF_{p,e}$.

Fact 1.2.1 *1. SCF_e is complete for arbitrary e.*
2. SCF'_e is model complete for arbitrary e.
3. $SCF_{e,\lambda}$ has quantifier elimination for arbitrary e.
4. (i) $\overline{F_p(x_0, \dots, x_{e-1})}^{sep}$ is a prime model of SCF'_e, for $e < \infty$.

(ii) $\overline{F_p(x_i : i \in \omega)}^{sep}$ *is a prime model of* SCF'_∞.

5. *Let* $K \models SCF'_e$. *For an* $A \subseteq K$ *and arbitrary* e *we have.*

   (i) $dcl(A)$ *is the smallest subfield of* K *containing* A *[and* $b_0, \ldots, b_{e-1}$, *for* $e < \infty$*] and closed under all* $\lambda_{i,n}$ *[*λ_i, *for* $e < \infty$*].*

   (ii) $acl(A) = \overline{dcl(A)}^{sep}$.

6. *Let* $K \models SCF'_e$ *and* $A = acl(A) \subseteq K$. *Then we have.*

   (i) $A \prec K$ *for* $e < \infty$.

   (ii) If $e = \infty$ *and a* p*-basis of* A *is infinite, then also* $A \prec K$.

7. *Let* $K \models SCF'_e$, $A = dcl(A) \subseteq K$ *and* $c \in K$. *Then we have.*

   (i) $tp(c/A)$ *is determined by the* $\mathcal{L}$*-isomorphism type over* A *of the field* $dcl(A, c)$.

   (ii) For $e < \infty$, $tp(c/A)$ *is determined by the* $\mathcal{L}$*-isomorphism type over* A *of the tree of coordinates of* c.

   (iii) For $e = \infty$, *if for all* $n \in \omega$ *we have that* $c \in K^{p^n}(A)$, *then* $tp(c/A)$ *is determined by the* $\mathcal{L}$*-isomorphism type over* A *of the tree of coordinates of* c *(in an Ershov basis of* A*).*

In the following we will assume that our language contains the λ-functions and instead of $SCF_{p,e,\lambda}$ we will write $SCF_{p,e}$ or even SCF_e.

Assume for a moment that $e = \infty$ and K is a monster model of SCF_∞. Let $F = dcl(F)$ and take an infinite set $\{e_i\}_{i \in I}$ which is p-independent over F (i.e. elements e_i, $i \in I$, together with a p-basis of F are p-independent) and algebraically independent over F. The following lemma will be very useful in Section 2.

Lemma 1.2.2 *(i) The field* F' *generated by* F *and* $\{e_i\}_{i \in I}$ *is* dcl*-closed.*
(ii) Each field-theoretic automorphism f *of* F *has an extension to an* $f' \in Aut(K)$.

Proof. (i) Let $\mathcal{B}$ be a p-basis of F. Then $\mathcal{B} \cup \{e_i : i \in I\}$ is a p-basis of F'. Moreover, the set $\mathcal{B} \cup \{e_i : i \in I\}$ is p-independent in K, hence K is a separable extension of F'. So F' is an $\mathcal{L}_\lambda$ substructure of K, i.e. it is closed on λ-functions. By Fact 1.2.1 (5 (i)) we get $F' = dcl(F')$.
(ii) By the choice of $\{e_i\}_{i \in I}$ we can extend our f to an automorphism of F'. From (i) and Fact 1.2.1 (5(ii) and 6(ii)) we have that $\overline{F'}^{sep} \prec K$. This allows us to extend our f to an $f' \in Aut(K)$. ■

If e is finite, then Lemma 1.2.2 (ii) is also true under the assumption that f fixes all elements of the named Ershov basis.

For field extensions $F \subseteq K$ and $F \subseteq L$ we use the following notations.

$$K \,|_F\, L \text{ means that } K \text{ and } L \text{ are algebraically disjoint over } F.$$

$$K \,\|_F\, L \text{ means that } K \text{ and } L \text{ are linearly disjoint over } F.$$

At the end we recall the definition of a Hilbertian field, which is crucial in the fourth section. Let F be any field. Let $T = (T_1, \dots, T_r)$ and $X = (X_1, \dots, X_n)$ denote finite sequences of variables. Consider polynomials $f_1(T, X), \dots, f_m(T, X) \in F(T)[X]$, which are irreducible in $F(T)[X]$. For a nonzero polynomial $g(T) \in F[T]$ denote by $H_F(f_1(T, X), \dots, f_m(T, X); g(T))$ the set of all tuples $a = (a_1, \dots, a_r) \in F^r$ such that $g(a) \neq 0$ and $f_1(a, X), \dots, f_m(a, X) \in F[X]$ are defined and irreducible in $F[X]$. Call $H_F(f_1(T, X), \dots, f_m(T, X); g(T))$ a Hilbert set of F.

Definition 1.2.3 *A field F is Hilbertian if its Hilbert sets are nonempty.*

The main examples of Hilbertian fields are global fields and functions fields of several variables over infinite fields. Moreover, any finitely generated field extension of a Hilbertian field remains Hilbertian. For details on Hilbertian fields see [FJ].

2 Profinite structures interpretable in SCF_e

2.1 Additive and multiplicative types

We define and investigate additive and multiplicative types. In the next subsection these notions will allow us to interpret each profinite structure in SCF_e in a special way. It is worth noticing that our notion of additive types is different from that in [BD], where an additive type is the generic type of a connected type-definable subgroup of the additive group.

Let K be a monster model of SCF_e and F be a subset of K.

Definition 2.1.1 *We say that a non-algebraic type $p \in S_1(F)$ is additive [multiplicative] if for every $a \models p$ and for every $n \in \omega$, $(a + K^{p^n}) \cap acl(F) \neq \emptyset$ [$(a \cdot K^{p^n}) \cap acl(F) \neq \emptyset$, respectively].*

Our first aim is to understand the additive and multiplicative types in terms of their tree of coordinates.

Recall that for a set $\mathcal{B} = \{b_s : s \in S\}$, a p-monomial over $\mathcal{B}$ is a monomial $\prod_{s \in S} b_s^{f(s)}$, where $f \in p^S$ is a function with finite support. In Proposition 2.1.2, 1^j denotes the sequence of length j whose elements are equal to the trivial monomial 1.

Proposition 2.1.2 *Assume $\mathcal{B}$ is a p-basis of $dcl(F)$ (the named p-basis when $e < \infty$) and $tp(a/F)$ is non-algebraic. Let I be the set of all p-monomials over $\mathcal{B}$ (so $1 \in I$).*
(i) The type $tp(a/F)$ is additive iff $a \in K^{p^n}(\mathcal{B})$ for each $n \in \omega$ and in the tree $(a_\eta)_{\eta \in I^{<\omega}}$ of coordinates of a with respect to $\mathcal{B}$ the elements $a_{1^j i}$, $j \geq 0, i \in I \setminus \{1\}$, belong to $acl(F)$ (equivalently, $a_\eta \in acl(F)$ for $\eta \neq 1^j$).

(ii) The type $tp(a/F)$ is multiplicative iff $a \in K^{p^n}(\mathcal{B})$ for each $n \in \omega$ and in the tree $(a_\eta)_{\eta \in I^{<\omega}}$ of coordinates of a with respect to $\mathcal{B}$ the elements $a_{1^j i} a^{-1}_{1^{j+1}}$, $j \geq 0, i \in I \backslash \{1\}$, belong to $acl(F)$.

Proof. $(\leftarrow)$ is obvious.
$(\rightarrow)$ By Definition 2.1.1 we have that for any $n \in \omega$ there is a $c_n \in acl(F)$ such that $a - c_n \in K^{p^n}$ [$ac_n^{-1} \in K^{p^n}$, in the multiplicative case]. Since each $c_n \in K^{p^n}(\mathcal{B})$, we get that $a \in K^{p^n}(\mathcal{B})$ for $n \in \omega$.

Suppose now for a contradiction that for some $j \geq 0$ and $i \in I \setminus \{1\}$ we have $a_{1^j i} \notin acl(F)$ [$a_{1^j i} a^{-1}_{1^{j+1}} \notin acl(F)$, respectively]. Then $a_{1^j i}$ [$a_{1^j i} a^{-1}_{1^{j+1}}$, respectively] has an infinite orbit under the action of $Aut(K/F)$. Moreover, for $f, g \in Aut(K/F)$ such that $f(a_{1^j i}) \neq g(a_{1^j i})$ [$f(a_{1^j i} a^{-1}_{1^{j+1}}) \neq g(a_{1^j i} a^{-1}_{1^{j+1}})$, respectively] we have that $f(a) - g(a) \notin K^{p^{j+1}}$ [$f(a)g(a)^{-1} \notin K^{p^{j+1}}$, in the multiplicative case]. Hence $a + K^{p^{j+1}}$ [$aK^{p^{j+1}}$, respectively] has an infinite orbit under the action of $Aut(K/F)$, a contradiction. ■

We have the following easy remark.

Remark 2.1.3 *Let $p \in S_1(F)$ and $a \models p$. Then p is additive [multiplicative] iff there is a sequence $(b_0, b_1, \dots) \subseteq acl(F)$ such that for every $i \in \omega$ we have $a - b_0 - b_1^p - \dots - b_i^{p^i} \in K^{p^{i+1}}$ [$ab_0^{-1} b_1^{-p} \dots b_i^{-p^i} \in K^{p^{i+1}}$, respectively].*

We can show something stronger.

Proposition 2.1.4 *For each additive [multiplicative] type $p = tp(a/F)$, there is a sequence $\overline{b} = (b_0, b_1, \dots) \subseteq acl(F)$ as in Remark 2.1.3, which is a name of $stp(a/F)$ over F, meaning that each automorphism over F fixes $\overline{b}$ iff it fixes $stp(a/F)$.*

Proof. Take the tree of coordinates of a as in Proposition 2.1.2. For any $j \in \omega$ we define $b_j = a_{1^j} - a^p_{1^{j+1}} \in acl(F)$ [$b_j = a_{1^j} a^{-p}_{1^{j+1}} \in acl(F)$, respectively], where we put $a_{1^0} = a$. Let us see now that the sequence $(b_j)_{j \in \omega}$ is a name of $stp(a/F)$ over F.

First if an $f \in Aut(K/F)$ fixes $(b_j)_{j \in \omega}$, then it fixes $a + K^{p^\infty}$ [aK^{p^∞}, respectively]. Hence, by minimality of this set ([Pi], Def. 5.1 (iii)) we get that f fixes $stp(a/F)$.

Assume now that an $f \in Aut(K/F)$ fixes $stp(a/F)$. If there was b_j such that $f(b_j) \neq b_j$, then we would get that $a - f(a) \notin K^{p^{j+1}}$ [$af(a)^{-1} \notin K^{p^{j+1}}$, respectively], a contradiction.

In fact we have showed that the sequence $(b_0, \dots, b_j)$ is a name of $a + K^{p^{j+1}}$ [$aK^{p^{j+1}}$, respectively]. ■

Let a coset $a + K^{p^\infty}$ be type-definable over a set A. We say that $q = tp(a/A)$ is a generic type of $a + K^{p^\infty}$ if for some non-forking extension r of q over $A \cup \{a\}$, the translation $-a + r$ is a generic type of K^{p^∞}. By minimality ([Pi], Def. 5.1 (iii)) of K^{p^∞} we get that $stp(a/F)$ is a generic type of the coset $a + K^{p^\infty}$ iff the coset $a + K^{p^\infty}$ is type-definable over $acl^{eq}(F)$ and the type $stp(a/F)$ is non-algebraic. If $a + K^{p^\infty}$ is type-definable over $acl^{eq}(F)$, then $a + K^{p^\infty}$ has a unique generic type over $acl^{eq}(F)$. For the general theory of generic types in stable and simple groups the reader is referred to [Pi], [Po] and [W].

Remark 2.1.5 *If $p \in S_1(F)$ is additive [multiplicative] and $a \models p$, then $stp(a/F)$ is minimal. More precisely, it is the generic type of the coset $a + K^{p^\infty}$ [aK^{p^∞}].*

Proof. By assumption, for each n, the set $a + K^{p^n}$ [aK^{p^n}, respectively] is definable over $acl(F)$, hence the coset $a + K^{p^\infty} = \bigcap_n (a + K^{p^n})$ [aK^{p^∞}, respectively] is type-definable over $acl(F)$. By the definition of additive [multiplicative] type we know that $stp(a/F)$ is non-algebraic. So $stp(a/F)$ is the generic type of $a + K^{p^\infty}$ [$a + K^{p^\infty}$, respectively], hence it is a minimal type. ■

We have some kind of converse of the last remark. However, to show it we need finite elimination of imaginaries for SCF_∞ proven in Proposition 2.2.2.

Proposition 2.1.6 *If $stp(a/F)$ is a generic type of $a + K^{p^\infty}$ [aK^{p^∞}, respectively], then $tp(a/F)$ is additive [multiplicative].*

Proof. Let $\mathcal{B}$ be a p-basis of $dcl(F)$ (the named p-basis when $e < \infty$). It is enough to prove that if $stp(a/F)$ is the generic type of $a + K^{p^\infty}$ [aK^{p^∞}, respectively], then $a \in K^{p^n}(\mathcal{B})$ for each $n \in \omega$ and the tree of coordinates of a with respect to $\mathcal{B}$ is described as in Proposition 2.1.2 (i) [(ii)].

Let us concentrate on the additive case (the multiplicative case is similar). So assume that $stp(a/F)$ is the generic type of $a + K^{p^\infty}$. Hence $a + K^{p^\infty}$ is type-definable over $acl^{eq}(F)$, so for each $n \in \omega$ we have that $a + K^{p^n}$ is definable over $acl^{eq}(F)$. Therefore, by elimination of imaginaries for $e < \infty$ and finite elimination of imaginaries for $e = \infty$ (Proposition 2.2.2), we get that for each $n \in \omega$ the coset $a + K^{p^n}$ is definable over $acl(F)$. Thus if we show that $a \in K^{p^n}(\mathcal{B})$ for every $n \in \omega$, then the same argument as in the proof of Proposition 2.1.2 shows that the tree of coordinates of a with respect to $\mathcal{B}$ satisfies our demands.

So it remains to prove that $a \in K^{p^n}(\mathcal{B})$ for all $n \in \omega$. For $e < \infty$ there is nothing to do. For $e = \infty$, by induction on n, we will show that $a \in K^{p^n}(\mathcal{B})$, $n \in \omega$, and the tree of coordinates of a with respect to $\mathcal{B}$ restricted to the level n satisfies our demands (i.e. $a_{1^j i} \in acl(F)$ for $j \in \{0, \dots, n-1\}$ and $i \in I \setminus \{1\}$). Assume that our statement holds for an $n \in \omega$. If we show that $a_{1^n} \in K^p(\mathcal{B})$, then the proof will be finished (the rest follows as in the proof of Proposition 2.1.2). By induction hypothesis and the fact that $a \notin acl(F)$ we get that $a_{1^n} \notin acl(F)$. Suppose for a contradiction that a_{1^n} is p-independent over $\mathcal{B}$. Take an infinite set A, which is p-independent over $\mathcal{B}$. Then $A \cap acl(F) = \emptyset$. Take an $a' \in A$. Arguing similarly as in the proof of Lemma 1.2.2 we get that there is an $f_{a'} \in Aut(K/acl(F))$ such that $f_{a'}(a_{1^n}) = a'$. Then for any two distinct elements $a', a'' \in A$ we have $f_{a'}(a) - f_{a''}(a) \notin K^{p^{n+1}}$. Hence $a + K^{p^{n+1}}$ has an infinite orbit under the action of $Aut(K/acl(F))$, a contradiction. ■

Corollary 2.1.7 *A non-algebraic type $p \in S_1(F)$ is additive [multiplicative] iff for every $a \models p$ and for every $n \in \omega$, $a + K^{p^n}$ [$a \cdot K^{p^n}$, respectively] is definable over $acl(F)$.*

Proof. ($\rightarrow$) is obvious.
($\leftarrow$) By assumptions we know that $stp(a/F)$ is non-algebraic and $a + K^{p^\infty} = \bigcap_n (a+$

K^{p^n}) [aK^{p^∞}, repectively] is type-definable over $acl(F)$. So $stp(a/F)$ is the generic type of $a + K^{p^\infty}$ [aK^{p^∞}, respectively], and we finish by Proposition 2.1.6. ■

2.2 Interpretability

Let K be a monster model of SCF_e and $F \subseteq K$ be countable. Of course profinite structures interpretable in SCF_e over F are the same as those interpretable over $dcl(F)$. So w.l.o.g. we can assume that $F = dcl(F)$. In fact we assume even less, namely, that F is a countable field such that $acl(F)$ is an algebraic normal extension of F and if $e < \infty$, then the named Ershov basis is contained in F. At the end of this section we explain why we work under such assumptions. For simplicity one can think that $F = dcl(F)$.

Our main goal in Section 2 is the following theorem.

Theorem 2.2.1 *A profinite structure is interpretable in $SCF_{p,e}$ over F iff it is weakly interpretable in ACF_p over F.*

When $e < \infty$ the direction $(\rightarrow)$ is easy, since we have elimination of imaginaries. The hardest case in the proof of Theorem 2.2.1 is when $e = \infty$. Then we do not have full elimination of imaginaries, instead we show finite elimination of imaginaries, which suffices to prove Theorem 2.2.1.

The proof of Theorem 2.2.1 will be given later. First we show finite elimination of imaginaries in SCF_∞. Then, in Proposition 2.2.4, we treat separably the special case, where the profinite structure in question is the trace of a type over F. After the proof of Theorem 2.2.1 we interpret profinite structures in SCF_e as traces of additive and multiplicative types.

Proposition 2.2.2 *SCF_∞ has finite elimination of imaginaries.*

Proof. It is obvious that in the definition of finite elimination of imaginaries we can assume that $F = dcl(F)$. Let $p \in S(acl^{eq}(F))$.

Claim $p \restriction acl(F) \vdash p$.

Proof of Claim. First notice that if a p-basis of F is infinite, then $acl(F) = \overline{F}^{sep} \prec K$, hence we get what we need. In the general case we proceed in a similar way. Take $c \models p$. We need to show that for $c' \equiv_{acl(F)} c$ we have $c' \equiv_{acl^{eq}(F)} c$. So it is enough to show that

(∗) if $c' \equiv_{acl(F)} c$, then there exists $M \prec K$ containing F and such that $c' \equiv_M c$.

Let $f \in Aut(K/acl(F))$ be such that $f(c) = c'$. Denote $acl(F)$ by $\hat{F}$. Let $F_1 = dcl(\hat{F}c)$ and $F_2 = dcl(\hat{F}c')$. Using the compactness theorem we can choose $\{e_i\}_{i\in\omega}$ p-independent and algebraically independent over $\hat{F}F_1F_2$. By Lemma 1.2.2 we have that $F' := \hat{F}(e_i : i \in \omega)$ is dcl-closed. Hence $acl(F') = \overline{F'}^{sep}$ and we denote this field by $\hat{F}'$. We have also that

$$F_1F_2 \mid_{\hat{F}} \hat{F}'.$$

On the other hand, since the field extension $\hat{F} \subseteq \hat{F'}$ is separable and $\hat{F}$ is algebraically closed in $\hat{F'}$, we have that $\hat{F'}$ is a regular extension of $\hat{F}$. Therefore,

$$(\dagger) \quad F_1F_2 \,\|_{\hat{F}}\, \hat{F'}.$$

Consider $f\restriction F_1 : F_1 \to F_2$ and $id\restriction\hat{F'} : \hat{F'} \to \hat{F'}$. We get the natural ring isomorphism

$$f\restriction F_1 \otimes id\restriction\hat{F'} : F_1 \otimes_{\hat{F}} \hat{F'} \to F_2 \otimes_{\hat{F}} \hat{F'}.$$

From $(\dagger)$ we have the natural isomorphisms between the field of fractions of $F_i \otimes_{\hat{F}} \hat{F'}$ and $F_i\hat{F'}$, $i = 1, 2$. Hence we obtain the natural isomorphism $g : F_1\hat{F'} \to F_2\hat{F'}$ extending $f\restriction F_1$ and $id\restriction\hat{F'}$ (see also [FJ], Lemma 9.4).

On the other hand, by Lemma 1.2.2, we conclude that $F_1(e_i : i \in \omega)$ and $F_2(e_i : i \in \omega)$ are dcl-closed. Hence $K_1 := F_1\hat{F'}$ and $K_2 := F_2\hat{F'}$ are also dcl-closed. This implies that $\hat{K_1} := \overline{K_1}^{sep} = acl(K_1)$ and $\hat{K_2} := \overline{K_2}^{sep} = acl(K_2)$. Thus we can extend our g to an isomorphism between $\hat{K_1}$ and $\hat{K_2}$. But $\hat{K_i} \prec K$ for $i = 1, 2$, so g is an elementary map and we can extend it to an isomorphism of K. On the other hand, $c \in K_1$ and $g(c) = c'$. Therefore $c \equiv_{\hat{F'}} c'$. The proof of the claim is completed because $\hat{F'} \prec K$. $\square$

Now we turn to the proof of Proposition 2.2.2. Let E be a finite equivalence relation definable over F and $a \in K$. By the claim we get a tuple $\overline{a} \in acl(F)$ and a formula $\phi(x, \overline{a}) \in tp(a/acl(F))$ such that $\phi(x, \overline{a}) \vdash E(x, a)$. Then for all $f \in Aut(K/F)$ we have $\phi(x, f(\overline{a})) \vdash E(x, f(a))$. Let

$$S = \{\overline{c} \in acl(F) : (\exists f \in Aut(K/F))(f(\overline{a}) = \overline{c} \text{ and } E(a, f(a))\}.$$

We will prove that

$$(**) \qquad (\forall f \in Aut(K/F))(f[S] = S \iff f(a/E) = a/E).$$

$(\leftarrow)$ Assume that $f(a/E) = a/E$. Then $E(a, f(a))$. Let $\overline{c} \in S$. Then $\overline{c} = h(\overline{a})$ for some $h \in Aut(K/F)$ such that $E(a, h(a))$. We have $\phi(x, h(\overline{a})) \vdash E(x, h(a)) \equiv E(x, a)$. Hence $\phi(x, f(\overline{c})) \vdash E(x, f(a)) \equiv E(x, a)$. On the other hand, $\phi(x, f(\overline{c})) \vdash E(x, f(h(a)))$. Therefore $E(a, f(h(a)))$. This means that $f(\overline{c}) \in S$.

$(\rightarrow)$ Assume that $f[S] = S$. This means that $f(\overline{a}) = g(\overline{a})$ for some $g \in Aut(K/F)$ such that $E(a, g(a))$. Since $g^{-1}(f(\overline{a})) = \overline{a}$, we have that $\phi(x, \overline{a}) \vdash E(x, g^{-1}(f(a)))$. On the other hand, we know that $\phi(x, \overline{a}) \vdash E(x, a)$, so $E(a, g^{-1}(f(a)))$. Hence $E(g(a), f(a))$. Finally we get that $E(a, f(a))$, so $f(a/E) = a/E$.

By $(**)$ it is enough to find a $b \in acl(F)$ such that for each $f \in Aut(K/F)$ we have $f(b) = b \iff f[S] = S$. This is standard ([MMP], page 148). Let $S = \{\overline{a}^1, \ldots, \overline{a}^m\}$, where $\overline{a}^i = (a_{i1}, \ldots, a_{in})$. Take $W \in K[y, x_1, \ldots, x_n]$ defined by

$$W(y, x_1, \ldots, x_n) = \prod_{i=1}^{m}(y + a_{i1}x_1 + \ldots + a_{in}x_n).$$

By Lemma 1.2.2 (ii) we now that the group of automorphisms of $acl(F)$ induced by $Aut(K/F)$ is equal to $Gal(acl(F)/F)$. Therefore we see that the coefficients of W form an appropriate tuple b. Since $acl(F) = \overline{F}^{sep}$, we can replace our tuple $b \in acl(F)$ by a single element. ■

Corollary 2.2.3 *In SCF_∞ every strong type p over a subset F of K has a name $\overline{b} \in acl(F)^\omega$ over F, i.e. for every $f \in Aut(K/F)$ we have that $f(p) = p \iff f(\overline{b}) = \overline{b}$.*

Below we take F as at the beginning of this subsection. Hence for every $\overline{b} \in acl(F)^\omega$ we have that $T_{\overline{b}} \subseteq acl(F)^\omega$, where $T_{\overline{b}}$ is the orbit of $\overline{b}$ under the action of $Gal(\overline{F}/F)$. In spite of the fact that the next proposition is not necessary to prove Theorem 2.2.1, it allows us to understand better the relation between interpretability and weak interpretability. This proposition together with Corollary 2.2.3 show that every profinite structure interpretable in SCF_e as the trace of a complete type over F is weakly interpretable in ACF_p over F.

Proposition 2.2.4 *Let $p = tp(a/F)$. If $\overline{b} \in acl(F)^\omega$ is a name of $stp(a/F)$, then $(Tr(p), Aut(K/F) \restriction Tr(p)) \cong (T_{\overline{b}}, Gal(T_{\overline{b}}/F))$.*

Proof. We define a map $f : T_{\overline{b}} \to Tr(p)$ in the following way. Every field theoretic automorphism of $T_{\overline{b}}$ over F can be extended to an automorphism of $acl(F)$ and then, using Lemma 1.2.2 (ii), to an automorphism of K. So each $\overline{c} \in T_{\overline{b}}$ can be written as $h(\overline{b})$ for an $h \in Aut(K/F)$. For such a $\overline{c}$ we put $f(\overline{c}) = h(stp(a/F))$. By the assumption this definition does not depend on the choice of h and the map f is a bijection.

By the above discussion about extending automorphisms we see that the pullback function $f^* : Aut(K/F) \restriction Tr(p) \to Gal(T_{\overline{b}}/F)$ is an isomorphism of groups.

To see that f is a homeomorphism take in $T_{\overline{b}}$ a basic closed set $U = \{\eta \in T_{\overline{b}} : \eta \restriction n = \overline{c} \restriction n\}$, where $\overline{c} = h(\overline{b})$ for some $h \in Aut(K/F)$ and $n \in \omega$. Then

$$f[U] = hAut(K/F\overline{b} \restriction n)(stp(a/F)) = h[Tr(tp(a/F\overline{b} \restriction n)].$$

$Tr(tp(a/F\overline{b} \restriction n)$ is closed, so is $f[U]$. This shows that f^{-1} is continous. Since both spaces $Tr(p)$ and $T_{\overline{b}}$ are compact we get that f is a homeomorphism. ■

Now we turn to the proof of Theorem 2.2.1.

Proof of Theorem 2.2.1. ($\rightarrow$) Let $(X, Aut^*(X))$ be interpretable in SCF_e over F. In virtue of Corollary 1.1.9 it is weakly interpretable in SCF_e over F. By elimination of imaginaries for $e < \infty$, finite elimination of imaginaries for $e = \infty$ and Proposition 1.1.7, w.l.o.g. we can assume that X is an F-type-definable subset of $acl(F)^\omega$ with $Aut^*(X)$ induced by $Aut(K/F)$. On the other hand, by Lemma 1.2.2 (ii) we get that field theoretic automorphisms of $acl(F)$ over F are exactly the ones induced by $Aut(K/F)$. Hence, one can easily conclude that $(X, Aut^*(X))$ is weakly interpretable in ACF_p over F.

($\longleftarrow$) Take a profinite structure $(Y, Aut^*(Y))$ weakly interpretable in ACF_p over F. By Proposition 1.1.7 we can assume that Y is an F-type-definable subset of $\overline{F}^{\omega}$.

Let us observe that we can assume that $F = dcl(F)$ and $Y \subseteq acl(F)^{\omega}$. Namely, using Lemma 1.2.2 (ii) and the assumption that $acl(F)$ is a normal extension of F and if $e < \infty$, then the named Ershov basis is contained in F, we see that $dcl(F)$ is a radical extension of F. Thus $Gal(Y/F) = Gal(Y/dcl(F))$, so Y is weakly interpretable in ACF_p over $dcl(F)$. If we show that Y is interpretable in SCF_e over $dcl(F)$, then it is true also over F. To include Y in $acl(F)^{\omega}$ we use the fact that $\overline{F}$ is a radical extension of $acl(F)$. Namely, we replace each element $(b_0, b_1, \ldots) \in Y$ by $(b_0^{p^{n_0}}, b_1^{p^{n_1}}, \ldots) \in acl(F)$, where numbers n_i are chosen in such a way that for each $(b_0, b_1, \ldots) \in Y$ we have that $b_i^{p^{n_i}} \in acl(F)$.

Now we turn to the main part of the proof. Let $\mathcal{B} = \{e_0, e_1, \ldots\}$ be a p-basis of F (the named p-basis, when $e < \infty$). Hence $\mathcal{B}$ is also a p-basis of $acl(F) = \overline{F}^{sep}$. For $\overline{b} \in Y$ we take $p_{\overline{b}} = stp(a/F)$ for an $a \in K \setminus acl(F)$ whose tree of coordinates in the basis $\mathcal{B}$ arises as follows (Fig. 2):

$$a = a_0^p + b_0^p e_0,\ a_0 = a_1^p + b_1^p e_0,\ a_1 = a_2^p + b_2^p e_0,\ \ldots$$

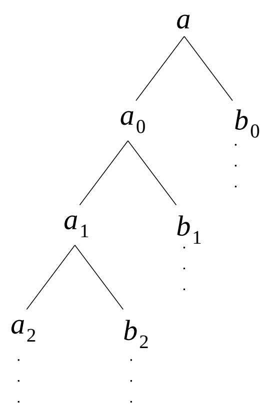


Figure 2

Of course the tree of coordinates of each b_i is contained in the field $F(b_i)$. Observe that the above conditions determine the field theoretic isomorphism type over $acl(F)$ of the tree of coordinates of a with respect to $\mathcal{B}$. Hence, by Fact 1.2.1 (7), we get that $tp(a/acl(F))$ does not depend on the choice of a. This together with Proposition 2.2.2 for $e = \infty$ and elimination of imaginaries for $e < \infty$ imply that also $p_{\overline{b}} = tp(a/acl^{eq}(F))$ does not depend on the choice of a.

Let

$$X = \{p_{\overline{b}} : \overline{b} \in Y\}.$$

It is quite easy that X is a closed subspace of $S_1(acl^{eq}(F))$ invariant under $Aut(K/F)$. So $(X, Aut(K/F) \restriction X)$ is a profinite structure interpretable in SCF_e over F. More precisely, it is interpretable as a union of traces of complete types over F. Our aim is to show that

$$(Y, Aut^*(Y)) \cong (X, Aut^*(X)).$$

We define a map $f : Y \to X$ by $f(\overline{b}) = p_{\overline{b}}$. By Fact 1.2.1 (7) we get that f is an injection, hence it is a bijection. Continuity of f is easy. The fact that the pullback function $f^* : Aut(K/F) \upharpoonright X \to Gal(Y/F)$ is an isomorphism follows from the fact that every element of $Gal(Y/F)$ can be extended to an automorphism from $Aut(K/F)$. This completes our proof. ∎

Let us notice that the proof of $(\to)$ in Theorem 2.2.1 can be done more directly. Namely, using functions obtained by Proposition 1.1.4, we can eliminate imaginary coordinates of elements of a profinite structure $(X, Aut^*(X))$ interpretable in SCF_e over F. Then, using Lemma 1.2.2 (ii), we conclude that a profinite structure obtained in this way is weakly interpretable in ACF_p over F.

In the following two results F is an arbitrary countable subset of K.

Corollary 2.2.5 *For a profinite structure X the following three conditions are equivalent.*
(i) X is interpretable in SCF_e over F.
(ii) X is weakly interpretable in SCF_e over F.
(iii) X is weakly interpretable in SCF_e in the home sort, i.e. $(X, Aut^*(X)) \cong (Y, Aut^*(Y))$, where $Y \subseteq acl(F)^\omega$ is F-type-definable and $Aut^*(Y) = Aut(K/F) \upharpoonright Y$.

Proof. $(i) \to (ii)$ follows from Corollary 1.1.9.
By Proposition 1.1.7 we get $(ii) \leftrightarrow (iii)$.
$(iii) \to (i)$ Take a Y as in (iii). First we have that $Aut(K/F) \upharpoonright Y = Aut(K/dcl(F)) \upharpoonright Y$, so we can assume that $F = dcl(F)$. By Lemma 1.2.2 (ii) we get that $Aut^*(Y) = Gal(Y/F)$, hence $(Y, Aut^*(Y))$ is weakly interpretable in ACF_p over F. So by Theorem 2.2.1 it is interpretable in SCF_e over F. ∎

Proposition 2.2.6 *Each profinite structure Y interpretable in SCF_e over F is interpretable as a union of traces of additive [multiplicative] types over F. In particular if Y is homogeneous, then it is intepretable as a trace of a single additive [multiplicative] type over F.*

Proof. W.l.o.g. we can assume that $F = dcl(F)$. By Theorem 2.2.1 we have that Y is weakly interpretable in ACF_p over F. As at the beginning of the proof of $(\leftarrow)$ in Theorem 2.2.1 we can assume that $Y \subseteq acl(F)^\omega$.

In the additive case the profinite structure X obtained in the proof of $(\leftarrow)$ in Theorem 2.2.1 is of course a union of traces of additive types.

In the multiplicative case we repeat this proof, modyfying the definition of $p_{\overline{b}}$. Namely, for a $\overline{b} \in Y$ we put $p_{\overline{b}} = stp(a/F)$, where the tree of coordinates (in a p-basis $\mathcal{B}$ of F) of an $a \in K \setminus acl(F)$ is determined by (Fig. 3):

$$a = a_0^p + a_0^p b_0^p e_0,\ a_0 = a_1^p + a_1^p b_1^p e_0,\ a_1 = a_2^p + a_2^p b_2^p e_0,\ \ldots ∎$$

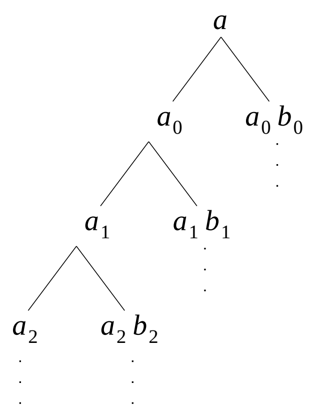


Figure 3

Remark 2.2.7 *Let $Y \subseteq acl(F)^\omega$ be a profinite structure weakly interpretable in ACF_p over F. The proof of the above proposition gives a very simple algorithm for interpreting Y in SCF_e over F as a union of traces of additive [multiplicative] types over F.*

Denote by ($\diamondsuit$) our assumption that $F \subseteq acl(F)$ is a normal field extension and if $e < \infty$, then F contains the named Ershov basis.

At the end of this section we explain why in Theorem 2.2.1 we consider the more general situation ($\diamondsuit$) and not only the case of $F = dcl(F)$. In fact a profinite structure is interpretable in SCF_e over F iff it is interpretable in SCF_e over $dcl(F)$, and ($\diamondsuit$) implies that $F \subseteq dcl(F)$ is radical, so a profinite structure is weakly interpretable in ACF_p over F iff it is weakly interpretable in ACF_p over $dcl(F)$. So if we have Theorem 2.2.1 for $F = dcl(F)$, we have it also for each F satisfying ($\diamondsuit$). So why do we formulate Theorem 2.2.1 for F satisfying ($\diamondsuit$)?

The answer is simple. We want to interpret many profinite structures in SCF_e over an F for each $e \in \omega \cup \{\infty\}$. By Theorem 2.2.1, ($\diamondsuit$) implies that it is enough to interpret profinite structures in ACF_p over F in the weak sense. As we will see in the last section, it is nice to do this over some special fields F, e.g. over the field of rational functions (over F_p) on finitely or infinitely many variables. It is not true that for each e every such field F is dcl-closed in some model K of SCF_e, whereas we have the following remark.

Remark 2.2.8 *For each field F of characteristic p with Ershov invariant e' and for each $e \in \omega \cup \{\infty\}$ such that $e' \geq e$ or $e = \infty$, there is a model K of SCF_e containing F and such that $acl(F)$ is a normal extension of F and if $e < \infty$, then F contains the named Ershov basis of K.*

Proof. There are two cases.
Case 1 $\infty = e > e'$. e' is finite, so let $a_0, \ldots, a_{e'-1}$ be a p-basis of F. Take X, a set

of ω-many variables. Then a p-basis of the field $F(X)$ of rational functions equals $\{a_i : i < e'\} \cup X$. Let $K = \overline{F(X)}^{sep}$. We see that $K \models SCF_e$. Moreover, since a p-basis of F is still p-independent in K, we have $F = dcl(F)$ and in particular $F \subseteq acl(F)$ is normal.

Case 2 $e \leq e'$. If $e = e'$, then $K = \overline{F}^{sep}$ satisfies our demands. Otherwise write a p-basis of F in the form $\{a_0, \ldots, a_{e-1}\} \cup \mathcal{B}$, where $\mathcal{B}$ consists of $(e'-e)$-many [ω-many, if $e' = \infty$] elements. Let $\mathcal{B}^{1/p^\infty} = \{b^{1/p^n} : b \in \mathcal{B}, n \in \omega\}$. If we put $K = \overline{F(\mathcal{B}^{1/p^\infty})}^{sep}$, then $K \models SCF_e$ because, as it is easy to see, a p-basis of K equals $\{a_0, \ldots, a_{e-1}\}$. Moreover, $acl(F) = K$ is a normal extension of F and we have $(\diamondsuit)$. ■

This remark gives us an algorithm for finding $K \models SCF_e$ containing F and satisfying $(\diamondsuit)$.

Notice that in the case when the Ershov invariant e' of F is less than e and $e < \infty$, taking a set X of $(e - e')$-many variables we get the field $F(X)$ of rational functions over F and, as in the proof of Remark 2.2.8, we see that a p-basis of $F(X)$ has e elements. Hence, adding to the language names for elements of a Ershov basis of $F(X)$ being a union of the set X and a Ershov basis of F, we obtain $K := \overline{F(X)}^{sep} \models SCF_e$. But in this case the extension $F \subseteq acl(F)$ is not even algebraic. However, if we have a profinite structure weakly interpretable in ACF_p over F, then it is also weakly interpretable over $F(X)$. Since $F(X)$ is dcl-closed in K, we get that our profinite structure is interpretable in SCF_e over $F(X)$, hence also over F.

3 Connection with the inverse Galois problem

Despite the fact that from the point of view of this paper we need the field theoretic version of Theorem 3.1, we formulate it in a general context of an arbitrary theory. To do this we recall that in an arbitrary complete theory T we can develop Galois theory for subsets of a monster model $\mathfrak{C}$ of T.

Let $K \subseteq L$ be subsets of $\mathfrak{C}^{eq}$. We say that the extension $K \subseteq L$ is Galois if $K = dcl^{eq}(K)$, $L = dcl^{eq}(L)$, $L \subseteq acl^{eq}(K)$ and L is invariant under $Aut(\mathfrak{C}/K)$. We define $Gal(L/K) = \{g \restriction L : g \in Aut(\mathfrak{C}/K)\}$. $Gal(L/K)$ is a profinite group with natural topology. Namely, it is the inverse limit of the system of all finite groups $Gal(M/K)$ with M ranging over all Galois extensions $K \subseteq M$ such that $M = dcl^{eq}(K, A)$ with A being a finite subset of L. If L is invariant under a subgroup G of $Aut(\mathfrak{C})$, then by L^G or $L^{G\restriction L}$ we denote the set of elements of L fixed by G.

It is easy to show that a dcl^{eq}-closed set L is a Galois extension of K iff $L \subseteq acl^{eq}(K)$ and there is a subgroup G of $Aut(\mathfrak{C}/K)$ such that L is invariant under G and $K = L^G$.

For a Galois extension $K \subseteq L$ the Galois theorem (i.e. the Galois correspondence between dcl^{eq}-closed sets M, such that $K \subseteq M \subseteq L$ and closed subgroups of $Gal(L/K)$) remains true. The proof of this fact is an adaptation of a proof of classical Galois theorem for fields ([FJ], Proposition 1.8).

Notice that in the case of $T = ACF_p$ this general notion of Galois extension is a little bit different from the classical field theoretic one. However, they are closely related. For a set K in $\mathfrak{C}^{eq}$ by K_h we denote the set of elements of K of the home sort. If $K \subseteq L$ is a Galois extension in the general sense, then $K_h \subseteq L \cap \overline{K_h}^{sep}$ is a field theoretic Galois extension and the Galois group $Gal(L/K)$ in the general sense is isomorphic to the Galois group $Gal(L \cap \overline{K_h}^{sep}/K_h)$ in the usual field theoretic sense. On the other hand, if $K \subseteq L$ is a field theoretic Galois extension, then $dcl^{eq}(K) \subseteq dcl^{eq}(L)$ is a Galois extension in the general sense and $Gal(L/K)$ is isomorphic to the Galois group $Gal(dcl^{eq}(L)/dcl^{eq}(K))$ in the general sense. This justifies our terminology.

Let T be an arbitrary complete theory.

Theorem 3.1 *A profinite structure $(X, Aut^*(X))$ is weakly interpretable in ACF_p over a field F [in T over a dcl^{eq}-closed set F, respectively] iff there is a Galois extension $F \subseteq L$ such that $Gal(L/F) \cong Aut^*(X)$, where $\cong$ is an isomorphism of topological groups.*

Before we start the proof notice that we can formulate Theorem 3.1 equivalently skipping the assumption that F is a field [dcl^{eq}-closed set] and claiming in the second part that there is an extension $L \subseteq acl(F)$ [$L \subseteq acl^{eq}(F)$] of F invariant under the action of $Aut(\mathfrak{C}/F)$ such that $Gal(L/F) \cong Aut^*(X)$.

Proof of Theorem 3.1. ($\rightarrow$) is easy. Let $X \subseteq acl^{eq}(F)^\omega$ be an F-type-definable set and X' the set of all coordinates of elements of X. Then $L = dcl^{eq}(F, X')$ works in the general case. In the field theoretic case, by Remark 1.1.7, we can assume that $X \subseteq acl(F)^\omega$ and we define $L = \overline{F}^{sep} \cap F(X')$.

($\leftarrow$) During the proof we concentrate on the field theoretic case. At some point of the proof we will give a hint on how to modify the proof in the general case. Moreover, we assume that $(X, Aut^*(X))$ is homogeneous (see Section 1.1). The non-homogeneous case will be discussed at the end of this proof.

Denote by G the structural group $Aut^*(X)$. Let

$$X = \varprojlim X_i$$

with connecting functions $f_{ij} : X_i \rightarrow X_j$ for $i > j$. Let

$$G_i = G/N_i,$$

where $N_i = \{g \in G : g \restriction X_i = id\}$ is a clopen normal subgroup of G. Then $G_i \cong G \restriction X_i$ and

$$G \cong \varprojlim G_i.$$

Let $x \in X$ and x_i be the i-th coordinate of x. The group $G_i \cong G \restriction X_i$ acts naturally on X_i. Let $H_i = Stab_{G_i}(x_i)$. As we assumed that X is homogeneous, so is (X_i, G_i) and by Remark 1.1.2 we get that $(G_i/H_i, G_i) \cong (X_i, G_i)$, where G_i acts on G_i/H_i by the left multiplication. This isomorphism is a pair (f_i, id), where

$f_i : G_i/H_i \to X_i$ is defined by $f_i(gH_i) = gx_i$ for $g \in G_i$ and $id : G_i \to G_i$ is the identity map.

We define a new profinite structure

$$(Y, Aut^*(Y)) = (\varprojlim G_i/H_i, \varprojlim G_i),$$

where $g_{ij} : G_i \to G_j$ and $h_{ij} : G_i/H_i \to G_j/H_j$, $i > j$, are defined naturally. For every $i > j$ we have

$$f_j h_{ij} = f_{ij} f_i,$$

so

$$(*) \qquad (Y, Aut^*(Y)) \cong (X, Aut^*(X)).$$

By the assumption we have a Galois extension $F \subseteq L$ such that $Gal(L/F) \cong G$. We identify these two groups by this isomorphism. Hence we obtain a sequence

$$F \subseteq L^{N_0} \subseteq L^{N_1} \subseteq \ldots \subseteq L$$

of Galois extensions of F. It is easy to check that $L = \bigcup_{i\in\omega} L^{N_i}$. Moreover, $Gal(L/L^{N_i}) = N_i$ and $Gal(L^{N_i}/F) \cong G_i$.

Since $F \subseteq L^{N_i}$ is Galois, for each $i \in \omega$ we can find a $c_i \in L$ such that $L^{N_i} = F(c_i)$.

Hint For an arbitrary theory T, for each $i \in \omega$, we choose a finite sequence c_i of imaginary elements from L^{N_i} such that $L^{N_i} = dcl_F^{eq}(c_i)$.

Now in both the field theoretic and the general case we proceed as follows.

Let $Z_i = \{gc_i : g \in G\}$. Then G_i acts on Z_i ($(gN_i)c = gc$ for $g \in G$ and $c \in Z_i$). This action is faithful and $(Z_i, G_i) \cong (Z_i, G\restriction Z_i)$. Moreover, $Stab_{G_i}(c_i) = \{id\}$.

On Z_i we define an equivalence relation E_i by

$$E_i(gc_i, hc_i) \iff gH_i = hH_i \text{ for } g, h \in G_i.$$

Classes of E_i are of the form gH_ic_i for $g \in G_i$. G_i acts transitively on Z_i/E_i ($g(hH_ic_i) = (gh)H_ic_i$ for $g, h \in G_i$). We see that $Stab_{G_i}(H_ic_i) = H_i$, so by Remark 1.1.2 we obtain an isomorphism $(G_i/H_i, G_i) \cong (Z_i/E_i, G_i)$, given by the bijection $f'_i : G_i/H_i \to Z_i/E_i$ ($f'(gH_i) = gH_ic_i$ for $g \in G_i$) and the identity map $id : G_i \to G_i$.

Notice that as G_i acts faithfully on X_i, so it does on G_i/H_i, too, and finally it acts faithfully on Z_i/E_i.

We define a profinite structure

$$(Z, Aut^*(Z)) = (\varprojlim Z_i/E_i, \varprojlim G_i),$$

where for $i > j$ the connecting map $f'_{ij} : Z_i/E_i \to Z_j/E_j$ is defined by $f'_{ij}(gH_ic_i) = g_{ij}(g)H_jc_j$ for $g \in G_i$.

Then for every $i > j$ we have

$$f'_j h_{ij} = f'_{ij} f'_i,$$

so

$$(**) \qquad (Z, Aut^*(Z)) \cong (Y, Aut^*(Y)).$$

Moreover, $(Z, Aut^*(Z)) = (Z, G) = (Z, Aut(\mathfrak{C}/F)\restriction Z)$, hence this profinite structure is weakly interpretable in T over F. (In fact there is a little problem here. Namely, the relations E_i, $i \in \omega$, are F-definable, so formally Z is an F-type-definable subset of $acl^{eq}(F)^\omega$ counted in the language expanded by constants from F. However, an easy argument (as in the proof of Proposition 1.1.8) shows that we can remove these additional contstants. For ACF_p we can also use elimination of imaginaries and Proposition 1.1.4.)

By $(*)$ and $(**)$ the homogeneous case is completed.

Having the homogeneous case completed, we discuss the modifications of the proof which are necessary in the case of a non-homogeneous structure $(X, Aut^*(X))$.

For each $i \in \omega$ we choose a set of representatives $\{x_{i1}, \ldots, x_{in_i}\}$ of the partition of X_i into orbits under the action of $G\restriction X_i$. We choose it in such a way that for $i > j$ and $k \leq n_i$ we have that $f_{ij}(x_{ik}) = x_{jl}$ for some $l \leq n_j$. Let $H_{ij} = Stab_{G_i}(x_{ij})$. By Remark 1.1.2 we have that $(X_i, G_i) \cong (G_i/H_{i1} \cup \ldots \cup G_i/H_{in_i}, G_i)$, where all actions and functions are natural. Then we define

$$(Y, Aut^*(Y)) = (\varprojlim (G_i/H_{i1} \cup \ldots \cup G_i/H_{in_i}), \varprojlim G_i),$$

where all connecting functions are defined naturally. Similarly as in the homogeneous case we conclude that

$$(*)' \qquad (Y, Aut^*(Y)) \cong (X, Aut^*(X)).$$

Next, on each Z_i we define equivalence relations $E_{i1}, \ldots, E_{in_i}$ by

$$E_{ij}(gc_i, hc_i) \iff gH_{ij} = hH_{ij} \text{ for } g, h \in G_i.$$

In the natural way we define a profinite structure

$$(Z, Aut^*(Z)) = (\varprojlim (Z_i/E_{i1} \cup \ldots \cup Z_i/E_{in_i}), \varprojlim G_i).$$

Similarly as in the homogeneous case we show

$$(**)' \qquad (Z, Aut^*(Z)) \cong (Y, Aut^*(Y)).$$

To finish the proof it is enough to ensure that $(Z, Aut^*(Z))$ is weakly interpretable in ACF_p (in the general case in T) over F. There arises a little problem that on the i-th coordinate in Z we have elements from the disjoint union of sorts $\mathfrak{C}/E'_{i1} \cup \ldots \cup \mathfrak{C}/E'_{in_i}$ (in the language expanded by constants from F), where the relation E'_{ij} on $\mathfrak{C}$ is defined by

$$E'_{ij}(x, y) \iff (x \notin Z_i \wedge y \notin Z_i) \vee (x \in Z_i \wedge y \in Z_i \wedge E_{ij}(x, y)).$$

For ACF_p we can use elimination of imaginaries and Proposition 1.1.4. In the general case we replace Z by

$$Z' = \varprojlim A_i,$$

where

$$\begin{aligned} A_i = \quad & \{(a_1, \ldots, a_n) \in \mathfrak{C}/E'_{i1} \times \ldots \times \mathfrak{C}/E'_{in_i} : \\ & (\exists j \leq n_i)(a_j \in Z_i/E'_{ij} \wedge (\forall k \neq j)(a_k \in (\mathfrak{C} \setminus Z_i)/E'_{ik}))\}. \end{aligned}$$

Connecting maps are obtained here naturally from connecting maps in Z. Now one can check that (Z', G) is weakly interpretable in T over F and

$$(Z', G) \cong (Z, G).$$

So by $(*)'$ and $(**)'$ the proof is completed. ■

The next proposition shows that there is a large class of theories (including the stable ones), which weakly interpret over some special sets all profinite structures.

Proposition 3.2 *Let T be a complete theory with a monster model $\mathfrak{C}$ for which we can find an indiscernible infinite set $I \subseteq \mathfrak{C}$. Then there is a countable set $F \subseteq dcl^{eq}(I)$ such that each profinite structure is weakly interpretable in T over F.*

Proof. W.l.o.g. we can assume that I is a countable infinite indiscernible set. We recall that w.l.o.g. we consider inverse systems with the connecting maps being surjections.

For a profinite structure $(X, Aut^*(X))$ and $n \in \omega$ we have a finite profinite structure $(X_{\leq n}, Aut^*(X) \restriction X_{\leq n})$, where $X_{\leq n}$ is the inverse limit of the finite system $X_0 \longleftarrow \ldots \longleftarrow X_n$.

We say that two profinite structures $(X, Aut^*(X))$ and $(Y, Aut^*(Y))$, treated as inverse limits of distinguished inverse systems $(X_i)_{i\in\omega}$ and $(Y_i)_{i\in\omega}$, are exactly isomorphic if there is an isomorphism between them induced by an isomorphism of systems $(X_i)_{i\in\omega}$ and $(Y_i)_{i\in\omega}$.

For each $n \in \omega$, up to exact isomorphism, there are only countably many finite profinite structures of the form $(X_{\leq n}, Aut^*(X) \restriction X_{\leq n})$. So let

$$S_n = \{(A_{nj}, G_{nj}) : j \in \omega\}$$

be a countable set of representatives of all exact isomorphism classes, where

$$A_{nj} := \varprojlim (X_i^{nj})_{i\leq n}$$

is the inverse limit of a system $X_0^{nj} \longleftarrow \ldots \longleftarrow X_n^{nj}$ of finite spaces. We can choose all S_n in such a way that for $n > m$ and $j \in \omega$ there is an $j(n,j) \in \omega$ such that for all $i \leq m$ we have $X_i^{nj} = X_i^{mj(n,j)}$ and

$$(\varprojlim (X_i^{nj})_{i\leq m}, G_{nj} \restriction (\varprojlim (X_i^{nj})_{i\leq m})) = (A_{mj(n,j)}, G_{mj(n,j)}).$$

Moreover, for each $n_1, n_2, j_1, j_2 \in \omega$ and $i_1 \leq n_1, i_2 \leq n_2$:
(i) if $i_1 \neq i_2$, then $X_{i_1}^{n_1 j_1}$ and $X_{i_2}^{n_2 j_2}$ are disjoint,
(ii) if $j_1 \neq j_2$, then $X_{n_1}^{n_1 j_1}$ and $X_{n_1}^{n_1 j_2}$ are disjoint.

We choose everything so that

$$I = \bigcup_{i,j,n \in \omega,\, i \leq n} X_i^{nj}.$$

We define d_{nj} as a name in $\mathfrak{C}^{eq}$ of the orbit of an $|A_{nj}|$-tuple η of all elements of A_{nj} under the action of G_{nj}.

Since $\eta \in A_{nj}^{|A_{nj}|} \subseteq (I^{n+1})^{|A_{nj}|}$, we have $d_{nj} \in dcl^{eq}(I)$. By indiscernibility of I we have that

$$(A_{nj}, G_{nj}) = (A_{nj}, Aut(\mathfrak{C}/d_{nj}) \restriction A_{nj})$$

and (A_{nj}, G_{nj}) is weakly interpretable in T over $\{d_{nj}\}$.

We define

$$F = \{d_{nj} : n, j \in \omega\}.$$

Then $F \subseteq dcl^{eq}(I)$ is countable. By the choice of S_n, using indiscernibility of I one can check that every profinite structure is weakly interpretable in T over F. ■

Alternatively, we could prove Proposition 3.2 as follows. First we show that for a given profinite structure $(X, Aut^*(X))$ we can find a countable set $F \subseteq acl^{eq}(I)$ over which X is weakly interpretable. This is an easier version of the above proof of Proposition 3.2. Then we apply this to a profinite structure whose structural group is the free profinite group on ω-many free generators. By Theorem 3.1 we see that the set F obtained in this way is appropriate.

The following corollary follows from Proposition 3.2 and elimination of imaginaries in ACF_p.

Corollary 3.3 *For each p there exists a countable field F of characteristic p such that every profinite structure is weakly interpretable in ACF_p over F.*

Alternatively, this corollary follows from Waterhouse theorem ([FJ], Corollary 1.11), which says that every profinite group is the Galois group of a Galois extension of some field. Applying this theorem to the free profinite group on ω-many free generators we obtain a field F (in virtue of the proof of Waterhouse theorem, F can be chosen countable) such that every profinite group, which is the inverse limit of a countable system, is the Galois group of a Galois extension of F. Using this together with Theorem 3.1 we get Corollary 3.3. Conversely, Corollary 3.3 implies Waterhouse theorem for inverse limits of countable systems of finite groups.

Some advanced results from Galois theory [MM] give many fields (e.g. all countable PAC Hilbertian fields) over which we can realise as a Galois group any profinite group (which is the inverse limit of a countable system). Of course each such field satisfies the conclusion of Corollary 3.3.

At the end of this section let us say something about the field F obtained in the proof of Corollary 3.3. By this corollary every profinite structure can be weakly interpreted in ACF_p over F, so one can ask, why in the next section we interpret profinite structures over fields of rational functions instead of over F. One answer is the fact that the field F is rather artificial from number theoretic point of view and it is difficult to construct new explicit examples of profinite structures weakly interpretable over F. The second reason is the connection with the inverse Galois problem. As it was mentioned in the introduction, one of the further ways of considerations can be interpreting profinite structures to get (by Theorem 3.1) new Galois groups over a fixed field. If we take our field F, then each profinite group is the Galois group of some Galois extension of F, so the situation is not interesting.

4 Field theoretic constructions of profinite structures

The goal of this section is to construct profinite structures weakly interpretable in ACF_p over some fields and satisfying various model theoretic properties.

Now we give model theoretic notions which we are going to consider. First recall that a profinite structure X is small if there are only countably many orbits in X over any finite subset of X. By $a, b, \dots$ we denote finite tuples of elements of X and by $A, B, \dots$ finite subsets of X.

For every finite $A, B \subseteq X$ we have that $o(a/AB)$ (AB denotes $A \cup B$) is open or nowhere dense in $o(a/A)$. In a profinite structure X we measure the size of orbits by means of the rank function $\mathcal{M}$.

Definition 4.1 *The rank $\mathcal{M}$ is the function from the collection of orbits over finite sets to the ordinals together with ∞ satisfying*

$$\mathcal{M}(a/A) \geq \alpha + 1 \quad \textit{iff} \quad \begin{array}{l} \textit{there is a finite set } B \supseteq A \textit{ such that} \\ o(a/B) \textit{ is nowhere dense in } o(a/A) \textit{ and } \mathcal{M}(a/B) \geq \alpha. \end{array}$$

X is m-stable if every orbit has ordinal $\mathcal{M}$-rank. Equivalently, there is no infinite sequence $A_1 \subseteq A_2 \subseteq \dots$ of finite subsets of X and $a \in X$ such that $o(a/A_{i+1})$ is nowhere dense in $o(a/A_i)$ for every i. We say that X has $\mathcal{M}$-rank n if the maximum of $\mathcal{M}$-ranks of 1-orbits in X equals n.

Definition 4.2 *A profinite structure X is m-normal if for every finite $a, A \subseteq X$, there is a clopen $U \ni a$, such that $U \cap o(a/A)$ has finitely many conjugates under $Aut^*(X/a)$.*

In the above definition we can choose as U a canonical open set definable over a, where by a canonical open set in

$$X = \varprojlim X_i \subseteq \prod_{i<\omega} X_i$$

we mean the set of elements of X with the i-th coordinate fixed (i is arbitrary). A canonical open set in X^n is a product of canonical open sets in X.

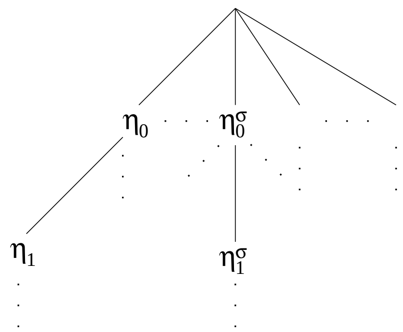
For a finite $A \subseteq X$, by $acl(A)$ we denote the algebraic closure of A, i.e. the set of these elements of X which have finitely many conjugates under $Aut^*(X/A)$. If o is an orbit of $\mathcal{M}$-rank 1, then the operator acl defines a pregeometry on o. We say that o is trivial if this pregeometry is trivial. Similarly, if each 1-orbit in X has $\mathcal{M}$-rank 1 or 0, then acl defines a pregeometry on X and we say that X is trivial if this pregeometry is trivial.

In the introduction it was explained how to consider products of finite groups as profinite structures. The following theorems appear in [Kr1].

Fact 4.3 *Let X be a product of countably many finite abelian groups of bounded exponent with the standard structural group. Then X is small, m-normal and m-stable.*

Fact 4.4 *Let p be a prime number and $X = \prod_{i \in \omega} X_i$, where each X_i is a finite abelian p-group. Let X have finite exponent and S be a Sylow p-subgroup of the standard structural group $Aut^*(X)$. Then (X, S) is small, m-normal and m-stable.*

Recall that for a field F of characteristic p and for an $\eta \in (\overline{F}^{sep})^\omega$ we define T_η as the orbit of η under the action of $Gal(\overline{F}^{sep}/F)$. Then $(T_\eta, Gal(T_\eta/F))$ is a profinite structure weakly interpretable in ACF_p over F (Fig. 4).



$\sigma \in Gal(\overline{F}^{sep}/F)$

Figure 4

In the next proposition F is an arbitrary field.

Proposition 4.5 *(i) If $\eta = (\eta_0, \eta_1, \ldots) \in (\overline{F}^{sep})^\omega$ satisfies $\eta_i \in F(\eta_{i+1})$ for all $i \in \omega$, then*

$$(T_\eta, Gal(T_\eta/F)) = (\varprojlim X_i, Gal(T_\eta/F)),$$

where X_i is the orbit of η_i under the action of $Gal(\overline{F}^{sep}/F)$ and the connecting map $f_{ij} : X_i \to X_j$ is defined by $f_{ij}(\eta_i^\sigma) = \eta_j^\sigma$ for $\sigma \in Gal(\overline{F}^{sep}/F)$.
(ii) If a homogeneous profinite structure $(X, Aut^*(X))$ is weakly interpretable in ACF_p over F, then $(X, Aut^*(X)) \cong (T_\eta, Gal(T_\eta/F))$ for some sequence η satisfying the assumption of (i).

Proof. Only (ii) needs an explanation. By Remark 1.1.7 we can assume that $X \subseteq \overline{F}^{\omega}$ and then taking large enough p-th power of each coordinate of X we can assume $X \subseteq (\overline{F}^{sep})^{\omega}$. Take an $\alpha = (\alpha_0, \alpha_1, \ldots) \in X$. Each extension $F \subseteq F(\alpha_0, \ldots, \alpha_i)$ is separable, so there exists an $\eta_i \in F(\alpha_0, \ldots, \alpha_i)$ such that $F(\eta_i) = F(\alpha_0, \ldots, \alpha_i)$. We take $\eta = (\eta_i)_{i \in \omega}$ and define

$$(Y, Aut^*(Y)) = (T_\eta, Gal(T_\eta/F)).$$

Obviously our η satisfies the assumption of (i). Moreover, for each $i \in \omega$ and $j \leq i$ there is a rational function $R_i^j(x) \in F(x)$ such that $\alpha_j = R_i^j(\eta_i)$. We define a map $f : Y \to X$, putting

$$f(\eta^\sigma) = (\alpha_i^\sigma)_{i \in \omega}$$

for any $\sigma \in Gal(\overline{F}^{sep}/F)$. It is easy to check that f is an isomorphism of profinite structures. ∎

From now on $F = F_p(a_0, a_1, \ldots)$ is the field of rational functions over the prime field F_p on finitely or infinitely many variables, unless it is stated otherwise (sometimes F will be an arbitrary Hilbertian field).

The rest of the paper is devoted to constructing profinite structures weakly interpretable in ACF_p over F and satisfying various model theoretic properties. We will do this using two methods mentioned at the end of the introduction.

Method 1 Direct field theoretic construction.

Method 2 Applying Theorem 3.1 and some more advanced Galois theory.

In the first method we do not have any abstract profinite structure at the beginning. We want to construct a new profinite structure with some model theoretic properties and we do this constructing step-by-step a sequence $\eta = \langle \eta_i \rangle_{i \in \omega}$ of elements $\eta_i \in \overline{F}^{sep}$ and defining our new profinite structure weakly interpretable in ACF_p over F as $(T_\eta, Gal(T_\eta/F))$. The point here is to choose successively elements η_i, $i \in \omega$, so that the orbits (over finite sets) of every initial part $\langle \eta_i \rangle_{i \leq k}$ under the action of $Gal(\overline{F}^{sep}/F)$ satisfy some combinatorial properties which finally give the appropriate model theoretic properties of the arising profinite structure. Using this method we will obtain examples from the list given at the end of the introduction (in the fourth item only the case $n = 1$).

In the second method we have to start from a given profinite structure X which has our required model theoretic properties. Knowing something about the structural group $Aut^*(X)$ of X and using some Galois theory we can sometimes conclude that $Aut^*(X)$ is the Galois group of some Galois extension of F. Then, by Theorem 3.1, we get that X is weakly interpretable in ACF_p over F. This method together with Facts 4.3 and 4.4 yield examples from the fourth item of the list from the end of the itroduction. At the end of the paper we discuss the difference between both methods.

In most of the following constructions we find a sequence $\eta \in (\overline{F}^{sep})^{\omega}$ satisfying assumptions of Proposition 4.5 (i). Then we define a new profinite structure as $(T_\eta, Gal(T_\eta/F))$. By ζ_n we denote a primitive n-th root of 1.

4.1 Example of a not m-normal, not m-stable and not small profinite structure

Method 1. $F = F_p(a_0, a_1, \ldots)$ is the field of rational functions on finitely or infinitely variables (p is a prime number).

Lemma 4.1.1 *There exist separable irreducible polynomials $P_i(x) \in F[x]$, $i \in \omega$, such that*
(i) their decomposition fields K_i, $i \in \omega$, are linearly disjoint over F, i.e. for every $i \in \omega$ we have $K_i \parallel_F K_0 \ldots K_{i-1}$,
(ii) $K_i \neq F(a)$ for any root a of P_i ,
(iii) $K_i = F(a, b)$ for any two distinct roots $a \neq b$ of P_i .
More precisely, we can take $P_i(x) = x^{q_i} - a_0$ for prime numbers q_i such that $q_0 \leq q_1 \leq \ldots$.

Proof. First of all notice that when we have prime numbers q_i satisfying the lemma except of the condition $q_0 \leq q_1 \leq \ldots$, then permuting q_i's we can satisfy this condition, too.

We construct a sequence $(P_i(x))_{i\in\omega}$ by induction on i. For $i = 0$ we take a prime number $q_0 \neq p$ such that $(q, p-1) = 1$ and put $P_0(x) = x^{q_0} - a_0$. By Eisenstein criterion $P_0(x)$ is irreducible over F and $P_0(x) = (x - \sqrt[q_0]{a_0})(x - \zeta_{q_0}\sqrt[q_0]{a_0}) \ldots (x - \zeta_{q_0}^{q_0-1}\sqrt[q_0]{a_0})$, hence we see that $P_0(x)$ satisfies our demands.
Assume now that we have chosen $P_0, \ldots, P_i$. Let $s = [K_0 \ldots K_i : K]$.

Claim 1 *There exist prime numbers r and q such that $(r, s) = (q, s) = (q, p-1) = (q, p) = 1$ and $q \mid p^r - 1$.*

Proof. For a prime number q we define $r_q = min\{r > 0 : q \mid p^r - 1\}$. Then $r_q = 1 \iff q \mid p - 1$. Let $d = \prod\{r_q : q \mid s(p-1), r_q > 1\}$. Take a prime number r such that $(r, s) = (r, d) = (r, p-1) = 1$. We have

$$p^r - 1 = (p-1)(p^{r-1} + \ldots + 1) \equiv (p-1)r \pmod{(p-1)^2}.$$

Hence

$$(p^r - 1, s^2(p-1)^2) = p - 1.$$

Therefore there exists a prime number q such that $(q, s) = (q, p-1) = (q, p) = 1$ and $q \mid p^r - 1$. $\square$

Take r and $q = q_{i+1}$ satisfying Claim 1. We define $P_{i+1}(x) = x^{q_{i+1}} - a_0$. By Eisenstein criterion P_{i+1} is separable and irreducible. K_{i+1} is the field of decomposition of P_{i+1}. For any q-th root $\sqrt[q]{a_0}$ we have that $K_{i+1} = F(\sqrt[q]{a_0}, \zeta_q) \neq F(\sqrt[q]{a_0})$, hence (ii) and (iii) are satisfied. Let $s_1 = [F(\sqrt[q]{a_0}) : F]$ and $s_2 = [F(\zeta_q) : F]$. We have that $F(\sqrt[q]{a_0}) \parallel_F F(\zeta_q)$, so

$$[K_{i+1} : F] = s_1 s_2.$$

Since $s_2 = min\{k : q \mid p^k - 1\}$ and $q \mid p^r - 1$, we have $s_2 \mid r$. But $(q, p-1) = 1$, so $s_2 = r$. On the other hand $s_1 = q$. Hence $(s_1 s_2, s) = 1$ and we conclude that

$K_{i+1} \|_F K_0 \dots K_i$. ■

Take a sequence $\alpha = (\alpha_i)_{i\in\omega}$ of roots of $(P_i(x))_{i\in\omega}$, i.e. $P_i(\alpha_i) = 0$.

We define a profinite structure

$$(X, Aut^*(X)) = (T_\alpha, Gal(T_\alpha/F))$$

and we will show that it is not small, not $m-$normal and not m-stable.

By X_i we denote the set of roots of $P_i(x)$. By Lemma 4.1.1 (i) we get that

$$X = \prod_{i\in\omega} X_i \quad \text{and} \quad Aut^*(X) = \prod_{i\in\omega} Gal(X_i/F),$$

where $\prod_{i\in\omega} Gal(X_i/F)$ acts on X on appropriate coordinates.

Let $d_i = [F(\zeta_{q_i}) : F]$. Fix an element of X, e.g. α. If for an arbitrary i we take an $\alpha'_i \in X_i$ different from α_i, then by Lemma 4.1.1 we have that $K_i = F(\alpha_i, \alpha'_i)$. Lemma 4.1.1 implies the following claim (Fig. 5).

Claim 2 *For an α'_i as above and an arbitrary $\alpha'_{<i} := (\alpha'_0, \dots, \alpha'_{i-1}) \in X_0 \times \dots \times X_{i-1}$ we have:*
(i) $|o(\alpha'_i/K_0 \dots K_{i-1}K_{i+1} \dots (\alpha))| = [F(\alpha_i, \alpha'_i) : F(\alpha_i)] = [F(\zeta_{q_i}) : F] = d_i$,
(ii) $|o(\alpha'_i/K_0 \dots K_{i-1}(\alpha))| = d_i$,
(iii)$|o(\alpha'_i/F(\alpha'_{<i}, \alpha))| = d_i$.
More precisely, we have

$$o := o(\alpha'_i/K_0 \dots K_{i-1}K_{i+1} \dots (\alpha)) = o(\alpha'_i/K_{<i}(\alpha)) = o(\alpha'_i/F(\alpha'_{<i}, \alpha)) = o(\alpha'_i/F(\alpha_i)).$$

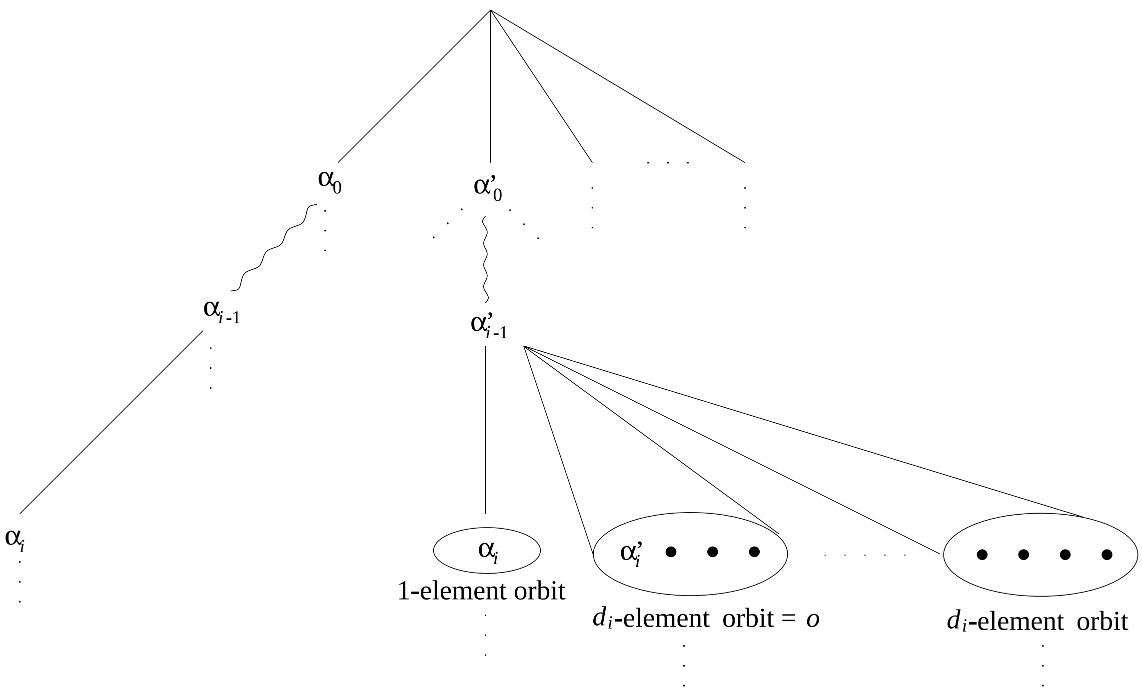


Figure 5

Claim 3 *X is not m-normal, not m-stable and not small.*

Proof. Choose for each $i \in \omega$ a root α_i' of P_i different from α_i. Take $Y = \{\beta \in X : (\forall i \in \omega)(\beta_i \in \{\alpha_i, \alpha_i'\})\} \subseteq X$. We have that any two distinct elements from Y lie in different orbits under the action of $Aut^*(X/\alpha)$, so X is not small.

Let $\alpha' = (\alpha_i')_{i\in\omega} \in X$. To show that X is not m-normal consider the orbit $o(\alpha'/\alpha)$ and a canonical open neighbourhood $U = \{\beta \in X : \beta \restriction n = \alpha' \restriction n\}$ of α'. By Claim 2 (iii), for each $i \in \omega$ we have

$$(**) \qquad |o(\alpha_i'/\alpha_{<i}'\alpha)| = d_i > 1.$$

Hence, for each $i \in \omega$, we can take an $\alpha_i'' \in o(\alpha_i'/\alpha_{<i}'\alpha)$ different from α_i'. By Claim 2 (ii), for each $i \in \omega$ we have

$$|o(\alpha_i''/K_0 \dots K_{i-1}(\alpha'))| = d_i \quad \text{and} \quad \alpha_i' \notin o(\alpha_i''/K_0 \dots K_{i-1}(\alpha')).$$

This together with $(**)$ implies that

$$o(\alpha_i''/K_{<i}\alpha') \setminus o(\alpha_i'/\alpha_{<i}'\alpha) \neq \emptyset.$$

for any $i \in \omega$. Hence, for each $i \in \omega$ we can find an $f_i \in Gal(T_\alpha/K_0 \dots K_{i-1}(\alpha'))$ such that $f_i(\alpha_i'') \notin o(\alpha_i'/\alpha_{<i}'\alpha)$. We easily see that the images of $U \cap o(\alpha'/\alpha)$ under f_i, $i \geq n$, are all distinct. This contradicts m-normality.

The last thing to show is a lack of m-stability. Let $N_0 \cup N_1 \cup \ldots = \omega$ be a partition of ω into infinitely many infinite sets. For $i \in \omega$ we define a $\beta^i = (\beta_0^i, \beta_1^i, \ldots) \in X$:

$$\beta_j^i = \begin{cases} \alpha_j', & \text{if } j \in \bigcup_{k\leq i} N_k \\ \alpha_j, & \text{otherwise.} \end{cases}$$

By Claim 2 (i) we see that for each $i \in \omega$, $o(\alpha'/\beta^0 \dots \beta^{i+1})$ is nowhere dense in $o(\alpha'/\beta^0 \dots \beta^i)$. ■

Let us notice that the sequence α from the above proof does not satisfy the assumption of Proposition 4.5 (i), but it is easy to modify it so that it satisfies this assumption. Namely, let $\eta = (\eta_i)_{i\in\omega}$, where $\eta_i = \alpha_0 + \ldots + \alpha_i$ for $i \in \omega$. Let $K_i' = F(\alpha_0, \ldots, \alpha_i)$. The next remark tells that η satisfies the assumption of Proposition 4.5 (i).

Remark 4.1.2 *For each $i \in \omega$ we have $K_i' = F(\eta_i)$, so $(\eta_j)_{j<i} \subseteq F(\eta_i)$. Moreover, $[K_i' : F] = q_0 \dots q_i$.*

Proof. By induction on i we will show that for any $j_0 < \ldots < j_i$ we have

$$F(\alpha_{j_0}, \ldots, \alpha_{j_i}) = F(\alpha_{j_0} + \ldots + \alpha_{j_i})$$

and so $[F(\alpha_{j_0} + \ldots + \alpha_{j_i}) : F] = q_{j_0} \dots q_{j_i}$.

We have $q_0 \leq q_1 \leq \ldots$.
For $i = 0$ there is nothing to do. Suppose that the statement is true for an $i-1 \in \omega$. To show that it is true for i we can assume that $j_0 = 0, \ldots, j_i = i$. By Lemma 4.1.1 we have that $F(\alpha_1, \ldots, \alpha_i) \parallel_F F(\alpha_0)$. This implies two statements:

1. $[K_i' : F] = q_0 \dots q_i$

2. $[F(\eta_i) : F] > q_1 \dots q_i$.

Only (2) needs an explanation. Let $\eta_{i-1}' = \alpha_1 + \dots + \alpha_i$. We have $\eta_i = \eta_{i-1}' + \alpha_0$. By the induction hypothesis we know that $F(\alpha_1, \dots, \alpha_i) = F(\eta_{i-1}')$ and $[F(\eta_{i-1}') : F] = q_1 \dots q_i$. By the fact that $F(\eta_{i-1}') \parallel_F F(\alpha_0)$ we get that $[F(\eta_i, \alpha_0) : F(\alpha_0)] = q_1 \dots q_i$, hence

$$[F(\eta_i) : F] \geq q_1 \dots q_i.$$

Suppose for a contradiction that $[F(\eta_i) : F] = q_1 \dots q_i$. Let $W(x) = x^n + \beta_{n-1}x^{n-1} + \dots + \beta_0$ be the minimal polynomial of η_i over F. As $n = [F(\eta_{i-1}') : F]$, we get that $(\eta_{i-1}')^n = \gamma_{n-1}(\eta_{i-1}')^{n-1} + \dots + \gamma_0$ for some $\gamma_0, \dots, \gamma_{n-1} \in F$ and the elements $1, \eta_{i-1}', \dots, (\eta_{i-1}')^{n-1}$ are linearly independent over F. So, looking at the coefficient standing by $(\eta_{i-1}')^{n-1}$ in $W(\eta_{i-1}' + \alpha_0) = 0$, we obtain $n\alpha_0 + \beta_{n-1} + \gamma_{n-1} = 0$. Hence $\alpha_0 \in F$ (because we have chosen all q_j's relatively prime to p), a contradiction.

By the assumption that $q_0 \leq q_1 \leq \dots$ together with (1), (2) and the fact that $F \subseteq F(\eta_i) \subseteq K_i'$, the proof is completed. ■

Hence our profinite structure $(X, Aut^*(X))$ is isomorphic to $(T_\eta, Gal(T_\eta/F))$.

One can ask if there exists a less complicated (”smaller”) not small, not m-normal and not m-stable profinite structure weakly interpretable in ACF_p over F. In our example the degrees of polynomials $P_i(x)$ and the sizes of sets X_i are unbounded. From the proof we see that if we had separable polynomials $P_i(x)$ of degree 3 such that their fields of decomposition K_i satisfy

1. $[K_i : F] = 6$,

2. $K_i \parallel_F K_0 \dots K_{i-1}$,

then $(\prod_{i\in\omega} X_i, Gal(\prod_{i\in\omega} X_i/F))$ would be a not small, not m-normal and not m-stable profinte structure weakly interpretable in ACF_p over F (X_i is the set of roots of $P_i(x)$). If $F = F_p(a_0, a_1, \dots)$ is the field of rational functions on infinitely many variables, then it is easy to find such polynomials $P_i(x)$. Namely, we define $P_i(x) = x^3 + a_{3i}x^2 + a_{3i+1}x + a_{3i+2}$ for $i \in \omega$.

Let us notice that the profinite structure obtained in this way is isomorphic to

$$(\{0, 1, 2\}^\omega, S_3^\omega),$$

with the obvious action of S_3^ω on appropriate coordinates (S_3 denotes here the group of all permutations of $\{0, 1, 2\}$).

Method 2 We already know that $(\{0, 1, 2\}^\omega, S_3^\omega)$ is not m-normal, not m-stable and not small. To prove this directly we can formulate Claim 2 using coordinates of the elements of $\{0, 1, 2\}^\omega$ instead of fields K_i. Then the profinite structure $(\{0, 1, 2\}^\omega, S_3^\omega)$ satisfies this claim and we can apply the proof of Claim 3.

We will show that this profinite structure is weakly interpretable in ACF_p over any Hilbertian field F. We need the following fact ([JF], Lemma 15.8).

Fact 4.1.3 *Let F be a Hilbertian field. There is a sequence $K_0, K_1, \dots$ of Galois extensions of F such that*
(i) $Gal(K_i/F) \cong S_3$,
(ii) the sequence $K_0, K_1, \dots$ is linearly disjoint over F.

The fact yields a Galois extension $K_0K_1\dots$ of F with the Galois group topologically isomorphic to S_3^ω. By Theorem 3.1 we are done.

4.2 Example of an m-normal, not small and non-trivial profinite structure of $\mathcal{M}$-rank 1

Method 1. $F = F_p(a_0, a_1, \dots)$ or $F = \mathbb{Q}(a_0, a_1, \dots)$ is the field of rational functions on finitely or infinitely many variables. Let $F_0 := \mathbb{Q}$.

Assume that $p \neq 2$. We define a sequence $\eta \in (\overline{F}^{sep})^\omega$ by

$$\eta_0 = a_0$$
$$\eta_{i+1} = \sqrt{\eta_i}, \text{ for } i \in \omega.$$

The sequence η satisfies the assumption of Proposition 4.5 (i), $[F(\eta_{i+1}) : F] = 2^{i+1}$ and $[F(\eta_{i+1}) : F(\eta_i)] = 2$.

We define a profinite structure (Fig. 6)

$$(X, Aut^*(X)) = (T_\eta, Gal(T_\eta/F))$$

and we will show that it satisfies our demands.

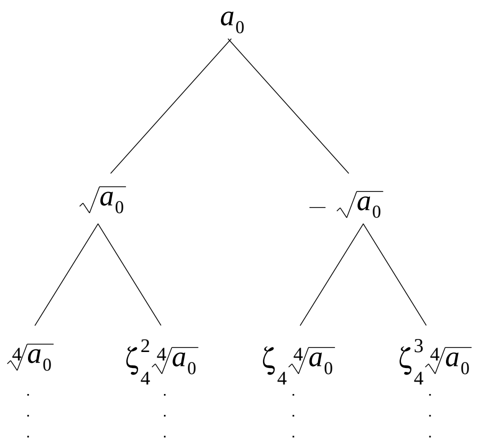


Figure 6

Take any $\eta' \in X$ distinct from η. Then $\eta \restriction n = \eta' \restriction n$ and $\eta_n \neq \eta'_n$ for some $n \geq 1$. We have that there are natural numbers $l_0, l_1, \dots$ such that

$$(*) \qquad \eta'_i = \zeta_{2^i}^{l_i}\eta_i \quad \text{and} \quad 2^{n-1} \parallel l_i, \; i \in \omega,$$

where $\|$ denotes the exact dividing relation. This gives

$$F(\bigcup T_\eta) = F(\eta, (\zeta_{2^i})_{i\in\omega}) = F(\eta, \eta'),$$

where $\bigcup T_\eta$ is the set of all coordinates of all elements of T_η.

Hence 1-orbits over $\{\eta, \eta'\}$ are singletons and there are uncountably many of them, so X is not small.

Claim 1 *(i) 1-orbits over 2-element sets are singletons.*
(ii) Each 1-orbit over a singleton is a singleton or an open set. More precisely, $o(\eta/\eta')$ *is open for all* $\eta \neq \eta'$.

Proof. (i) follows from the above observations.
To show (ii) it is enough to take η' as above and to show that for sufficiently large $i \in \omega$ we have

$$\eta'_i \notin F(\eta, (\eta'_j)_{j<i}).$$

By $(*)$ it remains to prove that

$$\zeta_{2^i}^{l_i} \notin F(\zeta_{2^{i-1}}^{l_i}, \eta).$$

Finally we reduce everything to the statement

$$\zeta_{2^k} \notin F(\zeta_{2^{k-1}}, \eta)$$

for sufficiently large k.

Let us notice that we will be done if we show that for sufficiently large k we have

$$(\dagger) \qquad \zeta_{2^k} \notin F_p(\zeta_{2^{k-1}}).$$

Indeed, suppose for a contradiction that there are arbitrary large k such that $\zeta_{2^k} \in F(\zeta_{2^{k-1}}, \eta)$. Then $\zeta_{2^k} \in F_p(\zeta_{2^{k-1}}, \eta_j, a_1, a_2, \ldots)$ for some $j \in \omega$. This is impossible, because of $(\dagger)$, the fact that $\eta_j, a_1, a_2, \ldots$ are algebraically independent over F_p and $\zeta_{2^k} \in \overline{F_p}$.

To finish the proof of Claim 1 we have to prove $(\dagger)$. Let $s_k = [F_p(\zeta_{2^k}) : F_p]$. For $p = 0$ (i.e. $F_0 = \mathbb{Q}$) $(\dagger)$ is obvious because $s_k = \varphi(2^k) = 2^{k-1}$, where $\varphi(x)$ denotes the Euler function.
For positive characteristic p we have to show that $s_{k-1} < s_k$ for sufficiently large k. As the fields of decomposition over F_p of polynomials $x^{2^k} - 1$ have unbounded sizes, we have

$$\lim_{k\to\infty} s_k = \infty.$$

On the other hand $s_k = min\{s : 2^k \mid p^s - 1\}$, $s_k \mid \varphi(2^k)$ and $\varphi(2^k) = 2^{k-1}$. For k large enough we have $s_k = 2^{n_k}$ for an $n_k > 1$. We claim that in this situation $s_k > s_{k-1}$.

We know that $2^k \mid p^{2^{n_k}} - 1$. But $p^{2^{n_k}} - 1 = (p^{2^{n_k-1}} - 1)(p^{2^{n_k-1}} + 1)$ and since $n_k > 1$, we have $p^{2^{n_k-1}} + 1 \equiv 2 \pmod 4$. Therefore $2^{k-1} \mid (p^{2^{n_k-1}} - 1)$, so $s_{k-1} < s_k$. ■

It is straightforward that Claim 1 implies all the desired properties of X.

If $p = 2$, we define η by

$$\begin{aligned}\eta_0 &= a_0\\ \eta_{i+1} &= \sqrt[3]{\eta_i}, \text{ for } i \in \omega\end{aligned}$$

and we prove similarly as above that $(X, Aut^*(X)) := (T_\eta, Gal(T_\eta/F))$ satisfies our demands.

4.3 Example of an m-normal, small and trivial profinite structure of $\mathcal{M}$-rank 1

Method 1. Let $F = F_p(a_0, a_1, \ldots)$ ($p = 0$ or p is a prime number $\neq 2$) be the field of rational functions on infinitely many variables.

We define an $\eta \in (\overline{F}^{sep})^\omega$ by

$$\begin{aligned}\eta_0 &= a_0\\ \eta_{i+1} &= \sqrt{\eta_i + a_{i+1}}.\end{aligned}$$

Of course the sequence η satisfies the assumption of Proposition 4.5. (i).

As usual we define

$$(X, Aut^*(X)) = (T_\eta, Gal(T_\eta/F))$$

and we will show that it satisfies our demands.

Claim 1 *(i)* $[F(\eta_{i+1}) : F] = 2^{i+1}$ *and* $[F(\eta_{i+1}) : F(\eta_i)] = 2$. *Hence* η_{i+1} *and* $-\eta_{i+1}$ *are conjugate over* $F(\eta_i)$.
(ii) $\eta_{i+1} \notin F(\eta_{\leq i}^{\sigma_1}, \eta_{i+1}^{\sigma_2} : \sigma_1, \sigma_2 \in Gal(T_\eta/F)$ *and* $\eta_{i+1}^{\sigma_2} \neq \pm\eta_{i+1})$.
(iii) $\eta_{i+1} \notin F(\eta_{\leq i}^{\sigma_1}, \tau : \sigma_1 \in Gal(T_\eta/F), \tau \in T_\eta, \tau_i \neq \eta_i)$.

Proof. (i) For each $i \in \omega$ we have $\eta_i = \eta_{i+1}^2 - a_{i+1}$, so

$$a_0 = \eta_0 = \eta_1^2 - a_1 = (\eta_2^2 - a_2)^2 - a_1 = \ldots = P(\eta_{i+1}),$$

for some polynomial $P(x) \in F_p[a_1, a_2, \ldots][x]$ of degree 2^{i+1}. The polynomial $P(x) - a_0$ is irreducible in $F[x]$, because it is irreducible in $F_p[x, a_0, a_1, \ldots]$ as a polynomial of degree 1 in variable a_0 with the highest coefficient -1. The rest of (i) is now obvious.
(ii) Suppose for a contradiction that

$$\eta_{i+1} \in F(\eta_{\leq i}^{\sigma_1}, \eta_{i+1}^{\sigma_2} : \sigma_1, \sigma_2 \in Gal(T_\eta/F) \text{ and } \eta_{i+1}^{\sigma_2} \neq \pm\eta_{i+1}).$$

We can present η_{i+1} as a rational function on $\eta_{i+1}^{\sigma_0}, \ldots, \eta_{i+1}^{\sigma_n}$ ($\eta_{i+1}^{\sigma_j} \neq \pm\eta_{i+1}$ for each $j \leq n$) over $F(\eta_{\leq i}^{\sigma} : \sigma \in Gal(T_\eta/F))$. Below we consider such presentations which use the minimal possible number $n+1$ of conjugates of η_{i+1} ($n \in \{-1\} \cup \omega$). So, in each such presentation we have $\eta_{i+1}^{\sigma_j} \neq \pm\eta_{i+1}, \pm\eta_{i+1}^{\sigma_k}$ for $j \neq k$.

We can find such a presentation so that one of the following cases holds.

Case 1 $\eta_{i+1} = a\eta_{i+1}^{\sigma_0} + b$, where $a, b \neq 0$ and $a, b \in F(\eta_{\leq i}^{\sigma}, \eta_{i+1}^{\tau} : \sigma, \tau \in Gal(T_\eta/F)$ and $\eta_{i+1}^{\tau} \neq \pm\eta_{i+1}, \pm\eta_{i+1}^{\sigma_0})$.

Let $\eta_{i+1}^{\sigma_0}, \ldots, \eta_{i+1}^{\sigma_n}$ be all the conjugates of η_{i+1} used in the above presentation of η_{i+1} (also inside a and b). So, for $j \neq k$ we have $\eta_{i+1}^{\sigma_j} \neq \pm\eta_{i+1}, \pm\eta_{i+1}^{\sigma_k}$. We obtain

$$\eta_{i+1}^{\sigma_0} = \frac{\eta_{i+1}^2 - a^2(\eta_{i+1}^{\sigma_0})^2 - b^2}{2ab} = \frac{\eta_i - a^2\eta_i^{\sigma_0} + a_{i+1} - a^2 a_{i+1} - b^2}{2ab}.$$

Hence $\eta_{i+1}^{\sigma_0} \in F(\eta_{\leq i}^{\sigma}, \eta_{i+1}^{\sigma_1}, \ldots, \eta_{i+1}^{\sigma_n} : \sigma \in Gal(T_\eta/F))$. Acting on both sides by σ_0^{-1} we get a contradiction with the minimality of n.

Case 2 $\eta_{i+1} = a\eta_{i+1}^{\sigma_0} \ldots \eta_{i+1}^{\sigma_n}$, where $a \in F(\eta_{\leq i}^{\sigma} : \sigma \in Gal(T_\eta/F))$ and for every $k \neq j$ we have $\eta_{i+1}^{\sigma_j} \neq \pm\eta_{i+1}, \pm\eta_{j+1}^{\sigma_k}$.

Notice that this case includes also the case, when $n = -1$, i.e. $\eta_{i+1} \in F(\eta_{\leq i}^{\sigma} : \sigma \in Gal(T_\eta/F))$.

As $\eta_{i+1}^{\sigma_j} \neq \pm\eta_{i+1}$,

$$(*) \qquad \eta_i^{\sigma_j} \neq \eta_i.$$

Observe that

$$F(\eta_{\leq i}^{\sigma} : \sigma \in Gal(T_\eta/F)) = F_p(\eta_{\leq i}^{\sigma}, a_j : \sigma \in Gal(T_\eta/F), j \neq i+1)(a_{i+1})$$

and a_{i+1} is transcendental over $F_p(\eta_{\leq i}^{\sigma}, a_j : \sigma \in Gal(T_\eta/F), j \neq i+1)$.

We write a in the form

$$a = \frac{R_1(a_{i+1})}{R_2(a_{i+1})},$$

where $R_1(x), R_2(x) \in F_p(\eta_{\leq i}^{\sigma}, a_j : \sigma \in Gal(T_\eta/F), j \neq i+1)[x]$.

The assumption of Case 2 implies

$$\eta_i + a_{i+1} = a^2(\eta_i^{\sigma_0} + a_{i+1}) \ldots (\eta_i^{\sigma_n} + a_{i+1}).$$

Therefore

$$R_2(a_{i+1})^2(\eta_i + a_{i+1}) = R_1(a_{i+1})^2(\eta_i^{\sigma_0} + a_{i+1}) \ldots (\eta_i^{\sigma_n} + a_{i+1}).$$

This gives us an equality of polynomials

$$L(x) := R_2(x)^2(x + \eta_i) = R_1(x)^2(x + \eta_i^{\sigma_0}) \ldots (x + \eta_i^{\sigma_n}) =: R(x),$$

where $L(x), R(x) \in F_p(\eta_{\leq i}^{\sigma}, a_j : \sigma \in Gal(T_\eta/F), j \neq i+1)[x]$.

By $(*)$ we obtain that $-\eta_i$ is a root of R(x) of even multiplicity, whereas it is a root of $L(x)$ of odd multiplicity, a contradiction.

Notice that point (ii) implies (i).

(iii) Suppose for a contradiction that $\eta_{i+1} \in F(\eta_{\leq i}^{\sigma}, \eta^{\sigma_0}, \ldots, \eta^{\sigma_n} : \sigma \in Gal(T_\eta/F))$, for some $\sigma_0, \ldots, \sigma_n \in Gal(T_\eta/F)$ such that $\eta_i \neq \eta_i^{\sigma_j}$ for each $j \leq n$.

By point (ii) we have that $n \geq 0$ (i.e. $\{\sigma_0, \ldots, \sigma_n\} \neq \emptyset$) and the minimal number k such that $\eta_{i+1} \in F(\eta_{\leq i}^{\sigma}, \eta_{\leq k}^{\sigma_0}, \ldots, \eta_{\leq k}^{\sigma_n} : \sigma \in Gal(T_\eta/F))$ is greater than $i+1$.

Hence for an element from $\{\sigma_0, \ldots, \sigma_n\}$, e.g. for σ_0, we can write

$$\eta_{i+1} = a\eta_k^{\sigma_0} + b,$$

for some $a, b \in F(\eta^{\sigma}_{\leq k-1}, \eta_k^{\sigma_{i_1}}, \ldots, \eta_k^{\sigma_{i_s}} : \sigma \in Gal(T_\eta/F))$, where $1 \leq i_1 < \ldots < i_s \leq n$ are such that $\eta_k^{\sigma_0} \neq \pm\eta_k^{\sigma_{i_j}}$ for $j \leq s$ and $a \neq 0$. This gives us that $\eta_k^{\sigma_0} \in F(\eta^{\sigma}_{\leq k-1}, \eta_k^{\tau} : \sigma, \tau \in Gal(T_\eta/F), \eta_k^{\tau} \neq \pm\eta_k^{\sigma_0})$. It is a contradiction with (ii). ■

In the next claim we consider orbits in X. Let $a = (a_0, \ldots, a_n) \in X^{n+1}$ be a finite tuple of pairwise distinct elements of X and A be a finite subset of X. Let $\{a_0, \ldots, a_n\} \cap A = \{a_0, \ldots, a_k\}$.

Claim 2 *(i) Each* 1*-orbit over a finite set is a singleton or an open subset of* X*.*
(ii) There is a clopen neighbourhood U *of* a *in* X^{n+1} *such that* $U \cap o(a/A) = \{a_0\} \times \ldots \times \{a_k\} \times U_{k+1} \times \ldots \times U_n$ *for some open subsets* $U_{k+1}, \ldots, U_n$ *of* X *such that* $U_{k+1} \subseteq o(a_{k+1}/A), \ldots, U_n \subseteq o(a_n/A)$*.*

Proof. Both points follow from Claim 1 (iii). ■

The fact that X has $\mathcal{M}$-rank 1 follows from Claim 2 (i). Smallness, triviality and m-normality of X follow from Claim 2 (ii).

In fact Claim 1 implies that

$$(X, Aut^*(X)) \cong (\{0,1\}^\omega, Aut^*(\{0,1\}^\omega)),$$

where $Aut^*(\{0,1\}^\omega)$ is the standard structural group of the product $\{0,1\}^\omega$.

4.4 Examples of profinite structures of $\mathcal{M}$-rank n (for arbitrary $n \in \omega$), m-normal, small and non-trivial for $n = 1$

Consider

$$(\mathbb{Z}_p^\omega, Aut^*(\mathbb{Z}_p^\omega/A_0)),$$

where

$$A_0 = \{\eta \in \mathbb{Z}_p^\omega \restriction n : n \geq 1, \eta \restriction n-1 = (0, \ldots, 0)\}$$

and $Aut^*(\mathbb{Z}_p^\omega)$ is the standard structural group of $\mathbb{Z}_p^\omega$. Recall that the standard structural group of the profinite group $\mathbb{Z}_p^\omega$ is the group of all topological automorphisms of $\mathbb{Z}_p^\omega$ preserving the inverse system

$$\mathbb{Z}_p \longleftarrow \mathbb{Z}_p \times \mathbb{Z}_p \longleftarrow \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \longleftarrow \ldots$$

inducing a profinite structure on $\mathbb{Z}_p^\omega$.

From the proof of Fact 4.4 (see [Kr1], the proof of Proposition 3.2.6) we know that $S := Aut^*(\mathbb{Z}_p^\omega/A_0)$ is a pro-p-group and $(\mathbb{Z}_p^\omega, S)$ is small, m-normal and m-stable. Moreover, it has $\mathcal{M}$-rank 1 and it is non-trivial because of the group action. One can show that S is a Sylow p-subgroup of $Aut^*(\mathbb{Z}_p^\omega)$.

Method 1 Let F be a Hilbertian field of characteristic p.

We will show that $(\mathbb{Z}_p^\omega, S)$ is weakly interpretable in ACF_p over F. More precisely, we will show the following theorem.

Theorem 4.4.1 *The profinite structure $(\mathbb{Z}_p^\omega, S)$ is weakly interpretable in ACF_p over any Hilbertian field F of characteristic p, in such a way that the group operation in $\mathbb{Z}_p^\omega$ becomes the field addition on each coordinate.*

Proof. We identify $\mathbb{Z}_p$ with the set $p = \{0, \ldots, p-1\}$, and $\mathbb{Z}_p^n$ with the set p^n of n-tuples of numbers $< p$.

By induction on n we construct sets of elements $\{x_\sigma : \sigma \in p^n\}$ ($x_\sigma \neq x_{\sigma'}$ for $\sigma \neq \sigma'$) such that for every $n \geq 1$

$$(\mathbb{Z}_p^n, S \restriction \mathbb{Z}_p^n) \cong (X_n, G_n),$$

where $X_n = \{(x_{\sigma\restriction 1}, \ldots, x_{\sigma\restriction n}) : \sigma \in p^n\} \subseteq (\overline{F}^{sep})^n$ is invariant under $Gal(\overline{F}^{sep}/F)$, $G_n = Gal(X_n/F)$ and the isomorphism denoted by Φ_n is given by

$$\Phi_n(\sigma) = (x_{\sigma\restriction 1}, \ldots, x_{\sigma\restriction n}).$$

Moreover, we require that for each n and $\sigma_1, \sigma_2 \in p^n$,

$$\Phi_n(\sigma_1 + \sigma_2) = (x_{\sigma_1\restriction 1} + x_{\sigma_2\restriction 1}, \ldots, x_{\sigma_1\restriction n} + x_{\sigma_2\restriction n}).$$

In this proof by S_n we denote the group $S \restriction \mathbb{Z}_p^n$.

For $n = 1$ we define

$$x_{\langle i\rangle} = i \text{ for } i = 0, \ldots, p-1.$$

Suppose now that we have found x_σ for $|\sigma| \leq n$. Our aim is to find x_σ, for $\sigma \in p^{n+1}$, such that $\sigma \mapsto (x_{\sigma\restriction 1}, \ldots, x_{\sigma\restriction n+1})$ defines an isomorphism Φ_{n+1} between $(\mathbb{Z}_p^{n+1}, S_{n+1})$ and (X_{n+1}, G_{n+1}) satisfying

$$\Phi_{n+1}(\sigma_1 + \sigma_2) = (x_{\sigma_1\restriction 1} + x_{\sigma_2\restriction 1}, \ldots, x_{\sigma_1\restriction n+1} + x_{\sigma_2\restriction n+1}).$$

We outline the construction. First we enlarge our field F to some field E. Then we find x'_σ, $\sigma \in p^{n+1}$, satisfying our demands over the field E. Finally, by specialization argument for Hilbertian fields, we find x_σ, $\sigma \in p^{n+1}$, satisfying our demands over F.

Let $\sigma_1 = \langle 1, 0, 0, \ldots, 0\rangle, \sigma_2 = \langle 1, 1, 0, \ldots, 0\rangle, \ldots, \sigma_n = \langle 1, 1, \ldots, 1, 0\rangle$ and $\sigma_0 = \langle 0, 0, \ldots, 0, 1\rangle$ be a basis of $\mathbb{Z}_p^{n+1}$ over F_p.

It is easy to show that any $f \in S_{n+1}$ arises from an $f \restriction n = g \in S_n$ ($f \restriction n$ denotes the automorphism of $\mathbb{Z}_p^n$ induced by f) by defining

$$f(\sigma_i) = g(\sigma_i \restriction n)^\frown \epsilon_i, 1 \leq i \leq n,$$

where $g \in S_n$ and $\epsilon_i \in \mathbb{Z}_p$ can be chosen arbitrarily. Since $S = Aut^*(\mathbb{Z}_p^\omega/A_0)$, we have $f(\sigma_0) = \sigma_0$. Then the value of f on an arbitrary $\sigma = \sum_{i=0}^n l_i\sigma_i \in \mathbb{Z}_p^{n+1}$ is given by

$$(*) \qquad f(\sigma) = g(\sigma \restriction n)^\frown(l_0 + \sum_{i=1}^n l_i\epsilon_i) = \langle 0, 0, \ldots, 0, l_0\rangle + \sum_{i=1}^n l_i f(\sigma_i).$$

In particular, by induction, from $(*)$ we get that $\sigma_1 \restriction n, \ldots, \sigma_n \restriction n$ lie in the same orbit under the action of S_n. By $\alpha_1, \ldots, \alpha_n$ we denote the elements $\sigma_1 \restriction n, \ldots, \sigma_n \restriction n$, respectively. They form a basis of $\mathbb{Z}_p^n$ over F_p.

Choose $\tau_1, \ldots, \tau_n \in S_n$ such that

$$\tau_i(\alpha_1) = \alpha_i$$

and let $t_{\tau_1}, \ldots, t_{\tau_n}$ be algebraically independent over F.

For each $\tau \in S_n$ we define

$$t_\tau = \sum_{i=1}^n l_i t_{\tau_i},$$

where the elements $l_i \in F_p$ appear in the expansion $\tau(\alpha_1) = \sum_{i=1}^n l_i\alpha_i$.

Let $L = F(x_\sigma : \sigma \in p^{\leq n})$. By induction hypothesis, Φ_n identifies S_n with $Gal(L/F)$. Under this identification each $\tau \in S_n$ is an automorphism of L, so we can extend it to an endomorphism of $L[t_{\tau_1}, \ldots, t_{\tau_n}] = L[t_\tau : \tau \in S_n]$ by defining

$$\tau t_{\tau_i} = t_{\tau\tau_i}$$

for $1 \leq i \leq n$.

Claim 1 *(i) For every $\tau, \tau' \in S_n$ we have $\tau t_{\tau'} = t_{\tau\tau'}$.*
(ii) S_n acts on $L[t_\tau : \tau \in S_n]$ as a group of automorphisms, so it acts on $L(t_\tau : \tau \in S_n)$ as a group of automorphisms, too.

Proof. (i) Let $\tau'(\alpha_1) = \sum_{i=1}^n l_i\alpha_i$ and $\tau(\alpha_i) = \sum_{j=1}^n l_{ij}\alpha_j$. Then

$$\tau t_{\tau'} = \tau(\sum_{i=1}^n l_i t_{\tau_i}) = \sum_{i=1}^n l_i\tau(t_{\tau_i}) = \sum_{i=1}^n l_i t_{\tau\tau_i},$$

so

$$\tau t_{\tau'} = \sum_{i=1}^n \sum_{j=1}^n l_i l_{ij} t_{\tau_j}.$$

On the other hand $\tau\tau'(\alpha_1) = \tau(\sum_{i=1}^n l_i\alpha_i) = \sum_{i=1}^n l_i\tau(\alpha_i) = \sum_{i=1}^n \sum_{j=1}^n l_i l_{ij}\alpha_j$, hence

$$t_{\tau\tau'} = \sum_{i=1}^n \sum_{j=1}^n l_i l_{ij} t_{\tau_j}.$$

(ii) By (i) it is enough to show that for every $\tau \in S_n$ the elements $t_{\tau\tau_1}, \ldots, t_{\tau\tau_n}$ are algebraically independent over L and that $L[t_{\tau_1}, \ldots, t_{\tau_n}] = L[t_{\tau\tau_1}, \ldots, t_{\tau\tau_n}]$.
Let $\tau(\alpha_i) = \sum_{j=1}^n l_{ij}\alpha_j$. Then

$$A = (l_{ij})_{1 \leq i,j \leq n}$$

is an invertible matrix over F_p. On the other hand

$$t_{\tau\tau_i} = \sum_{j=1}^{n} l_{ij} t_{\tau_j}.$$

So our proof is completed. $\square$

Let $K = L(t_\tau : \tau \in S_n)$ and $E = K_{S_n}$, where $K_{S_n} = \{a \in K : (\forall \tau \in S_n)(\tau(a) = a)\}$. We have $L = F(c)$ for some $c \in L$. Let for $i = 1, \ldots, |S_n|$

$$(*)_i \qquad t_i = \sum_{\tau \in S_n} \tau(c)^{i-1} t_\tau.$$

Notice that by Claim 1 (i), $t_i \in E$ for each i.

Claim 2 *$E = F(t_{i_1}, \ldots, t_{i_m})$, where $\{t_{i_1}, \ldots, t_{i_m}\}$ is a transcendence basis of the set $\{t_i : 1 \leq i \leq |S_n|\}$ over L. This is also its linear basis over L and $m = n$.*

Proof. The coefficient matrix of the system of linear equations $((*)_i)_{i=1}^{|S_n|}$ in variables $t_\tau, \tau \in S_n$, is invertible (Vandermonde's matrix). Hence the linear [transcendence] dimension of $\{t_i : 1 \leq i \leq |S_n|\}$ equals the linear [transcendence] dimension of $\{t_\tau : \tau \in S_n\}$. Moreover, we know that the linear and transcendence dimensions of the last set are the same and equal to n.

So let $\{t_{i_1}, \ldots, t_{i_n}\}$ be a linear (= transcendence) basis of $\{t_i : 1 \leq i \leq |S_n|\}$. We get also that $K = L(t_{i_1}, \ldots, t_{i_n})$, hence

$$[L : F] = [K : F(t_{i_1}, \ldots, t_{i_n})].$$

On the other hand, we have $t_{i_1}, \ldots, t_{i_n} \in E$. Hence $F(t_{i_1}, \ldots, t_{i_n}) \subseteq E$ and we have $|S_n| = [K : E] \leq [K : F(t_{i_1}, \ldots, t_{i_n})] = [L : F] = |S_n|$. This implies that $E = F(t_{i_1}, \ldots, t_{i_n})$. $\square$

Now we define x'_σ, $\sigma \in p^{n+1}$, in the following way

$$\begin{cases} x'_{\sigma_0} = 1 & \\ x'_{\sigma_i} = \text{one of the roots of the polynomial } x^p - x - t_{\tau_i}, & \text{for } 1 \leq i \leq n \\ x'_\sigma = \sum_{i=0}^{n} l_i x'_{\sigma_i}, & \text{for } \sigma = \sum_{i=0}^{n} l_i \sigma_i. \end{cases}$$

For a given $\alpha = \sum_{i=1}^{n} l_i \alpha_i \in p^n$ and $\epsilon \in p$ we have that $x'_{\alpha^\frown\epsilon} = \sum_{i=1}^{n} l_i x'_{\sigma_i} + \epsilon$ is a root of the polynomial $x^p - x - \sum_{i=1}^{n} l_i t_{\tau_i}$. Since $t_{\tau_1}, \ldots, t_{\tau_n}$ are algebraically independent over F we get that $x'_\sigma \neq x'_{\sigma'}$ for $\sigma \neq \sigma' \in p^{n+1}$. Moreover, we easily see that $x'_{\alpha^\frown 0}, \ldots, x'_{\alpha^\frown p-1}$ are all the roots of the polynomial $x^p - x - \sum_{i=1}^{n} l_i t_{\tau_i}$.

Of course we have also that

$$(X_n, Gal(X_n/E)) = (X_n, Gal(X_n/F)) \cong (\mathbb{Z}_p^n, S_n).$$

Let $X'_{n+1} = \{(x_{\sigma\restriction 1}, \ldots, x_{\sigma\restriction n}, x'_{\sigma\restriction n+1}) : \sigma \in p^{n+1}\} \subseteq (\overline{E}^{sep})^{n+1}$.

Claim 3 *X'_{n+1} is invariant under $Gal(\overline{E}^{sep}/E)$.*

Proof. Take any $\sigma = \sum_{i=0}^{n} l_i\sigma_i \in p^{n+1}$. Let $\alpha = \sigma \restriction n$. Let $g \in Gal(\overline{E}^{sep}/E)$ and $\tau = g \restriction K \in Gal(K/E)$. We recall that τ can be identified with an element of S_n. Let

$$\alpha = \sum_{i=1}^{n} l_i\alpha_i, \quad \tau(\alpha) = \sum_{i=1}^{n} k_i\alpha_i \ \text{ and } \ \tau(\alpha_i) = \sum_{j=1}^{n} k_{ij}\alpha_j$$

for $i = 1, \ldots, n$. Then $\tau(\alpha) = \sum_{i=1}^{n} l_i\tau(\alpha_i)$. Therefore

$$\tau(\alpha) = \sum_{i=1}^{n}\sum_{j=1}^{n} l_i k_{ij}\alpha_j.$$

Hence

$$(**) \qquad k_j = \sum_{i=1}^{n} l_i k_{ij}.$$

By remarks before Claim 3 we know that x'_σ is a root of the polynomial $x^p - x - \sum_{i=1}^{n} l_i t_{\tau_i}$. Hence $g(x'_\sigma)$ is a root of the polynomial

$$x^p - x - \sum_{i=1}^{n} l_i\tau t_{\tau_i} = x^p - x - \sum_{i=1}^{n} l_i t_{\tau\tau_i} = x^p - x - \sum_{i=1}^{n}\sum_{j=1}^{n} l_i k_{ij} t_{\tau_j}.$$

By $(**)$ we get that $g(x'_\sigma)$ is a root of the polynomial $x^p - x - \sum_{i=1}^{n} k_i t_{\tau_i}$. Once again by remarks before Claim 3, we get that there is a $\sigma' = \tau(\alpha)^\frown\epsilon$ such that $g((x_{\sigma\restriction 1}, \ldots, x_{\sigma\restriction n}, x'_{\sigma\restriction n+1})) = (x_{\sigma'\restriction 1}, \ldots, x_{\sigma'\restriction n}, x'_{\sigma'\restriction n+1}) \in X_{n+1}$. $\square$

We define a map $\Phi'_{n+1} : \mathbb{Z}_p^{n+1} \to X'_{n+1}$ by

$$\Phi'_{n+1}(\sigma) = (x_{\sigma\restriction 1}, \ldots, x_{\sigma\restriction n}, x'_{\sigma\restriction n+1}).$$

By the remark just after the definition of x'_σ, $\sigma \in p^{n+1}$, we see that Φ'_{n+1} is a bijection.

Claim 4 *(i) Φ'_{n+1} is an isomorphism between $(\mathbb{Z}_p^{n+1}, S_{n+1})$ and $(X'_{n+1}, Gal(X'_{n+1}/E))$.*
(ii) For $\xi_1, \xi_2 \in p^{n+1}$ we have $\Phi'_{n+1}(\xi_1 + \xi_2) = (x_{\xi_1\restriction 1} + x_{\xi_2\restriction 1}, \ldots, x'_{\xi_1\restriction n+1} + x'_{\xi_2\restriction n+1})$.

Proof. (ii) By induction hypothesis it is enough to show that for $\xi_1, \xi_2 \in p^{n+1}$ we have

$$x'_{\xi_1+\xi_2} = x'_{\xi_1} + x'_{\xi_2}.$$

Let $\xi_1 = \sum_{i=0}^{n} l_{1i}\sigma_i$ and $\xi_2 = \sum_{i=0}^{n} l_{2i}\sigma_i$. Then $\xi_1 + \xi_2 = \sum_{i=0}^{n}(l_{1i} + l_{2i})\sigma_i$ and by the definition of x'_σ's we get

$$x'_{\xi_1+\xi_2} = \sum_{i=0}^{n}(l_{1i} + l_{2i})x'_{\sigma_i} = \sum_{i=0}^{n} l_{1i}x'_{\sigma_i} + \sum_{i=0}^{n} l_{2i}x'_{\sigma_i} = x'_{\xi_1} + x'_{\xi_2}.$$

(i) At the beginning of the proof (see $(*)$) we described how the action of S_n on $\mathbb{Z}_p^n$ extends to the action of S_{n+1} on $\mathbb{Z}_p^{n+1}$. By induction hypothesis it is enough to prove the corresponding description for $Gal(X'_{n+1}/E)$ acting on X'_{n+1}.

Let $L' = L(x'_\sigma : \sigma \in p^{n+1})$. So $L' = L(x'_{\sigma_i} : 1 \leq i \leq n)$ and $E \subseteq K \subseteq L'$. We have also $L \subseteq L(t_{\tau_i}) \subseteq L(x'_{\sigma_i})$ and it is easy to check that $L(x'_{\sigma_i})$ is a regular extension of L. Hence the fields $L(x'_{\sigma_i}), i = 1, \ldots, n$, are linearly disjoint over L. Moreover, $L(x'_{\sigma_i})$ is a cyclic extension of $L(t_{\tau_i})$ of degree p for $i = 1, \ldots, n$.

Therefore, any $f \in Gal(X'_{n+1}/E)$ arises from an $f \restriction X_n = \tau \in Gal(X_n/E)$ ($f \restriction X_n$ denotes the automorphism of X_n induced by f and it can be identified with an element of S_n) by defining

$$f(x'_{\sigma_i}) = x'_{\tau(\alpha_i)^\frown \epsilon_i}, 1 \leq i \leq n,$$

where $\tau \in Gal(X_n/E)$ and $\epsilon_i \in \mathbb{Z}_p$ can be chosen arbitrarily. Then the value of f on an arbitrary $(x_{\sigma\restriction 1}, \ldots, x_{\sigma\restriction n}, x'_{\sigma\restriction n+1}) \in X'_{n+1}$, where $\sigma = \sum_{i=0}^n l_i\sigma_i$ (so $x'_\sigma = \sum_{i=0}^n l_i x'_{\sigma_i}$) is given by

$$f(x_{\sigma\restriction 1}, \ldots, x_{\sigma\restriction n}, x'_{\sigma\restriction n+1}) = (\tau(x_{\sigma\restriction 1}), \ldots, \tau(x_{\sigma\restriction n}), \sum_{i=0}^{n} l_i f(x'_{\sigma_i})).$$

Hence, by point (ii) we get

$$f(x_{\sigma\restriction 1}, \ldots, x_{\sigma\restriction n}, x'_{\sigma\restriction n+1}) = (x_{\tau(\sigma\restriction n)\restriction 1}, \ldots, x_{\tau(\sigma\restriction n)\restriction n}, x'_{\tau(\sigma\restriction n)^\frown(l_0 + \sum_{i=1}^n l_i\epsilon_i)}).$$

This completes the proof of Claim 4. $\square$

We have almost made the induction step. The last thing is to replace $E = F(t_{i_1}, \ldots, t_{i_n})$ by F. We will do this by a standard specialization argument for Hilbertian fields.

Let L' be defined as in the proof of Claim 4 and T denote the sequence $(t_{i_1}, \ldots, t_{i_n})$. Then $L' = E(\theta) = F(t_{i_1}, \ldots, t_{i_n})(\theta)$ for some θ integral over $F[T]$.

Choose $g_1(T), g_2(T), g_3(T) \in F[T]$ so that

1. x_σ and $x'_{\sigma'}$ are integral over $F[T, g_1(T)^{-1}]$ for any $\sigma \in p^{\leq n}$ and $\sigma' \in p^{n+1}$,
2. $$\prod_{\sigma_1 \neq \sigma_2 \in p^{n+1}} (x'_{\sigma_1} - x'_{\sigma_2}) = \frac{g_2(T)}{g_1(T)},$$
3. $g_3(T)$ is the discriminant of θ in the field extension $E \subseteq L'$.

Let

$$g(T) = g_1(T)g_2(T)g_3(T) \in F[T],\ R = F[T, g(T)^{-1}],\ R' = R[\theta].$$

Since the discriminant of θ is a unit of R, we get that R' is integrally closed in L' (see [FJ], Lemma 5.3). Hence $x_\sigma \in R'$ for any $\sigma \in p^{\leq n}$. In particular $L \subseteq R'$. Moreover, $x'_\sigma \in R'$ for any $\sigma \in p^{n+1}$.

Let $H_F(T,x) \in F[T][x]$ $[H_L(T,x) \in L[T][x]$, respectively] be the minimal monic polynomial of θ over $F[T]$ $[L[T]$, repectively]. Since F is Hilbertian and L is a separable extension of F, there exists an $a \in F^n$ such that (see [FJ], Corollary 11.7)

1. $h_F(a,x) \in F[x]$ is irreducible,
2. $h_L(a,x) \in L[x]$ is irreducible,
3. $g(a) \neq 0$.

Let L'' be the field of decomposition of the polynomial $h_L(a,x)$ over the field L. There exists an epimorphism $\phi : R' \to L''$ defined by the specialization $T \mapsto a$ and such that $\phi \restriction L = id$. ϕ maps θ to a root of $h_L(a,x)$, which must be of course a root of $h_F(a,x)$. It is easy to see that L'' is a Galois extension of F.

It is standard that defining

$$\psi(\delta)(\phi(x)) = \phi(\delta(x)),$$

for $x \in R'$ and $\delta \in Gal(L'/F(T))$ we obtain an isomorphism

$$\psi : Gal(L'/F(T)) \to Gal(L''/F).$$

From the choice of $g_2(T)$ we get that

$$\prod_{\sigma_1 \neq \sigma_2 \in p^{n+1}} (\phi(x'_{\sigma_1}) - \phi(x'_{\sigma_2})) = \frac{g_2(a)}{g_1(a)} \neq 0.$$

Hence the elements $\phi(x'_\sigma)$, $\sigma \in p^{n+1}$, are pairwise distinct. For $\sigma \in p^{n+1}$ we define

$$x_\sigma = \phi(x'_\sigma)$$

and $X_{n+1} = \{(x_{\sigma\restriction 1}, \ldots x_{\sigma\restriction n}, x_\sigma) : \sigma \in p^{n+1}\} \subseteq (\overline{F}^{sep})^{n+1}$.

Finally we see that (ϕ, ψ) defines an isomorphism between

$$(X'_{n+1}, Gal(X'_{n+1}/F(T))) \text{ and } (X_{n+1}, Gal(X_{n+1}/F)).$$

This completes the induction step.

The above construction yields the profinite structure

$$X = \{(x_{\sigma\restriction n})_{n\geq 1} : \sigma \in p^\omega\},$$

being a weak interpretation in ACF_p over F of the profinite group $(\mathbb{Z}_p^\omega, S)$. Moreover, the group operation in $\mathbb{Z}_p^\omega$ corresponds to the field addition in X. ■

Notice that if we work over the field of rational functions on infinitely many variables over F_p, then we do not need to do a specialization argument in the above induction construction. Namely, in each induction step we add a new finite set of variables.

Method 2 This method yields more examples of profinite groups weakly interpretable in ACF_p over some fields. In particular we obtain here (in Theorem 4.4.2 and 4.4.4) once again that the profinite group $(\mathbb{Z}_p^\omega, S)$ is weakly interpretable in ACF_p over some fields. However, theorems 4.4.2 and 4.4.4 do not yield an explicit interpretation and do not imply that there is an interpretation for which the group operation in $\mathbb{Z}_p^\omega$ corresponds to the field addition. Moreover, Theorem 4.4.2 does not work over any Hilbertian field F but rather is restricted to the case, when F is the field of rational functions on finitely or infinitely many variables over F_p.

Theorem 4.4.2 *Let F be the field of rational functions on finitely or infinitely many variables over F_p. Any profinite structure X, whose structural group S is a pro-p-group, is interpretable in ACF_p over F.*

Proof. For a field k of characteristic p we consider its maximal p-extension $\hat{k}$, which is the composition of all its finite p-extensions. In [Ko] we have the following fact.

Fact 4.4.3 *$Gal(\hat{k}/k)$ is a free pro-p-group of rank $dim_{F_p}(k^+/\mathfrak{p}(k^+))$, where $\mathfrak{p} : k \to k$ is defined by $\mathfrak{p}(a) = a^p - a$.*

We easily see that $dim_{F_p}(F^+/\mathfrak{p}(F^+)) = \omega$. Hence S is an epimorphic image of $Gal(\hat{F}/F)$, so there is a Galois extension L of F such that $Gal(L/F) \cong S$. By Theorem 3.1 we get that (X, S) is weakly interpretable in ACF_p over F. ■

By Fact 4.4 we know that each product of finite abelian p-groups of bounded exponent with a structural group being a Sylow p-subgroup of the standard structural group is small, m-normal and m-stable. Hence, by Theorem 4.4.2, we get a big class of groups with these properties, which are weakly interpretable in ACF_p over any field F of rational functions over F_p.

Method 2 allows us to interpret in ACF_p ($p = 0$ or a prime number) over any Hilbertian field F more profinite groups, even with the standard structural groups. Namely, we have the following theorem.

Theorem 4.4.4 *Let F be a Hilbertian field. For a profinite group X, the group $Aut^*(X)$ denotes the standard structural group of X.*
(i) If $X = \prod_{i\in\omega} X_i$, where $X_i = \mathbb{Z}_{p_{i1}^{j_{i1}}} \times \ldots \times \mathbb{Z}_{p_{ik_i}^{j_{ik_i}}}$ for prime numbers p_{ik} ($p_{ik} \neq p_{il}$ for $k \neq l$), then $(X, Aut^*(X))$ is weakly interpretable in ACF_p over F.
(ii) If $X = \prod_{i\in\omega} X_i$ is a product of arbitrary finite abelian groups and $G = Aut^*(X/A_0)$, where $A_0 = \{\eta \in X \upharpoonright n : n \geq 1, \eta \upharpoonright n-1 = (0, \ldots, 0)\}$, then (X, G) is weakly interpretable in ACF_p over F.

Proof. By Theorem 3.1 it is enough to find a Galois extension L of F such that $Gal(L/F) \cong Aut^*(X)$ in (i) and $Gal(L/F) \cong G$ in (ii).

To do this we need the following Uchida's theorem (see [JF], Proposition 24.47)

Fact 4.4.5 *Let L be a finite Galois extension of a Hilbertian field F and let $G = Gal(L/F)$. Suppose that G acts as a group of automorphisms on a finite abelian group A. Let $A \rtimes G$ be the corresponding semidirect product and $\alpha : A \rtimes G \to G$ be the projection map. Then there exists a Galois extension L' of F containing L, for which there exists an isomorphism $\gamma : Gal(L'/F) \to A \rtimes G$ such that $\alpha \circ \gamma = res_L$.*

Let us consider a profinite group S. We consider the question:

Is S the Galois group of some Galois extension of F?

By Uchida's theorem and an easy induction we see that to answer positively this question it is enough to show that S can be presented as an inverse limit

$$\varprojlim S_i, \text{ with connecting maps } f_{ij} : S_i \to S_j, i > j,$$

of finite groups such that for any $i \in \omega$ the extension

$$1 \to ker(f_{i+1,i}) \to S_{i+1} \to S_i \to 1$$

is isomorphic to the extension

$$1 \to ker(f_{i+1,i}) \to ker(f_{i+1,i}) \rtimes S_i \to S_i \to 1$$

and $ker(f_{i+1,i})$ is an abelian group.

We recall that two extensions of groups

$$1 \to A \to B \to C \to 1 \text{ and } 1 \to A \to B' \to C \to 1$$

are isomorphic if there exists an isomorphism $\alpha : B \to B'$ such that the following diagram commutes:

$$\begin{tikzcd}
& & B \arrow[dd, "\alpha"] \arrow[dr] & & \\
1 \arrow[r] & A \arrow[ur] \arrow[dr] & & C \arrow[r] & 1 \\
& & B' \arrow[ur] & &
\end{tikzcd}$$

Now we turn to the proof of (ii) in Theorem 4.4.4. We put $S = G$ and $S_i = G \restriction (X \restriction i)$ for $i \geq 1$. Then

$$S \cong \varprojlim S_i,$$

where the connecting maps $f_{i,j} : S_i \to S_j$, $i > j$, are defined as restrictions.

By the above observation we will be done if we show the following claim.

Claim 1 *For every $i \in \omega$ we have that*
(1) $ker(f_{i+1,i})$ is an abelian group,
(2) the extension

$$1 \to ker(f_{i+1,i}) \to S_{i+1} \to S_i \to 1$$

is isomorphic to the extension

$$1 \to ker(f_{i+1,i}) \to ker(f_{i+1,i}) \rtimes S_i \to S_i \to 1.$$

Proof. Let $H_{i+1} := ker(f_{i+1,i}) = \{g \in S_{i+1} : g \restriction (X \restriction i) = id_{X \restriction i}\}$.

For every $k \leq i$ we can write $X_k = \langle \xi_{k1} \rangle \oplus \ldots \oplus \langle \xi_{kl_k} \rangle$, where each $\langle \xi_{kj} \rangle$ is a cyclic group. Let E consist of these elements $\varepsilon \in X \restriction i+1$ which have only one non-zero coordinate and this coordinate has a form $\varepsilon(k) = \xi_{kj}$ for some $j \leq l_k$. For $\varepsilon \in E$ let E_ε be the set of elements of X_i with the exponent dividing the exponent of ε. It is easy to show (see [Kr1], the proof of Proposition 3.2.6) that for any $f \in H_{i+1}$ and $\varepsilon \in E$

$$(*) \qquad f(\varepsilon) = \begin{cases} \varepsilon, & \text{when } \varepsilon(i) \neq 0 \\ (\varepsilon \restriction i)^\frown \theta & \text{for some } \theta \in E_\varepsilon, \text{ otherwise.} \end{cases}$$

Conversely, when we choose arbitrarily $\theta_\varepsilon \in E_\varepsilon$ for each $\varepsilon \in E$, then there is a unique $f \in H_{i+1}$ such that for any $\varepsilon \in E$ the statement $(*)$ holds. From this description of H_{i+1} we see that it is an abelian group.

Part (2) of Claim 1 follows from the fact that there is a map $\rho : S_i \to S_{i+1}$ which is a section to $f_{i+1,i} : S_{i+1} \to S_i$. Namely, we define ρ by

$$\rho(g)(\eta) = g(\eta \restriction i)^\frown \eta(i). \ \square$$

To prove item (i) in Theorem 4.4.4 we proceed similarly. This time we put $S = Aut^*(X)$ and for $l \geq 1$

$$S_{2l} = Aut^*(X) \restriction (X \restriction l),$$

$$S_{2l+1} = Aut^*(X) \restriction Y_l,$$

where $Y_l = \{\eta : \eta \in X \restriction l \text{ or } \eta = (0, \ldots, 0, \eta(l)) \in X \restriction (l+1)\}$. Then

$$S \cong \varprojlim S_i,$$

where the connecting maps $f_{i,j} : S_i \to S_j$, $i > j$, are defined as restrictions.

To finish the proof we need to show Claim 1 in this context.

If i is odd we repeat the proof of Claim 1 with several obvious modifications. So assume that $i = 2l$. By the assumption of Theorem 4.4.4 we know that

$$X_l = \mathbb{Z}_{p_{l1}^{j_{l1}}} \times \ldots \times \mathbb{Z}_{p_{lk_l}^{j_{lk_l}}}.$$

Let

$$H_{2l+1} = ker(f_{2l+1,2l}) = \{g \in S_{2l+1} : g \restriction (X \restriction l) = id_{X \restriction l}\}.$$

We get here that

$$H_{2l+1} \cong Aut(X_l) = Aut(\mathbb{Z}_{p_{l1}^{j_{l1}}} \times \ldots \times \mathbb{Z}_{p_{lk_l}^{j_{lk_l}}}).$$

Hence H_{2l+1} is abelian.

To prove (2) in Claim 1 in our context we define a section $\rho : S_{2l} \to S_{2l+1}$ to $f_{2l+1,2l}$ by

$$\rho(g)(\eta) = \begin{cases} g(\eta), & \text{for } \eta \in X \restriction l \\ (0, \ldots, 0, \eta(l)), & \text{for } \eta = (0, \ldots, 0, \eta(l)) \in X \restriction (l+1). \end{cases} \quad \blacksquare$$

By Fact 4.3 and the proof of Fact 4.4 (see [Kr1], Theorem 3.2.1 and the proof of Proposition 3.2.6) or directly by Proposition 2.6 from [Kr2] we have that when we assume that profinite groups from Theorem 4.4.4 have finite exponents then they are small, m-normal and m-stable. So many profinite groups with good model theoretic properties are weakly interpretable in ACF_p over any Hilbertian field.

In particular, for any $n \in \omega$ and any prime number q we have that $(\mathbb{Z}^{\omega}_{q^n}, Aut^*(\mathbb{Z}^{\omega}_{q^n}))$ is weakly interpretable in ACF_p over any Hilbertian field. Corollary 3.2.4 from [Kr1] tells us that $\mathcal{M}(\mathbb{Z}^{\omega}_{q^n}) = n$. So we have weakly interpreted small m-normal profinite groups of arbitrary finite $\mathcal{M}$-rank.

The question arises whether all products of countably many finite abelian groups with the standard structural group are weakly interpretable in ACF_p over the field of rational functions or even over any Hilbertian field. More generally, we can also ask about weak interpretability of arbitrary abelian profinite groups.

Now we will discuss the differences between Methods 1 and 2. The advantage of the first method is the possibility of getting new examples of profinite structures, maybe yielding the positive answer to the questions like $(*)$ or $(**)$ from the introduction. Method 2 can not give new examples of profinite structures because in this method we start from a given profinite structure with a given structural group. This method allows us only to show weak interpretability in ACF_p of some profinite structures known in advance. Moreover, in contrast with Method 1, it does not yield any explicit weak interpretations of them.

The structural group of a profinite structure obtained by Method 1 is of course a Galois group over F. So there is a chance to obtain new Galois groups in this way. In Method 2 we use a solution of the inverse Galois problem to show that $Aut^*(X)$ is a Galois group over F, so we do not obtain a new Galois group here. However, there is one advantage of Method 2. If it works, it is much simpler.

The typical application of Method 1 can be seen in Subsections 4.1, 4.2, 4.3, where we start not from a given profinite structure but we construct in ACF_p a new profinite structure with prescribed properties. In some cases (e.g. in Subsections 4.1 and 4.3) we obtain more or less known profinite structures (easy to define abstractly, without using interpretations in fields) but there is still a chance to get completely new profinite structures giving the positive answer to the questions like $(*)$ or $(**)$ from the introduction. The application of Method 1 in Subsection 4.4 is not typical because we construct in ACF_p a given profinite structure.

Let F be a Hilbertian field of characteristic p. It is noteworthy that in Subsection 4.4 Method 1 gives such a weak interpretation over F of the profinite group $(\mathbb{Z}_p^{\omega}, S)$ that the group action becomes the field addition on each coordinate. On the other hand, Method 2 (see Theorem 4.4.4) shows that there are profinite groups of arbitrary exponent interpretable in ACF_p over F. We do not know explicit interpretations of such groups, but we know that if the exponent of a profinite group X is different from p, then the group action in X does not correspond to the field addition in any weak interpretation of X in ACF_p. Hence it seems that the weak interpretations of X are not so natural as in the case of $(\mathbb{Z}_p^{\omega}, S)$.

Let $(X, Aut^*(X))$ be a profinite group and F be a field of characteristic p. It would be interesting to find some general properties of $(X, Aut^*(X))$ which imply that it is weakly interpretable in ACF_p over F. For example, in Theorem 4.4.2, the assumption that $Aut^*(X)$ is a pro-p-group works, if F is the field of rational functions over F_p. However, it would be more interesting to find some properties (model theoretic or algebraic) of X (not of $Aut^*(X)$) which give the weak interpretability of $(X, Aut^*(X))$. This could yield new examples of Galois groups over a given field F. This is the new approach to the inverse Galois problem described in the introduction. If we assume something only about $Aut^*(X)$, then it seems that the only way to show that $(X, Aut^*(X))$ is weakly interpretable in ACF_p over F is to use a solution of the inverse Galois problem for groups satisfying these assumptions (as in the proof of Theorem 4.4.2). If we were able to use some general assumptions on X to show that $(X, Aut^*(X))$ is weakly interpretable in ACF_p over F, then it could turn out (by Theorem 3.1) that $Aut^*(X)$ is a new Galois group over F.

At the end of the paper we give some corollary to Subsection 4.1 for SCF_e. Namely, we can consider the notions of m-normality and m-stability for first order theories (see [N3]). Subsection 4.1 together with Theorem 2.2.1 and Proposition 2.2.6 give the following corollary.

Corollary 4.6 *SCF_e is not small, not m-normal and not m-stable.*

Of course, the fact that SCF_e is not small is well known. The proof of Corollary 4.6 is a standard forking calculation. We omit it here since it falls beyond the scope of this paper.

References

[Ba] J. T. Baldwin, *Fundamentals of stability theory*, Springer-Verlag, Heidelberg, 1988.

[BD] E. Bouscaren, F. Delon, *Minimal groups in separably closed fields*, J. Symb. Logic (67), No. 1, 239-259, 2002.

[Bu] S. Buechler, *Essential stability theory*, Springer-Verlag, Berlin, 1996.

[CCSSW] Z. Chatzidakis, G. Cherlin, S. Shelah, G. Srour, C. Wood, *Orthogonality of types in separably closed fields*, Classification theory, Proceedings of the 1985 Chicago conference, Lecture Notes in Mathematics, vol. 1292, Springer-Verlag.

[CW] Z. Chatzidakis, C. Wood, *Minimal types in separably closed fields*, J. Symb. Logic (65), No. 3, 1443-1450, 2000.

[D] F. Delon, *Idéaux et types sur les corps séparablement clos*, Supplément au Bull. de la S.M.F., Mémoire 33, Tome 116, 1988.

[FJ] M. D. Fried, M. Jarden, *Field arithmetic*, Springer-Verlag, Berlin, 1986.

[Ko] H. Koch, *Galois theory of p-extensions*, Mir, Moscow, 1973.

[Kr1] K. Krupiński, *Products of finite abelian groups as profinite groups*, Journal of Algebra (288), 556-582, 2005.

[Kr2] K. Krupiński, *Abelian profinite groups*, Fund. Math. (185), 41-59, 2005.

[M] D. Marker, *Model theory: an introduction*, Springer-Verlag, New York, 2002.

[MM] G. Malle, B .H. Matzat, *Inverse Galois Theory*, Springer-Verlag, Berlin, 1999.

[MMP] D. Marker, D. Messmer, A.Pillay, *Model theory of fields*, Springer-Verlag, Berlin, 1996.

[N1] L. Newelski, *Small profinite groups*, J. Symb. Logic (66), 859-872, 2001.

[N2] L. Newelski, *Small profinite structures*, Trans. Amer. Math. Soc. (354), 925-943, 2002.

[N3] L. Newelski, *$\mathcal{M}$-gap conjecture and m-normal theories*, Israel Journal of Math. (106), 285-311, 1998.

[Pi] A. Pillay, *Geometric stability theory*, Clarendon Press, Oxford, 1996.

[Po] B. Poizat, *Groupes stables*, Nur al-Mantiq wal-Ma'rifah, Villeurbanne, 1987.

[RZ] L. Ribes, P. Zaleski, *Profinite groups*, volume 40, Springer, 2000.

[S] G. E. Sacks, *Saturated model theory*, W. A. Benjamin, Inc. 1972.

[W] F. Wagner, *Small profinite m-stable groups*, Fund. Math. (176), 181-191, 2003.

address:
Mathematical Institute, University of Wrocław,
pl. Grunwaldzki 2/4, 50-384 Wrocław, Poland
e-mail: kkrup@math.uni.wroc.pl
and
Mathematical Institute of the Polish Academy of Sciences