ILLINOIS JOURNAL OF MATHEMATICS
Volume 42, Number 1, Spring 1998

MODEL THEORY OF PROFINITE GROUPS HAVING THE IWASAWA PROPERTY[1]

ZOÉ CHATZIDAKIS

Introduction

The notion of complete systems of finite groups first appeared in a paper by Cherlin, Van den Dries and Macintyre [CDM], where it was used to give invariants for the theory of regularly closed fields (see also the work of Eršov [E]).

To a profinite group G they associate the complete system $S(G)$, which encodes the inverse system of all finite (continuous) quotients of G together with the projection maps. In an appropriate language, the systems $S(G)$ are ω-sorted structures and form an elementary class. The connection with field theory is obtained as follows: for K a field and $G(K)$ the absolute Galois group of K (i.e., the Galois group of K in its separable closure), the theory of the system $S(G(K))$ is interpretable in $\mathrm{Th}(K)$, and is in some sense the strongest such theory.

Besides field theory, complete systems can also be used to study profinite groups. Their main advantage is that one replaces the study of a group together with its topology, by the study of a fairly simple algebraic system. An other advantage is that by dualizing, one works with embeddings of complete systems instead of continuous epimorphisms of profinite groups.

The profinite groups we are interested in are the profinite groups having the Iwasawa property (IP). This property was first discovered by Iwasawa [I], who used it to characterize countably generated free profinite groups. This property was then considered by Cherlin, Van den Dries and Macintyre [CDM], and by Haran and Lubotzky [HL], among others.

The main result concerning the Iwasawa property given in [CDM], is that $\mathrm{Th}(S(G))$ is $\aleph_0$-categorical when G has the Iwasawa property. It turns out that the types are easy to describe, and that $\mathrm{Th}(S(G))$ is ω-stable. This allows one to use all the existing stability theoretic machinery in the study of these groups.

Besides characterizations of some model-theoretic properties, the main algebraic results obtained in this paper are:

THEOREM 2.6. *Let H be a profinite group. Then H has a universal* IP*-cover G, which is unique up to isomorphism over H.*

Received January 16, 1997.
1991 Mathematics Subject Classification. Primary 03C60, 20E18; Secondary 03C45.
[1] Most of this work is part of the author's Ph. D. thesis, Yale University, 1984.

The definition of universal IP-covers is analogous to the one of projective covers. The case when H is finitely generated was obtained by Haran and Lubotzky [HL], using algebraic methods. The use of Shelah's theorem on the uniqueness of the prime model for ω-stable theories plays a major part in the proof of Theorem 2.6, and seems unavoidable, in view of the fact that a universal IP-cover can have proper quotients which are also universal IP-covers.

We also give a description of saturated models, and derive from it a result originally obtained by Mel'nikov [Me1] on free pro-$\mathcal{C}$-groups. This also gives an alternate description of free pro-$\mathcal{C}$-groups, see Corollary 3.2. From this description one obtains:

THEOREM 3.5. *Let $(K_i)_{i\in I}$ be a family of fields with free absolute Galois groups. Let $\mathcal{U}$ be an ultrafilter on I and let $K = \prod_{i\in I} K_i/\mathcal{U}$. Then $G(K)$ is free.*

For κ an infinite cardinal, we also characterize the profinite groups G having the following property, which we call κ-strong homogeneity: Every isomorphism between two quotients of G having less than κ open subgroups lifts to an automorphism of G.

THEOREM 6.4. *Suppose that G is κ-strongly homogeneous. Let N be a normal subgroup of G such that $|S(G/N)| < \kappa$ and let U be a characteristic subgroup of N. Then every automorphism of G/U lifts to an automorphism of G.*

This result extends results given by Mel'nikov in [Me2]. The group of automorphisms of a strongly homogeneous group has other nice properties; see 6.5. We also produce an example of a group having the Iwasawa property which is not ω-strongly homogeneous, thus answering by the negative a question posed in [HL].

We conclude this paper with a study of the pro-p-groups having the Iwasawa property, and show that they are exactly the quotients of free pro-p-groups by characteristic subgroups. The main result (Theorem 7.1) shows that the isomorphism type of such groups is entirely determined by the set of isomorphism classes of their finite quotients, and by the size of a minimal set of generators.

From a model-theoretic point of view, the groups with the Iwasawa property provide an abundant supply of $\aleph_0$-categorical ω-stable theories. In [C], we describe the groups with the Iwasawa property whose theory is non-multidimensional or has the NDOP.

1. Profinite groups and their complete systems

(1.1) *Conventions.* Throughout this paper, all subgroups of profinite groups are closed, all morphisms between profinite groups are continuous epimorphisms, and all quotients of profinite groups are continuous quotients.

(1.2) We recall that a profinite group G is a topological group which is compact, Haussdorff and totally disconnected. The open subgroups of G (which are therefore of finite index) form a base for the neighbourhoods of 1. Equivalently, a profinite group is an inverse limit of finite groups. We refer to [Ri] for the properties of profinite groups.

(1.3) *Definition of* $S(G)$. Let G be a profinite group, and $N \subseteq M$ open normal subgroups of G. There is a natural epimorphism $\pi_{MN}\colon G/N \to G/M$, and the system of all finite quotients of G together with the epimorphisms π_{MN} is a projective system. Relative to this system one has

$$G = \varprojlim G/N.$$

Thus G is completely determined by the projective system of its finite quotients, and conversely. This leads us to the following definition. Let $\mathcal{L}$ be the language $\{\leq, C, P, 1\}$.

To G we associate the $\mathcal{L}$-structure $S(G)$ with universe the set of all cosets gN of open normal subgroups N of G. The structure on $S(G)$ is defined by:

$gN \leq hM$ if and only if $N \subseteq M$.
$1 = gG$.
$P(g_1N_1, g_2N_2, g_3N_3)$ if and only if $N_1 = N_2 = N_3$ and $g_1g_2N_1 = g_3N_3$.
$C(gN, hM)$ if and only if $N \subseteq M$ and $gM = hM$.

Thus, C encodes the group epimorphisms π_{MN}, P the group multiplication on the finite quotients G/N, and 1 corresponds to the trivial quotient of G.

It is clear that, as given above, the class of the $S(G)$ is not elementary. To make it into an elementary class, we will transform $S(G)$ into a many-sorted structure. We first recall briefly the definition of many-sorted languages and structures.

(1.4) *Many-sorted languages.* A many-sorted language $\mathcal{L}$ is specified by a non-empty set J of sorts, a set of relations $(R_i)_{i\in I_0}$, a set of constants $(c_i)_{i\in I_1}$ and a set of functions $(F_i)_{i\in I_2}$. In addition to these symbols, $\mathcal{L}$ contains infinitely many variables of each sort; each variable has a sort and variables of distinct sorts are distinct. Formulas are built in the usual manner, and the classical results (compactness, completeness, ...) hold. See [KK] for more details.

An $\mathcal{L}$-structure is a structure $\mathbf{M} = \langle (M_j)_{j\in J}; (R_i)_{i\in I_0}, (c_i)_{i\in I_1}, (F_i)_{i\in I_2}\rangle$ where:

The elements of M_j are of sort j, and M_j is non-empty. Let $M = \bigcup_{j\in J} M_j$.
Each R_i is contained in $M^{k(i)}$ for some integer $k(i)$.
Each c_i is an element of sort $\ell(i)$ for some $\ell(i) \in J$, and therefore $c_i \in M_{\ell(i)}$.
Each F_i is a function : $M_{j(1)} \times \cdots \times M_{j(m)} \to M_{j(m+1)}$ for some integer m and $(m+1)$-tuple $(j(1), \ldots, j(m+1)) \in J^{m+1}$.

Many-sorted logic usually requires that $M_j \cap M_k = \emptyset$ for $j \neq k \in J$. We will drop this requirement, by noting that a structure $\mathbf{M}$ with non-disjoint sorts can be made into a structure $\mathbf{M}'$ with disjoint sorts by adding to the language binary relations $R^{(j,k)}$ for each pair (j, k) of distinct elements of J, and using them to identify the elements of $M_j \cap M_k$.

(1.5) *The ω-sorted structure $S(G)$.* We now view $\mathcal{L}$ as a many-sorted language indexed by the positive integers. We assign to the elements of $S(G)$ sorts in the following manner:

$$gN \text{ is of sort } n \iff [G : N] \leq n.$$

Note that $S(G)_n \subseteq S(G)_{n+1}$ for every n, and that $\bigcap S(G)_n = \{1\}$.

We call the ω-structure $S(G)$ the complete system associated to G. The theory T_0 of the systems $S(G)$ is then axiomatized as follows:

(1) $\leq$ is reflexive and transitive, with a unique largest element, 1.

Let $\sim$ denote the equivalence relation induced by the preorder $\leq$ (i.e., $x \sim y$ if and only if $x \leq y$ and $y \leq x$), and let $[x]$ denote the $\sim$-equivalence class of x.

(2) $P \subseteq \bigcup [x]^3$ and $P \cap [x]^3$ defines a group law on $[x]$ for every x.
(3) $C \subseteq \bigcup_{x \leq y} [x] \times [y]$, and for every $x \leq y$, $C \cap [x] \times [y]$ is the graph of a group epimorphism $\pi_{xy}\colon [x] \to [y]$.
(4) If V is a normal subgroup of $[x]$, there is a unique $[y]$ such that V is the kernel of π_{xy}.
(5) If $x \leq y \leq z$, then $\pi_{yz} \circ \pi_{xy} = \pi_{xz}$; $\pi_{xx} = id_{[x]}$.
(6) $S(G)/\sim$ is a lattice. (Note that $[N] \vee [M] = [NM]$ and $[N] \wedge [M] = [N \cap M]$; this gives the appropriate bounds on the sorts.)
(7) An element is of sort n if and only if its $\sim$-equivalence class has at most n elements.

It is clear that if G is a profinite group then $S(G)$ satisfies these axioms. Conversely, let S be a model of T_0. Then S encodes a projective system $\{[\alpha]; \pi_{\alpha\beta} \mid \alpha \leq \beta \in S\}$ of finite groups. Let $G(S)$ be the profinite group defined by this system. Then axioms (4) and (6) ensure that $S = S(G(S))$. One also has $G(S(G)) = G$. For $\alpha \in S$, denote by π_α the projection $G(S) \to [\alpha]$; then $\pi_\beta = \pi_{\alpha\beta} \circ \pi_\alpha$ for $\alpha \leq \beta \in S$.

Furthermore, let $\varphi\colon G \to H$ be an epimorphism. Then φ induces an embedding $S(\varphi)\colon S(H) \to S(G)$ defined by $S(\varphi)(gN) = \varphi^{-1}(gN)$. Conversely, if S_1, S_2 are models of T_0 and $f\colon S_1 \to S_2$ is an embedding of $\mathcal{L}$-structures, there is an epimorphism $G(f)\colon G(S_2) \to G(S_1)$ such that $SG(f) = f$. The definition of $G(f)$ follows from the following observations: the restriction of f to $[\alpha]$ is an isomorphism onto $[f(\alpha)]$ for every $\alpha \in S_1$; if $\alpha \leq \beta \in S_1$, then $\pi_{\alpha\beta} \circ f^{-1} = f^{-1} \circ \pi_{f(\alpha)f(\beta)}$; hence we have a system $\{f^{-1} \circ \pi_{f(\alpha)} \mid \alpha \in S_1\}$ compatible with the system $\{[\alpha], \pi_{\alpha\beta} \mid \alpha \leq$

$\beta \in S_1\}$, which gives a morphism $G(f)$: $G(S_2) \to G(S_1)$; the image of $G(S_2)$ being dense in $G(S_1)$, $G(f)$ is onto.

Note that if f is an inclusion $S_1 \subseteq S_2$ then $G(f)$ is the canonical projection $G(S_2) \to G(S_2)/N$ with $N = \bigcap\{\mathrm{Ker}\,\pi_\alpha \mid \alpha \in S_1\}$.

We will often refer to φ and $S(\varphi)$, or to f and $G(f)$, as dual of each other.

(1.6) *Connections with* 1*-sorted logic.* Let $\mathcal{L}^*$ be the language $\{S_n, \leq^{nm}, C^{nm}, P^n, 1 \mid m, n \in \mathbb{N}^{>0}\}$; we associate to an $\mathcal{L}$-structure S the $\mathcal{L}^*$-structure S^*, with the same universe as S and where, for $a, b, c \in S$ we have:

$$\begin{aligned}
S^* \models S_n(a) &\iff a \text{ is of sort } n \text{ in } S\\
S^* \models a \leq^{nm} b &\iff S^* \models S_n(a) \wedge S_m(b) \text{ and } S \models a \leq b\\
S^* \models C^{nm}(a,b) &\iff S^* \models S_n(a) \wedge S_m(b) \text{ and } S \models C(a,b)\\
S^* \models P^n(a,b,c) &\iff S^* \models S_n(a) \wedge S_n(b) \wedge S_n(c) \text{ and } S \models P(a,b,c).
\end{aligned}$$

To T_0 we associate an $\mathcal{L}^*$-theory T_0^* in the obvious manner, replacing occurences of $\exists x$ by $\exists x\ S_n(x)\wedge$ where x is of sort n, and similarly for $\forall x$. The structures S^* are then precisely the models of T_0^* which omit the type $\Sigma(x) = \{\neg S_n(x) \mid n > 0\}$. Conversely, a model of T_0^* is of the form $S^* \cup S'$ with $S \models T_0$ and S' the set of realizations of $\Sigma(x)$ (on which there is therefore no structure).

Most of the classical results of 1-sorted logic extend to ω-sorted logic. In particular, all the model-theoretic results involving a "local" behaviour of types, such as forking and orthogonality, remain unchanged in many-sorted logic; see for example the treatment of T^{eq}. At the "global level", let us note the following differences:

(1) If a many-sorted structure S is small, i.e., has only finitely many elements of each sort, then it is the unique model of its theory. Thus small structures are the analogue of finite structures in the 1-sorted case.
(2) (Ryll-Nardzewsky Theorem) A many-sorted theory T is $\aleph_0$-categorical if and only if for every n and n-tuple $j_1, \dots, j_n$ of sorts, there are only finitely many n-types of sort $(j_1, \dots, j_n)$.

(1.7) *Substructures.* Let $A \subseteq S(G) \models T_0$. Then $A \models T_0$ if and only if A satisfies the following conditions: $\alpha \leq \beta$ and $\alpha \in A$ imply $\beta \in A$; the restriction of $\leq$ to A is downward directed. By (1.5), A corresponds to a quotient of G. Since we are only interested in profinite groups, we will make the following definition:

Definition. Let $S \models T_0$ and $A \subseteq S$. A is a substructure of S if A satifies the following:

(1) For all x and y, if $x \leq y$ and $x \in A$, then $y \in A$.
(2) For all x and y in A, there is z in A such that $z \leq x$ and $z \leq y$.

If $A \subseteq S \models T_0$, we denote by $\langle A \rangle$ the smallest substructure of S containing A. Note that our notion of substructure is different from the usual one; it can be made to coincide with the usual one by enlarging appropriately the language.

Remark. If A is a finite substructure of S, then A has a minimal element α for $\leq$, which is unique up to $\sim$. Then, as groups, $[\alpha]$ and $G(A)$ are isomorphic. Furthermore, the elements of A are definable from the elements of $[\alpha]$.

(1.8) We conclude this section with some properties of the systems $S(G)$.

Conventions and notation. We use $S(G)$, $S(H)$ to denote models of T_0, with associated profinite groups G, H. For $\alpha, \beta \in S(G)$ and A a substructure of $S(G)$, we define $\alpha \wedge \beta$ to be the greatest lower bound of α and β satisfying $P(\alpha \wedge \beta, \alpha \wedge \beta, \alpha \wedge \beta)$; thus $\alpha \wedge \beta$ is the identity element of $[\alpha \wedge \beta]$. Similarly, we define $\alpha \vee \beta$ to be the least upper bound of α and β satisfying $P(\alpha \vee \beta, \alpha \vee \beta, \alpha \vee \beta)$. Finally, we denote by $\alpha \vee A$ the infimum of the (finite) set $\{\alpha \vee \gamma \mid \gamma \in A\}$.

(1.9) LEMMA. *Let $\alpha \leq \beta, \gamma \in S(G)$ and assume that $\beta \vee \gamma = \delta$. Then*

(1) $\operatorname{Ker} \pi_{\alpha\beta\wedge\gamma} = \operatorname{Ker} \pi_{\alpha\beta} \cap \operatorname{Ker} \pi_{\alpha\gamma}$.
(2) $\operatorname{Ker} \pi_{\alpha\beta\vee\gamma} = \operatorname{Ker} \pi_{\alpha\beta} \operatorname{Ker} \pi_{\alpha\gamma}$.
(3) $[\beta \wedge \gamma] \simeq [\beta] \times_{[\delta]} [\gamma] = \{(a, b) \in [\beta] \times [\gamma] \mid \pi_{\beta\delta}(a) = \pi_{\gamma\delta}(b)\}$.
(4) (*Modular equality*) $\alpha \vee (\beta \wedge \varepsilon) = \beta \wedge (\alpha \vee \varepsilon)$.
(5) (*Symmetry*) $\varepsilon \vee (\beta \wedge \gamma) < \varepsilon \vee \beta$ *implies* $\gamma \vee (\beta \wedge \varepsilon) < \gamma \vee \beta$.

Proof. (1) and (2) are obvious. For (3), by dualizing, it suffices to show that if N_1 and N_2 are normal subgroups of a group G, then the morphism

$$f\colon G/N_1 \cap N_2 \to G/N_1 \times G/N_2,$$

induced by the canonical projections $G/N_1 \cap N_2 \to G/N_1$ and $G/N_1 \cap N_2 \to G/N_2$, is an isomorphism onto $G/N_1 \times_{G/N_1N_2} G/N_2$. The morphism f is clearly injective and takes its values in $G/N_1 \times_{G/N_1N_2} G/N_2$. Let $(gN_1, hN_2) \in G/N_1 \times_{G/N_1N_2} G/N_2$; there exist $n_1 \in N_1$ and $n_2 \in N_2$ such that $n_1 n_2 = g^{-1}h$; then $gn_1 = hn_2^{-1}$ is our desired element.

For (4), let $N_1 \subseteq N_2$ and N_3 be normal subgroups of G. The inclusion $N_1(N_2 \cap N_3) \subseteq (N_1N_2) \cap (N_1N_3)$ ($= N_2 \cap (N_1N_3)$) always holds. For the reverse inclusion, let $g \in N_1$ and $h \in N_3$ be such that $gh \in N_2$. Then $g^{-1}gh \in N_2$, and therefore $h \in N_2 \cap N_3$.

For (5), let N_1, N_2 and N_3 be normal subgroups of a group G such that $N_1(N_2 \cap N_3) \subsetneq N_1N_2$, and let $n \in N_2$ be such that $ng \notin N_2 \cap N_3$ for every $g \in N_1$. Suppose that for some $g \in N_3$ we have $ng \in N_1 \cap N_2$. Then $g \in N_2 \cap N_3$ and $(ng)^{-1}n \in N_2 \cap N_3$, which is a contradiction. Therefore $N_3(N_1 \cap N_2) \subsetneq N_3N_2$.

In fact this property holds in all modular lattices.

(1.10) *The length function.*

Definition. Let $\alpha \leq \beta \in S(G) \models T$, and let $A \subseteq S(G)$. We define the length of α over β, $L(\alpha/\beta)$, to be the largest integer n such that there exists a chain

$$\alpha = \alpha_0 < \alpha_1 < \cdots < \alpha_n = \beta.$$

Thus, $L(\alpha/\beta) = 0$ if and only if $\alpha \sim \beta$; $L(\alpha/\beta) = 1$ if and only if α is an immediate strict predecessor of β for $\leq$ (if and only if $\operatorname{Ker} \pi_{\alpha\beta}$ is a minimal normal subgroup of $[\alpha]$).

Similarly, we define $L(\alpha/A)$ to be $L(\alpha/\alpha \vee \langle A\rangle)$. Thus, $L(\alpha/A) = 0$ if and only if $\alpha \in \langle A\rangle$.

Note that because of Jordan-Hölder Theorem on principal series, $L(\alpha/\beta)$ does not depend on the choice of the sequence $\alpha_0, \ldots, \alpha_n$. Even though $L(\alpha/\beta)$ does not usually coincide with $U(\alpha/\beta)$, the length function shares some of the properties of ranks. The following is immediate:

LEMMA. *Let $\alpha, \beta, \gamma \in S(G)$ with $\gamma < \beta$. Then $L(\gamma \wedge \alpha/\beta \wedge \alpha) \leq L(\gamma/\beta)$, and equality holds iff $\gamma \vee \alpha \geq \beta$.*

2. The Iwasawa property – universal IP-covers

(2.1) *Definitions.* Let G be a profinite group.

(1) The image of G, $\operatorname{Im}(G)$, is the set of isomorphism classes of finite quotients of G.
(2) G has the Iwasawa property (from now on abbreviated by IP) if for every epimorphism θ: $B \to A$ of finite groups with $B \in \operatorname{Im}(G)$, and for every epimorphism φ: $G \to A$, there is an epimorphism ψ: $G \to B$ such that $\varphi = \theta \circ \psi$.

We will denote by T_{IP} the theory obtained by adjoining to T_0 the following scheme of axioms: for every epimorphism θ: $B \to A$ of finite groups, a first-order sentence expressing for all x, if $[x]$ is isomorphic to A by an isomorphism φ, and if there exists y such that $[y]$ is isomorphic to B, then there exists $y \leq x$ and an isomorphism ψ: $[y] \to B$ such that $\varphi \circ \pi_{yx} = \theta \circ \psi$.

Then, $S(G) \models T_{IP}$ whenever G has IP, and conversely, if $S \models T_{IP}$, then $G(S)$ has IP.

(2.2) The next result was proved by Cherlin-Van den Dries-Macintyre in [CDM], but is to our knowledge unpublished.

THEOREM. *Let G and H be two profinite groups having IP. If* $|S(G)| = |S(H)| = \aleph_0$ *and* $\mathrm{Im}(G) = \mathrm{Im}(H)$ *then* $G \simeq H$.

Proof. The proof is a standard back and forth argument between $S(G)$ and $S(H)$. Fix enumerations $(\alpha_n)_{n\in\mathbb{N}}$ and $(\beta_n)_{n\in\mathbb{N}}$ of the elements of $S(G)$ and $S(H)$. The main step is as follows:

Suppose that we have constructed an isomorphism f between two finite substructures A and B of $S(G)$ and $S(H)$ respectively, let $i \in \mathbb{N}$ be minimal such that $\alpha_i \notin A$, and let $\alpha \in A$ and $\beta \in B$ be minimal (for $\leq$). Then $\langle\alpha\rangle = A$ and $\langle\beta\rangle = B$, and the restriction of f to $[\alpha]$ is an isomorphism onto $[\beta]$; let $[\gamma] = [\alpha \wedge \alpha_i]$; by IP, there exist $\delta \in S(H)$ and an isomorphism g: $[\gamma] \to [\delta]$ such that

$$f \circ \pi_{\gamma\alpha} = \pi_{\delta\beta} \circ g.$$

Since $[\gamma] \simeq G(\langle A, \alpha_i\rangle)$, g extends uniquely to an isomorphism g' between $\langle A, \alpha_i\rangle = \langle\gamma\rangle$ and $\langle\delta\rangle$. From the definition of g, it follows that g' extends f.

This theorem has important corollaries, which we will now list.

(2.3) THEOREM [CDM]. *Suppose that G has IP. Then*:

(1) $\mathrm{Th}(S(G))$ *is axiomatized by* T_{IP} *together with the following axioms, for every* $A \in \mathrm{Im}(G)$ *and* $B \notin \mathrm{Im}(G)$: *there exists* x (*of sort* $|A|$) *such that* $[x] \simeq A$; *for all* x, $[x] \not\simeq B$.
(2) $\mathrm{Th}(S(G))$ *is* $\aleph_0$*-categorical.*

(2.4) Another application of Theorem 2.2, or rather of its proof, is a characterization of the types.

THEOREM. *Let A be a substructure of* $S(G) \models T_{IP}$, *and let* $\alpha, \beta \in S(G)$. *Then*:

(1) $t(A/\emptyset)$ *is determined by the isomorphism type of* A.
(2) $t(\alpha/A) = t(\beta/A)$ *if and only if* $\alpha \vee A = \beta \vee A = \gamma$ *and there is an isomorphism* f: $[\alpha] \to [\beta]$ *such that* $f(\alpha) = \beta$ *and* $\pi_{\alpha\gamma} = \pi_{\beta\gamma} \circ f$.
(3) $\mathrm{Th}(S(G))$ *is* ω*-stable.*

Proof. (1) By compactness, it suffices to prove the result for A finite, and we may assume that $S(G)$ is countable. But this follows immediately from the main step of Theorem 2.2.

(2) As in (1), we may assume that A is finite and that $S(G)$ is countable. Since $t(\alpha/A) \vdash t(\alpha/\langle\gamma\rangle)$, the existence of such an f is necessary. For the converse, let $\delta \in A$ be minimal for $\leq$; then $G(\langle A, \alpha\rangle)$ is isomorphic to $[\alpha] \times_{[\gamma]} [\delta]$, and $G(\langle A, \beta\rangle)$ is

isomorphic to $[\beta]\times_{[\gamma]}[\delta]$. There is therefore an isomorphism g between $G(\langle\delta,\alpha\rangle)$ and $G(\langle\delta,\beta\rangle)$ which lifts the isomorphisms f and $id_{[\delta]}$. The dual of g is an isomorphism between $\langle A,\alpha\rangle$ and $\langle A,\beta\rangle$ which sends α to β and is the identity on A.

(3) We first note that the study of n-types reduces to the study of 1-types: indeed, let $\alpha_1,\dots,\alpha_n \in S(G)$, and let $\alpha = \alpha_1 \wedge \dots \wedge \alpha_n$. Then $\alpha \in \mathrm{acl}(\alpha_1,\dots,\alpha_n)$ and $\alpha_1,\dots,\alpha_n \in \mathrm{acl}(\alpha)$.

Suppose that A is a countable subset of $S(G)$. Then the substructure generated by A is also countable and we may therefore assume that A is a substructure of $S(G)$. By (2), the type of an element $\alpha \in S(G)$ is determined by: $\alpha \vee A$ — $|A|$ many possibilities; by the isomorphism type of $[\alpha]$ — countably many possibilities; and by the map $\pi_{\alpha\alpha\vee A}$ — finitely many possibilities. There are therefore only countably many types over A.

(2.5) *Isolated types.*

PROPOSITION. *Let $S(G) \models T_{IP}$, let $A \subseteq S(G)$ and $\alpha \in S(G)$. Let $\beta = \alpha \vee \langle A\rangle$ and let B be the set of all elements $\delta \in \langle A\rangle$ satisfying: there exists an immediate (strict) predecessor γ of β such that $\alpha \le \gamma$ and $t(\gamma/\langle\beta\rangle) = t(\delta/\langle\beta\rangle)$.*

Then $t(\alpha/A)$ is isolated if and only if B is finite.

Proof. Suppose that B is finite. Then $t(\alpha/\langle A\rangle)$ is isolated by $t(\alpha/\langle\beta\rangle) \cup \{x \not\le \delta \mid \delta \in B\}$. Since $\langle A\rangle$ is atomic over A, $t(\alpha/A)$ is isolated.

For the converse, we may assume that $S(G)$ is countable. Let $\varphi(x)$ be a formula with parameters in A satisfied by α, let C be the (finite) substructure of $\langle A\rangle$ generated by β and the parameters of φ. If B is infinite, then there exists $\delta \in B\setminus C$, and we have $\delta \vee C = \beta$. Let f be an automorphism of $S(G)$ which leaves C fixed and sends δ to an element γ with $\alpha \le \gamma$. Then $f^{-1}(\alpha)$ satisfies $\varphi(x)$, but $f^{-1}(\alpha) \vee \langle A\rangle \le \delta < \beta$. Hence $\varphi(x)$ does not isolate $t(\alpha/A)$.

(2.6) *Definition.* Let H be a profinite group. A profinite group G, together with an epimorphism $\varphi\colon G \to H$, is a universal IP-cover of H if G has IP, and for every profinite group G' having IP and epimorphism $\psi\colon G' \to H$, there is an epimorphism $\theta\colon G' \to G$ such that $\psi = \varphi \circ \theta$.

We are going to prove that every profinite group H has a universal IP-cover, which furthermore is unique up to isomorphism over H. This result was proved by D. Haran and A. Lubotzky [HL] in the case of a finitely generated profinite group H. Given H, they show how to compute effectively the image of the universal IP-cover G, and show that G has the same rank as H. Their method of proof however cannot be generalized to the infinite rank case.

(2.7) THEOREM. *Let H be a profinite group. Then H has a universal IP-cover G, which is unique up to isomorphism over H.*

Proof. We will first determine the theory of $S(G)$. If $A \in \mathrm{Im}(H)$, then A has a universal IP-cover by results from [HL]. Let Γ be the set of isomorphism classes of finite groups B such that B is a homomorphic image of the universal IP-cover of A for some $A \in \mathrm{Im}(H)$. Let T be the theory

$$T = T_{IP} \cup \mathrm{Diag}(S(H)) \cup \{\exists x\ [x] \simeq A \mid A \in \Gamma\} \cup \{\forall x\ [x] \not\simeq A \mid A \notin \Gamma\}.$$

We first claim that T is consistent. Let C be a finite substructure of $S(H)$, $A_1, \ldots, A_n \in \Gamma$ and $B_1, \ldots, B_m \notin \Gamma$; choose $\delta_1, \ldots, \delta_n \in S(H)$ such that A_i is a homomorphic image of the universal IP-cover of $[\delta_i]$ for every i, and let $D = \langle C, \delta_1, \ldots, \delta_n\rangle$. Then D is finite, and therefore, if E is the universal IP-cover of $G(D)$, then $A_1, \ldots, A_n \in \mathrm{Im}(E) \subseteq \Gamma$ and $B_1, \ldots, B_m \notin \mathrm{Im}(E)$. This shows that T is finitely consistent, and hence consistent. By Theorem 2.4(1), T is also complete.

The proof of the existence and uniqueness of prime models for ω-stable theories generalises easily to the ω-sorted case. Let $S(G)$ be a model of T prime over $S(H)$ and let $\pi\colon G \to H$ be the epimorphism dual to the inclusion $S(H) \subseteq S(G)$. Then $S(G)$ is unique up to $S(H)$-isomorphism. We will show that $\pi\colon G \to H$ is the universal IP-cover of H.

Let $S(M) \models T_{IP}$, $S(H) \subseteq S(M)$. Then $\mathrm{Im}(M)$ contains Γ because M has IP. Let $\mathcal{F}$ be the set of all substructures A of $S(M)$ containing $S(H)$ and such that $\mathrm{Im}(G(A)) \subseteq \Gamma$. Then $\mathcal{F}$ is non-empty and is inductive (for the inclusion). It therefore has a maximal element, which we will call $S(G')$. Since $\mathrm{Im}(G') \subseteq \Gamma$, it remains to show that $S(G') \models T_{IP}$. Let $\alpha \in S(G')$, $B \in \Gamma$ and let $\theta\colon B \to [\alpha]$ be an epimorphism. Because $S(M) \models T_{IP}$, there exist $\beta \in S(M)$ and an isomorphism $\psi\colon [\beta] \to B$ such that $\pi_{\beta\alpha} = \theta \circ \psi$. If $\beta \in S(G')$, we are done. Suppose therefore that $\beta \notin S(G')$.

Let us first assume that $L(\beta/\alpha) = 1$. By the definition of $S(G')$, there is $\gamma \in S(G')$ such that $\beta \wedge \gamma \notin \Gamma$. We may assume $\gamma \leq \alpha$, which gives $\beta \vee \gamma \sim \alpha$.

Let $S(N) \models T$ and let α', β', $\gamma' \in S(N)$ be such that the following diagrams commute for some isomorphisms φ_0, φ_1 and φ_2 (the vertical maps being the canonical epimorphisms encoded by C):

$$\begin{array}{ccc} [\beta] & \xrightarrow{\varphi_1} & [\beta'] \\ \downarrow & & \downarrow \\ [\alpha] & \xrightarrow{\varphi_0} & [\alpha'] \end{array} \qquad\qquad \begin{array}{ccc} [\gamma] & \xrightarrow{\varphi_2} & [\gamma'] \\ \downarrow & & \downarrow \\ [\alpha] & \xrightarrow{\varphi_0} & [\alpha']. \end{array}$$

Then $\beta' \vee \gamma' \leq \alpha'$ because $\beta' \leq \alpha'$ and $\gamma' \leq \alpha'$. If $\beta' \vee \gamma' \sim \alpha'$, then $[\beta' \wedge \gamma'] \simeq [\beta \wedge \gamma] \notin \Gamma$, a contradiction. Therefore $\beta' \vee \gamma' < \alpha'$, and because β' is an immediate predecessor of α', we obtain $\beta' \vee \gamma' \sim \beta'$; i.e., $\gamma' \leq \beta'$. Let $V = \varphi_2^{-1}(\mathrm{Ker}\,\pi_{\gamma'\beta'})$ and let δ be such that $V = \mathrm{Ker}\,\pi_{\gamma\delta}$. Then $\delta \in S(G')$ and for some isomorphism $\varphi\colon [\delta] \to B$, $\pi_{\delta\alpha} = \theta \circ \varphi$.

For the general case, find a sequence $\beta = \beta_1 < \beta_2 \ldots < \beta_n = \alpha$ such that $L(\beta_i/\beta_{i+1}) = 1$ for every i, and use the first case to find $\delta \in S(G')$ realizing

$t(\beta/\langle\alpha\rangle)$. This shows that $S(G') \models T_{IP}$. Because $S(G)$ is prime over $S(H)$, there is an embedding $f\colon S(G) \to S(G')$ which is the identity on $S(H)$. By dualizing we obtain the result.

Remarks. (1) The universal cover of H is in general not minimal; it may have proper quotients which are also universal IP-covers of H.

(2) Let G_1 and G_2 be profinite groups having IP and suppose that $\mathrm{Im}(G_1) \subseteq \mathrm{Im}(G_2)$. Let G be a quotient of G_2 maximal with the property that $\mathrm{Im}(G) \subseteq \mathrm{Im}(G_1)$. Then G has IP and $\mathrm{Im}(G) = \mathrm{Im}(G_1)$. This is an immediate consequence of the proof of the theorem.

3. Saturated models and free profinite groups

(3.1) PROPOSITION. *Let $S(G) \models T_{IP}$ and let κ be an infinite cardinal. Then $S(G)$ is κ-saturated if and only if, for every $\alpha < \beta \in S(G)$ with $L(\alpha/\beta) = 1$, $t(\alpha/\langle\beta\rangle)$ is realized either finitely many times (i.e., is algebraic), or is realized at least κ times.*

Proof. The necessity of our condition is obvious. Conversely, suppose that $S(G)$ satisfies the above condition, and let A be a substructure of $S(G)$ of cardinality $< \kappa$, let p be a type over A and let α be an element (in some large extension of $S(G)$) realizing p. Let $\beta = \alpha \vee A$. If p is algebraic then p is realized in $S(G)$ because p is isolated. We may therefore assume that p, and therefore $t(\alpha/\langle\beta\rangle)$, is not algebraic. We will first assume that $L(\alpha/\beta) = 1$. The set of realizations of $t(\alpha/\langle\beta\rangle)$ has size κ, and is therefore not contained in A. Hence there exists $\alpha' \in S(G) \setminus A$ which realizes this type. Then $\alpha' \vee A = \beta$ because $L(\alpha'/\beta) = 1$ and $\alpha' \notin A$.

For the general case, let $\alpha = \alpha_1 < \alpha_2 < \dots < \alpha_n = \beta$ be such that $L(\alpha_i/\alpha_{i+1}) = 1$ for every i and use the first case to realize successively $t(\alpha_{n-1}/A)$, $t(\alpha_{n-2}/\langle A, \alpha_{n-1}\rangle)$, $\dots, t(\alpha/\langle A, \alpha_2\rangle)$.

(3.2) *Free profinite groups.* Let $\mathcal{C}$ be a class of finite groups which is closed under subgroups, direct products and homomorphic images. A profinite group G is a pro-$\mathcal{C}$-group if $\mathrm{Im}(G) \subseteq \mathcal{C}$.

Definition. Let X be a set, and $F(X)$ the free discrete group on X. The free pro-$\mathcal{C}$-group on X, $\hat{F}_{\mathcal{C}}(X)$, is defined as

$$\hat{F}_{\mathcal{C}}(X) = \varprojlim F(X)/N$$

where N ranges over all normal subgroups N of $F(X)$ of finite index which contain all but a finite number of the elements of X and such that $F(X)/N \in \mathcal{C}$.

Free pro-$\mathcal{C}$-groups have the usual universal properties, see e.g., [Ri], Proposition 7.3. In particular, one immediately obtains:

THEOREM. *Let X be an infinite set. Then $S(\hat{F}_{\mathcal{C}}(X))$ is a saturated model of T_{IP} of cardinality $|X|$.*

Proof. Let T be a cofinite subset of X. Then there is a one-to-one correspondence between the open normal subgroups of $\hat{F}_{\mathcal{C}}(X)$ containing T and those of $\hat{F}_{\mathcal{C}}(X \setminus T)$, and therefore $\hat{F}_{\mathcal{C}}(X)$ has at most $\aleph_0$ open normal subgroups containing T. Hence $|S(\hat{F}_{\mathcal{C}}(X))| = |X|$.

When X is countable, $\hat{F}_{\mathcal{C}}(X)$ has IP (e.g., see [Ri], p. 84), and it follows easily that $\hat{F}_{\mathcal{C}}(X)$ has IP when X is arbitrary. It suffices to show that, given epimorphisms $\varphi\colon \hat{F}_{\mathcal{C}}(X) \to A$ and $\theta\colon B \to A$ with $B \in \mathcal{C}$, there are $|X|$ epimorphisms $\psi\colon \hat{F}_{\mathcal{C}}(X) \to B$ such that $\theta \circ \psi = \varphi$. Fix such an epimorphism $\psi_0\colon \hat{F}_{\mathcal{C}}(X) \to B$, and let Y be a finite subset of X such that $X \setminus Y \subseteq \operatorname{Ker}\psi_0$. Let c be a non-identity element of $\operatorname{Ker}\theta$. For each $x \in X \setminus Y$ define a map $f_x\colon X \to B$ as follows:

$$f_x(y) = \begin{cases} \psi_0(y) & \text{if } y \in Y, \\ c & \text{if } y = x, \\ 1 & \text{otherwise,} \end{cases}$$

and extend f_x to a group morphism $\psi_x\colon \hat{F}_{\mathcal{C}}(X) \to B$ using the universal property of $\hat{F}_{\mathcal{C}}(X)$. Then $\varphi = \theta \circ \psi_x$ for every $x \in X \setminus Y$. Since $|X \setminus Y| = |X|$, $S(\hat{F}_{\mathcal{C}}(X))$ is saturated.

COROLLARY. *A profinite group G is isomorphic to $\hat{F}_{\mathcal{C}}(X)$ if and only if, for every epimorphism $\theta\colon B \to A$ with $B \in \mathcal{C}$, for every epimorphism $\varphi\colon G \to A$, there are $|X|$ epimorphisms $\psi\colon G \to B$ such that $\varphi = \theta \circ \psi$.*

(3.3) Theorem 3.2 has been obtained by Mel'nikov in [Me], using different techniques. He shows indeed that a profinite group G is isomorphic to $\hat{F}_{\mathcal{C}}(X)$ if and only if, for any group epimorphisms $\theta\colon B \to A$ and $\varphi\colon G \to A$ where B is a pro-$\mathcal{C}$-group, $|S(B)| < |X|$ and $\operatorname{Ker}\theta$ is finite, there exists $\psi\colon G \to B$ such that $\theta \circ \psi = \varphi$. When dualized, this property is the exact translation of being $|X|$-saturated.

He also shows that various pro-$\mathcal{C}$-completions of $F(X)$ are in fact free pro-$\mathcal{C}$-groups. His main result in that line can be stated as follows:

Let T be a topological space with a distinguished point t, and define

$$F^*(T) = \varprojlim F(T)/N$$

where N ranges over all normal subgroups of $F(T)$ of finite index containing t and such that $gN \cap T$ is a closed subset of T for every $g \in F(T)$. Then $F^*(T)$ is the free group on the set of closed equivalence relations on T with finite quotient space.

(3.4) Recall that ultraproducts of ω-sorted structures are defined in the following manner:

Let I be an index set, S_i a family of $\mathcal{L}$-structures indexed by I and $\mathcal{U}$ an ultrafilter on I. Then $\prod_{i\in I} S_i/\mathcal{U}$ is obtained by taking the usual ultraproduct and deleting the elements of "infinite" sort. As an application of Theorem 3.2 we obtain:

THEOREM. *Let $\mathcal{U}$ be an ultrafilter on I, and for every $i \in I$, let G_i be the free pro-$\mathcal{C}$-group on r_i generators (r_i some cardinal number). Then $G = G(\prod_{i\in I} S(G_i)/\mathcal{U})$ is a free pro-$\mathcal{C}$-group.*

Proof. G is obviously a pro-$\mathcal{C}$-group having IP and with image $\mathcal{C}$. It therefore suffices to show that $S(G)$ is saturated.

If for some positive integer r, the set $\{i \in I \mid r_i = r\}$ is in $\mathcal{U}$, then $S(G) \simeq S(\hat{F}_{\mathcal{C}}(r))$ and G is therefore free. Suppose therefore that there is no such integer r. Let $[\alpha] = ([\alpha_i])_{\mathcal{U}} \in S(G)$, let $A \in \mathcal{C}$ and let θ: $A \to [\alpha]$ be a group epimorphism. Because there are only finitely many groups of size $|[\alpha]|$, we may assume that the $[\alpha_i]$ are chosen so that $[\alpha]$ is naturally isomorphic to $[\alpha_i]$ for every i. Let us call p_i this isomorphism, and let B_i be the set of all $[\beta]$ in $S(G_i)$ such that $\pi_{\beta\alpha_i} = p_i \circ \theta \circ g$ for some isomorphism g: $[\beta] \to A$. It then suffices to show that $|\prod B_i/\mathcal{U}| = |S(G)|$.

First case. $\{i \in I \mid r_i \geq \aleph_0\} \in \mathcal{U}$.

We may then assume that $r_i \geq \aleph_0$ for every $i \in I$. Then $|S(G_i)| = r_i = |B_i|$ for every i, and therefore $|\prod B_i/\mathcal{U}| = |S(G)|$.

Second case. $\{i \in I \mid r_i < \aleph_0\} \in \mathcal{U}$.

Let s be the rank of B. Using the properties of free pro-$\mathcal{C}$-groups, we have

$$|B_i| \geq 2^{r_i - s}$$

for every i such that $r_i \geq s$. As the set of i's such that $r_i \geq s$ belongs to $\mathcal{U}$, we may assume that $r_i \geq s$ for every $i \in I$. M. Hall proved in [Ha] that, if $N(n, r)$ denotes the number of subgroups of index n in the free group on r generators, then $N(1, r) = 1$ and $N(n, r) = n(n!)^{r-1} - \sum_{i=1}^{n-1}((n-i)!)^{r-1}N(i, r)$. This gives

$$|S(G_i)_n| \leq n(n!)^{r_i - 1}$$

for every $i \in I$ and integer n. Let $n = |B|$ and let a be such that $2^a \geq n!$. Then $n(2^{r_i-s}2^{s-1})^a \geq n(n!)^{r-1}$ and therefore

$$2^{r_i - s} \leq |B_i| \leq |S(G_i)|_n \leq n(|B_i|2^{s-1})^a$$

for every i. Hence

$$\prod_{i\in I} 2^{r_i-s}/\mathcal{U} \leq \left|\prod_{i\in I} B_i/\mathcal{U}\right| \leq |S(G)_n| \leq n2^{(s-1)a}\left|\prod_{i\in I} B_i/\mathcal{U}\right|^a.$$

This shows that $\prod_{i\in I} B_i/\mathcal{U}$ is infinite, of cardinality $|S(G)_n|$.

(3.5) *Application to field theory.* For a field K we denote by $G(K)$ the absolute Galois group of K, i.e., the Galois group of K in its separable closure K_s.

THEOREM. *Let $(K_i)_{i\in I}$ be a family of fields, the absolute Galois groups of which are free. Let $\mathcal{U}$ be an ultrafilter on I and $K = \prod_{i\in I} K_i/\mathcal{U}$. Then $G(K)$ is free.*

Proof. Any finite Galois extension L of K is of the form $\prod_{i\in I} L_i/\mathcal{U}$ where L_i is a Galois extension of K_i of degree $[L : K]$ over K_i for a set of i's in $\mathcal{U}$. It follows easily from this observation that

$$S(G(K)) = \prod S(G(K_i))/\mathcal{U}.$$

The result follows then by 3.4.

4. Ranks and forking

In this section, we fix a complete extension T of T_{IP}.

(4.1) PROPOSITION. *Let $A \subseteq B$ be substructures of $S(G) \models T$ and let $\alpha \in S(G)$. Then*

$$\alpha \underset{A}{\perp} B \iff \alpha \vee B \in \operatorname{acl}(A) \iff \alpha \vee B \in \operatorname{acl}(\alpha \vee A).$$

Proof. We may assume that A and B are algebraically closed, because $\alpha \underset{A}{\perp} \operatorname{acl}(A)$. Let $\beta = \alpha \vee A$, $\gamma = \alpha \vee B$. Then $\gamma \leq \beta$. Suppose that $\gamma < \beta$. Then $\gamma \notin \operatorname{acl}(A)$, $\gamma \in \operatorname{acl}(\alpha, A)$ (because $\gamma \geq \alpha$) so that $\alpha \underset{A}{\not\perp} \gamma$, and therefore $\alpha \underset{A}{\not\perp} B$. For the converse of the first implication, note that the type $t(\alpha/\langle\beta\rangle) \cup \{x \vee \delta = \beta \mid \delta \in B,\ \delta \leq \beta\}$ is consistent and complete. Hence it is the unique non-forking extension of $t(\alpha/A)$ to B.

The second equivalence is a direct consequence of the following lemma:

LEMMA. *Let $\gamma < \beta \in S(G)$, let A be a substructure of $S(G)$ and suppose that $\beta = \gamma \vee A$. Then $\gamma \in \operatorname{acl}(A) \iff \gamma \in \operatorname{acl}(\beta)$.*

Proof. One direction is clear. Suppose therefore that $\gamma \in \operatorname{acl}(A)$. Then $t(\gamma/A)$ is isolated by some formula, and we may therefore assume that A is finite. Let us first suppose that $L(\gamma/\beta) = 1$. If $\gamma \notin \operatorname{acl}(\beta)$, then $t(\gamma/\langle\beta\rangle)$ is realized infinitely many times in $S(G)$, and is therefore realized infinitely many times outside of A. But any such realization satisfies $t(\gamma/A)$ which is a contradiction. Therefore $t(\gamma/\langle\beta\rangle)$ is algebraic.

If $L(\gamma/\beta) = n \geq 1$, choose $\gamma = \gamma_0 < \gamma_1 < \ldots < \gamma_n = \beta$; by the previous case, $\gamma_i \in \mathrm{acl}(\gamma_i \vee \langle A, \gamma_{i+1}\rangle)$ for every $i < n$. From $\gamma_i \vee \langle A, \gamma_{i+1}\rangle \sim \gamma_{i+1}$ we obtain the result.

(4.2) THEOREM. *Let $\alpha \in S(G) \models T$, let $A \subseteq S(G)$ and let $n = L(\alpha/\langle A\rangle)$. Choose a sequence $\alpha = \alpha_0 < \alpha_1 < \cdots < \alpha_n = \alpha \vee \langle A\rangle$. Then $U(\alpha/A)$ (the U-rank of $t(\alpha/A)$) equals the number of indices $i < n$ such that $\alpha_i \notin \mathrm{acl}(\alpha_{i+1})$.*

Proof. Because $\alpha_1, \ldots, \alpha_n \in \mathrm{acl}(\alpha)$, we have $U(\alpha/A) = U(\alpha, \alpha_1, \ldots, \alpha_{n-1}/A)$. The fundamental rank equality then gives

$$U(\alpha/A) = U(\alpha/A, \alpha_1, \ldots, \alpha_{n-1}) + U(\alpha_1/A, \alpha_2, \ldots, \alpha_n) + \cdots + U(\alpha_{n-1}/A).$$

The result follows from $\alpha_i \vee \langle A, \alpha_{i+1}\rangle \sim \alpha_{i+1}$ and $U(\alpha_i/A, \alpha_{i+1}) = 1$ if and only if $\alpha_i \notin \mathrm{acl}(A, \alpha_{i+1})$.

Remark. Since T is $\aleph_0$-categorical, the U-rank coincides with the Morley rank. Observe also that $U(\alpha/A) \leq L(\alpha/A)$. They coincide if $\alpha \in \mathrm{acl}(\beta)$ implies $\beta \leq \alpha$ for every $\alpha, \beta \in S(G)$. This is the case for example when T is the theory of the system associated to a free pro-$\mathcal{C}$-group.

(4.3) We conclude this section by a finer study of forking. We start with an easy lemma.

LEMMA. *Let $A \subseteq B$ be substructures of $S(G) \models T$, let $\alpha, \beta \in S(G)$ and suppose that $\alpha \vee B < \alpha \vee A$.*

(1) *There exists $\gamma \in B$ such that $\alpha \leq \gamma < \alpha \vee A$ and $L(\gamma/A) = 1$.*
(2) *Suppose that $B = \langle A, \beta\rangle$. Then there exists δ such that $\beta \leq \delta < \beta \vee A$, $L(\delta/A) = 1$ and $\langle A, \delta\rangle = \langle A, \gamma\rangle$. If $\varepsilon \in B$, then $L(\varepsilon/A) \leq L(\beta/A)$.*
(3) *If V is a normal subgroup of $[\alpha]$ which intersects trivially $\mathrm{Ker}\,\pi_{\alpha\alpha\vee A}$, and $\delta \in S(G)$ is such that $\mathrm{Ker}\,\pi_{\alpha\delta} = V$, then $\alpha \sim (\alpha \vee A) \wedge \delta$.*

Proof. (1) Take any γ such that $\alpha \vee B \leq \gamma < \alpha \vee A$ and $L(\gamma/\alpha \vee A) = 1$. Then $\gamma \vee A = \alpha \vee A$ and therefore $L(\gamma/A) = 1$.

(2) By symmetry (see Lemma 1.9), we have $\beta \vee \langle A, \gamma\rangle < \beta \vee A$. Take δ such that $\beta \vee \langle A, \gamma\rangle \leq \delta < \beta \vee A$ and $L(\delta/\beta \vee A) = 1$; as in (1), $L(\delta/A) = 1$. Using symmetry, we obtain $\langle A, \gamma\rangle = \langle A, \delta\rangle$.

The second assertion follows from Lemma 1.10.

(3) Obvious. Note that this implies that $L(\delta/A) = L(\alpha/A)$.

(4.4) Lemma 4.3 allows us to reduce to the following situation:

LEMMA. *Let A be a substructure of $S(G) \models T$, let $\alpha, \beta, \gamma, \delta \in S(G)$ be such that $\alpha < \alpha \vee A = \gamma$, $\beta \vee A = \delta$ and $\langle A, \alpha\rangle = \langle A, \beta\rangle$. Suppose furthermore that* $\operatorname{Ker}\pi_{\alpha\gamma}$ *is the unique minimal normal subgroup of* $[\alpha]$.

(1) *If $\alpha \sim \beta \wedge \varepsilon$ for some $\varepsilon \in A$, then $\beta \sim \alpha$ and $\varepsilon \geq \gamma$.*
(2) *If $\beta \sim \alpha \wedge \varepsilon$ for some $\varepsilon \in A$, then $\delta \sim \varepsilon \wedge \gamma$ and $\beta \sim \alpha \wedge \delta$.*
(3) *If $\beta \not\sim \alpha \wedge \delta$ then $\beta \wedge \gamma \not\sim \alpha \wedge \delta$ and* $\operatorname{Ker}\pi_{\alpha\gamma}$ *is abelian; there is $\varepsilon \in A$ with $\varepsilon \leq \gamma \wedge \delta$ and $L(\varepsilon/\gamma \wedge \delta) = 1$, and such that $\alpha \wedge \varepsilon = \alpha \wedge \beta = \beta \wedge \varepsilon$;* $\operatorname{Ker}\pi_{\varepsilon\gamma\wedge\delta}$ *and* $\operatorname{Ker}\pi_{\beta\delta}$ *are abelian, and isomorphic to* $\operatorname{Ker}\pi_{\alpha\gamma}$*; as $[\gamma \wedge \delta]$-modules,* $\operatorname{Ker}\pi_{\alpha\wedge\delta\gamma\wedge\delta}$, $\operatorname{Ker}\pi_{\varepsilon\gamma\wedge\delta}$ *and* $\operatorname{Ker}\pi_{\beta\wedge\gamma\gamma\wedge\delta}$ *are isomorphic, and* $\operatorname{Ker}\pi_{\gamma\wedge\delta\gamma\vee\delta}$ *acts on them trivially.*

Proof. (1) If $\alpha \sim \beta \wedge \varepsilon$ then $\operatorname{Ker}\pi_{\alpha\beta} \cap \operatorname{Ker}\pi_{\alpha\varepsilon} = (1)$; since $\varepsilon \in A$, $\operatorname{Ker}\pi_{\alpha\varepsilon}$ is non-trivial and therefore contains $\operatorname{Ker}\pi_{\alpha\gamma}$, which gives $\varepsilon \geq \gamma$. Then $\operatorname{Ker}\pi_{\alpha\beta}$ must be trivial, which gives $\alpha \sim \beta$.

(2) From $L(\alpha \wedge \varepsilon/\gamma \wedge \varepsilon) = 1 = L(\alpha \wedge \varepsilon/A)$, we deduce that $(\alpha \wedge \varepsilon) \vee A = \gamma \wedge \varepsilon$, which implies $\delta \sim \gamma \wedge \varepsilon$.

(3) If $\beta \wedge \gamma \sim \alpha \wedge \delta$, then $\beta \wedge \gamma \leq \alpha$; using the modular equality we obtain $\alpha \sim \alpha \vee (\beta \wedge \gamma) = \gamma \wedge (\alpha \vee \beta)$; hence $\alpha \vee \beta \notin A$ and $\langle A, \alpha\rangle = \langle A, \alpha \vee \beta\rangle$; by (1), $\alpha \vee \beta \sim \alpha$, and therefore $\beta \leq \alpha$ and $\beta \wedge \delta \sim \beta$, contradicting our hypothesis and showing that $\beta \wedge \gamma \not\sim \alpha \wedge \delta$.

By Lemma 4.3, there exists $\varepsilon \in A$ such that $\alpha \wedge \varepsilon \leq \beta \wedge \gamma$ and $\varepsilon \leq \gamma \wedge \delta$; we may choose it so that $L(\varepsilon/\gamma \wedge \delta) = 1$. By the above we have $\alpha \wedge \varepsilon < \beta \wedge \gamma$. Let $\alpha' = \alpha \wedge \delta$, $\beta' = \beta \wedge \gamma$, let $U = \operatorname{Ker}\pi_{\alpha\wedge\varepsilon\beta'}$ and let $p = \pi_{\alpha\wedge\varepsilon\alpha'}$, $q = \pi_{\alpha\wedge\varepsilon\varepsilon}$. Then $p(U)$ is a non-trivial normal subgroup of $[\alpha']$ contained in $\operatorname{Ker}\pi_{\alpha'\gamma\wedge\delta}$ and therefore $p(U) = \operatorname{Ker}\pi_{\alpha'\gamma\wedge\delta}$; similarly, $q(U) = \operatorname{Ker}\pi_{\varepsilon\gamma\wedge\delta}$. We identify $[\alpha \wedge \varepsilon]$ with $[\alpha'] \times_{[\gamma\wedge\delta]} [\varepsilon]$, and from $L(\varepsilon/\gamma \wedge \delta) = L(\alpha'/\gamma \wedge \delta) = 1$ and $\beta' \not\sim \varepsilon$, $\beta' \not\sim \alpha'$, we obtain

$$U \cap (\operatorname{Ker}\pi_{\alpha'\gamma\wedge\delta} \times (1)) = U \cap ((1) \times \operatorname{Ker}\pi_{\varepsilon\gamma\wedge\delta}) = (1).$$

Hence p and q define group isomorphisms from U onto $\operatorname{Ker}\pi_{\alpha'\gamma\wedge\delta}$ and $\operatorname{Ker}\pi_{\varepsilon\gamma\wedge\delta}$; furthermore, $\alpha \wedge \varepsilon = \beta \wedge \varepsilon = \alpha \wedge \beta$.

Let $(a, b) \in U$, $c \in \operatorname{Ker}\pi_{\alpha'\gamma\wedge\delta}$. Then $(a, b)^{(c,1)} = (a^c, b) \in U$, so that $a^c = a$; hence $\operatorname{Ker}\pi_{\alpha'\gamma\wedge\delta}$ is abelian; similarly, $\operatorname{Ker}\pi_{\varepsilon\gamma\wedge\delta}$ is abelian. Let $(c, d) \in [\alpha \wedge \varepsilon]$. Then $(a, b)^{(c,d)} = (a^c, b^d)$, so that p and q are isomorphisms of $[\gamma \wedge \delta]$-modules. Furthermore, $\operatorname{Ker}\pi_{\alpha'\gamma\wedge\delta} \times (1)$ forms a set of representatives for $\operatorname{Ker}\pi_{\beta'\gamma\wedge\delta}$ modulo U, and therefore $\operatorname{Ker}\pi_{\beta'\gamma\wedge\delta}$ and U are isomorphic $[\gamma \wedge \delta]$-modules. From $\alpha' = \alpha \wedge \delta$, we obtain $\operatorname{Ker}\pi_{\alpha'\gamma\wedge\delta} \simeq \operatorname{Ker}\pi_{\alpha\gamma}$ and $\operatorname{Ker}\pi_{\gamma\wedge\delta\delta}$ acts trivially on $\operatorname{Ker}\pi_{\alpha'\gamma\wedge\delta} \simeq U$; similarly, $\operatorname{Ker}\pi_{\beta'\gamma\wedge\delta} \simeq \operatorname{Ker}\pi_{\beta\delta}$ and $\operatorname{Ker}\pi_{\gamma\wedge\delta\gamma}$ acts trivially on U, which finishes the proof.

5. Rudin-Keisler ordering and orthogonality

We fix a complete theory T extending T_{IP}; all models will be models of T.

In this section we will study the Rudin-Keisler ordering $\leq_{RK}$ on types and the notion of orthogonality. Recall that if p and q are types defined over a model $S(G)$, $p \leq_{RK} q$ if every model containing $S(G)$ and realizing q also realizes p. If p and q are stationary types defined over a set A, we will say that $p \leq_{RK} q$ if the non-forking extensions p' and q' of p and q to a model of T satify $p' \leq_{RK} q'$. Recall that, because T is $\aleph_0$-categorical, all types defined over an algebraically closed set of parameters are stationary.

The notion of RK-ordering is closely related to the one of domination, and for strongly regular types corresponds to non-orthogonality. Let us first start with an easy observation:

(5.1) PROPOSITION. *Let $\alpha, \beta \in S(G) \models T$, and let A, B be substructures of $S(G)$. Let $P(\alpha/A)$ denote the set $\{\gamma \mid \alpha \leq \gamma < \alpha \vee \mathrm{acl}(A),\ L(\gamma/\mathrm{acl}(A)) = 1\}$.*

(1) *Then $t(\alpha/A) \perp t(\beta/B) \iff \forall \gamma \in P(\alpha/A), \forall \delta \in P(\beta/B), t(\gamma/A) \perp t(\delta/B)$.*
(2) *$t(\gamma/\mathrm{acl}(A))$ is strongly regular and RK-minimal (i.e., minimal non-algebraic for $\leq_{RK}$) for every $\gamma \in P(\alpha/A)$.*
(3) *Let $\{\gamma_1, \dots, \gamma_n\}$ be a subset of $P(\alpha/A)$ which is maximal independent over A. Then*

$$t(\alpha/\mathrm{acl}(A)) \sim_{RK} t(\gamma_1/\mathrm{acl}(A)) \times \cdots \times t(\gamma_n/\mathrm{acl}(A)).$$

(4) *Suppose that $A = \mathrm{acl}(A) = B$. Then $t(\alpha/A) \leq_{RK} t(\beta/A)$ if and only if there is a map $f\colon P(\alpha/A) \to P(\beta/B)$ which preserves independence over A and is such that $t(\gamma/A) \sim_{RK} t(f(\gamma)/A)$ for every $\gamma \in P(\alpha/A)$.*

Proof. (1) We may assume that A and B are algebraically closed. Observe that, for any algebraically closed C containing $A \cup B$ and such that $\alpha \vee C = \alpha \vee A$ and $\beta \vee C = \beta \vee B$ we have

$$\begin{aligned} \alpha \not\mathop{\smile}\limits_{C} \beta &\iff \alpha \vee \langle C, \beta\rangle < \alpha \vee C \\ &\iff \exists \gamma \in P(\alpha/C) \cap \langle C, \beta\rangle \\ &\iff \exists \gamma \in P(\alpha/C),\ \delta \in P(\beta/C),\ \langle C, \gamma\rangle = \langle C, \delta\rangle \qquad \text{(by Lemma 4.3)}, \end{aligned}$$

which gives the result.

(2) Let $\varphi(x)$ be the formula isolating $t(\gamma/\langle \alpha \vee \mathrm{acl}(A)\rangle)$, and let $S(H)$ be any model containing $S(G)$. If $\gamma' \in S(H) \setminus S(G)$ satisfies φ, then $\gamma' < \gamma' \vee S(G) \leq \alpha \vee \mathrm{acl}(A)$, and therefore $\gamma' \vee S(G) = \alpha \vee \mathrm{acl}(A)$. Since γ' has the same type as γ over $\langle \alpha \vee \mathrm{acl}(A)\rangle$, it follows that γ' is a realization of the non-forking extension

of $t(\gamma/\mathrm{acl}(A))$ to $S(G)$. This shows that $t(\alpha/\mathrm{acl}(A))$ is strongly regular; since it has U-rank 1, it is RK-minimal.

(3) Without loss of generality, we may suppose that A is a model. Clearly $t(\gamma_1/A) \times \cdots \times t(\gamma_n/A) \leq_{RK} t(\alpha/A)$. Let $S(H)$ be a model of T containing $\gamma_1, \ldots, \gamma_n$, and let $\alpha' \in S(H)$ realize $t(\alpha/\langle\gamma_1, \ldots, \gamma_n\rangle)$. Then $\alpha' \vee A = \alpha \vee A$ and therefore α' realizes $t(\alpha/A)$.

(4) We may suppose that A is a model of T. Assume that $t(\alpha/A) \leq_{RK} t(\beta/A)$, let $S(H)$ be the prime model over $A \cup \beta$ and let $\alpha' \in S(H)$ be a realization of $t(\alpha/A)$. Then $t(\alpha'/A \cup \beta)$ is isolated because $S(H)$ is prime over $A \cup \beta$. Let $\varepsilon = \alpha' \vee \langle A, \beta\rangle$ and suppose that $\varepsilon \not\leq \gamma$ for some $\gamma \in P(\alpha'/A)$. Then $\gamma \vee \langle A, \beta\rangle = \gamma \vee A$, and $t(\gamma/\langle\gamma \vee A\rangle)$ has infinitely many realizations in A. This contradicts the fact that $t(\alpha'/\langle A, \beta\rangle)$ is isolated (Proposition 2.5). Hence $\varepsilon \leq \gamma$ for every $\gamma \in P(\alpha/A)$. By Lemma 4.3, for every $\gamma \in P(\alpha'/A)$ there exists $\delta \in P(\beta/A)$ such that $\langle A, \gamma\rangle = \langle A, \delta\rangle$. This gives us the desired map f.

(5.2) The previous result makes it clear that we can restrict our attention to types of length 1 over an algebraically closed set of parameters. Since RK-minimal types are RK-equivalent if and only if their non-forking extensions to a model are non-orthogonal, we will study more in detail the conditions under which two types are orthogonal. Let us first make a simple observation.

Let $A \models T$, α, β such that $L(\alpha/A) = L(\beta/A) = 1$. Then $t(\alpha/A) \not\perp t(\beta/A)$ if and only if $\langle A, \alpha\rangle$ contains a realization of $t(\beta/A)$.

(5.3) Before coming to our main result on orthogonality, we need one more lemma:

LEMMA. *Let $A \subseteq S(G) \models T$ be algebraically closed, let $\alpha, \gamma, \eta \in S(G)$ be such that $\alpha \vee A = \gamma$, $\operatorname{Ker}\pi_{\alpha\gamma}$ is abelian and $\operatorname{Ker}\pi_{\alpha\eta}$ is the centralizer $C_{[\alpha]}\operatorname{Ker}\pi_{\alpha\gamma}$ of $\operatorname{Ker}\pi_{\alpha\gamma}$ in $[\alpha]$. Then there is $\varepsilon < \eta = \varepsilon \vee A$ such that $L(\varepsilon/A) = L(\alpha/A)$, $\operatorname{Ker}\pi_{\varepsilon\eta} = C_{[\varepsilon]}\operatorname{Ker}\pi_{\varepsilon\eta}$, and $t(\varepsilon/A) \not\perp t(\alpha/A)$.*

Proof. Without loss of generality, we may assume that A is a model of T. Let $\beta \in A$ realize $t(\alpha/\langle\gamma\rangle)$ and let $f\colon [\alpha] \to [\beta]$ be a group isomorphism inducing the identity on $[\gamma]$.

We identify $[\alpha \wedge \beta]$ with $[\alpha] \times_{[\gamma]} [\beta]$ and let $p = \pi_{\alpha\gamma}$, $q = \pi_{\beta\gamma}$. Define $U = \{(a, f(a)) \mid a \in \operatorname{Ker}\pi_{\alpha\eta}\}$. We claim that U is normal: if $(c, d) \in [\alpha \wedge \beta]$, then

$$\begin{aligned}(a, f(a))^{(c,d)} &= (a^c, f(a)^d)\\ &= (a^{p(c)}, f(a)^{q(d)}) \qquad \text{(because } \operatorname{Ker}\pi_{\alpha\eta} \subseteq C_{[\alpha]}\operatorname{Ker}\pi_{\alpha\gamma})\\ &= (a^{p(c)}, f(a^{p(c)})) \in U.\end{aligned}$$

Let $\varepsilon < \eta$ be such that $\operatorname{Ker}\pi_{\alpha\wedge\beta\varepsilon} = U$. From $U \cap \operatorname{Ker}\pi_{\alpha\wedge\beta\beta} = (1)$ we obtain $\alpha \wedge \beta = \beta \wedge \varepsilon$. Since $\operatorname{Ker}\pi_{\alpha\gamma} \times (1)$ forms a set of coset representatives for $\operatorname{Ker}\pi_{\varepsilon\eta}$

modulo U, they are isomorphic as $[\eta]$-modules, which gives $\operatorname{Ker}\pi_{\varepsilon\eta} = C_{[\varepsilon]}\operatorname{Ker}\pi_{\varepsilon\eta}$ and $L(\alpha/\gamma) = L(\varepsilon/\eta)$.

Remark. $[\varepsilon]$ is isomorphic to the semi-direct product $\operatorname{Ker}\pi_{\alpha\beta} \rtimes [\eta]$, and the map $\pi_{\varepsilon\eta}$ is the natural projection onto $[\eta]$.

(5.4) *Definition.* Let $\alpha < \beta \in S(G)$ be such that $L(\alpha/\beta) = 1$ and $\alpha \notin \operatorname{acl}(\beta)$.

(1) We say that $t(\alpha/\langle\beta\rangle)$ is *minimal modular* if α is the identity element of $[\alpha]$ and satisfies:
   (a) If $\operatorname{Ker}\pi_{\alpha\beta}$ is non-abelian then $C_{[\alpha]}\operatorname{Ker}\pi_{\alpha\beta} = (1)$.
   (b) If $\operatorname{Ker}\pi_{\alpha\beta}$ is abelian, then the extension $[\alpha] \to [\beta]$ is split and $[\beta]$ acts faithfully on $\operatorname{Ker}\pi_{\alpha\beta}$.

(2) Let η be defined by $\operatorname{Ker}\pi_{\alpha\eta} = \operatorname{Ker}\pi_{\alpha\beta}C_{[\alpha]}\operatorname{Ker}\pi_{\alpha\beta}$. By Lemmas 4.3 and 5.3, there is a unique minimal modular type defined on $\langle\eta\rangle$ and non-orthogonal to $t(\alpha/\langle\beta\rangle)$. We will call this type the *minimal modular type associated to* $t(\alpha/\langle\beta\rangle)$.

This reduces the study of non-orthogonality of types to the ones which are minimal modular. But, in the case of minimal modular types, the result is particularly simple:

THEOREM. *Let $A \subseteq S(G) \models T$ be a substructure, let α, β, γ and δ be such that $L(\alpha/\operatorname{acl}(A)) = L(\beta/\operatorname{acl}(A)) = 1$ and $\alpha \vee \operatorname{acl}(A) = \gamma$, $\beta \vee \operatorname{acl}(A) = \delta$. Suppose that $t(\alpha/\langle\gamma\rangle)$ and $t(\beta/\langle\delta\rangle)$ are minimal modular. Then*

$$t(\alpha/A) \not\perp t(\beta/A) \iff t(\alpha/A) = t(\beta/A).$$

Proof. The sufficiency is clear. For the other direction, we will first suppose that A is algebraically closed. By assumption, there is a model $S(H)$ of T containing A and independent from α, β over A such that $t(\alpha/S(H)) \not\perp^a t(\beta/S(H))$. Lemma 4.4 and 5.2 allow us to conclude that $\gamma = \delta$ and $t(\alpha/\langle\gamma\rangle) = t(\beta/\langle\delta\rangle)$, i.e., that $t(\alpha/A) = t(\beta/A)$.

Suppose now that A is arbitrary. The extensions of $t(\alpha/A)$ to $\operatorname{acl}(A)$ determine the non-forking extensions of $t(\alpha/A)$ to any model containing A. Furthermore, these types are conjugate by A-automorphisms of $\operatorname{acl}(A)$. Hence, $t(\alpha/A) \not\perp t(\beta/A)$ implies that for some A-automorphism f of $\operatorname{acl}(A)$, we have $f(t(\alpha/\operatorname{acl}(A)) \not\perp t(\beta/\operatorname{acl}(A))$. By the above, this implies $f(t(\alpha/\operatorname{acl}(A)) = t(\beta/\operatorname{acl}(A))$, and therefore $t(\alpha/A) = t(\beta/A)$.

(5.5) COROLLARY. *Let A, B be substructures of $S(G) \models T$, let $\alpha, \gamma \in S(G)$ be such that $\gamma = \alpha \vee \operatorname{acl}(A)$ and $L(\alpha/\gamma) = 1$; let η be such that* $\operatorname{Ker}\pi_{\alpha\eta} = \operatorname{Ker}\pi_{\alpha\beta}C_{[\alpha]}\operatorname{Ker}\pi_{\alpha\gamma}$. *Then*

$$t(\alpha/A) \perp B \iff \eta \notin \operatorname{acl}(B).$$

Proof. Let $t(\varepsilon/\langle\eta\rangle)$ be the minimal modular type associated to $t(\alpha/\langle\beta\rangle)$. If $\eta \in \operatorname{acl}(B)$, then the non-forking extension of $t(\varepsilon/\langle\eta\rangle)$ to $\langle B, \gamma\rangle$ is non-orthogonal to itself, and therefore $t(\alpha/A) \not\perp B$ (by transitivity of non-orthogonality of regular types).

The reverse implication follows from Theorem 5.4.

6. Strongly homogeneous models and automorphisms

We call a model κ-strongly homogeneous if every partial isomorphism between two substructures of size $< \kappa$ extends to an automorphism of the model. In [HL], Haran and Lubotsky asked the following question: let G be a profinite group having IP; is it true that every isomorphism between two finite quotients of G lifts to an automorphism of G? When dualized, this question reduces to the question of whether every model of T_{IP} is ω-strongly homogeneous. Note that this is always true for countable models. In this section we will characterize the strongly homogeneous models, from which it will follow that the question of Haran and Lubotsky has a negative answer. We will then study the automorphism group of such models and show some extension properties. All our results follow from the next proposition.

(6.1) PROPOSITION. *Let $A \subseteq B$, $A' \subseteq B'$ be substructures of $S(G)$ and $S(H)$ respectively, with $S(G) \equiv S(H) \models T_{IP}$. Suppose that B is normal over A (i.e., if $\alpha \in B$, then the set $t(\alpha/A)^{S(G)}$ of all realisations of $t(\alpha/A)$ in $S(G)$ is contained in B), B' is normal over A' and that φ: $B \to B'$ is an isomorphism satisfying*:

(*a*) $\varphi(A) = A'$.
(*b*) *For every $\alpha, \beta \in S(G)$ such that $\alpha < \beta \leq \alpha \vee A$ and $L(\alpha/\beta) = 1$, for every $\alpha', \beta' \in S(H)$ realizing $\varphi(t(\alpha, \beta/A))$, the sets $t(\alpha/\langle A, \beta\rangle)^{S(G)}$ and $t(\alpha'/\langle A', \beta'\rangle)^{S(H)}$ have the same dimension over $\langle A, \beta\rangle$ and $\langle A', \beta'\rangle$ respectively.*

Then φ can be extended to an isomorphism from $S(G)$ onto $S(H)$.

Proof. We may assume that B and B' are algebraically closed. By a standard argument, it suffices to extend φ to a set $C \cup B$ where C is the set of realizations of the restriction to A of a type of U-rank 1 over B.

Let $\alpha \in S(G)$ be maximal (for $\leq$) such that $\alpha \notin B$, let $\beta = \alpha \vee B$. Then $t(\alpha/\langle\beta\rangle)$ is not algebraic, and using the maximality of α and Lemma 4.3 one obtains $L(\alpha/\beta) = 1$, $\operatorname{Ker}\pi_{\alpha\beta}$ is the unique minimal normal subgroup of $[\alpha]$; this implies that $\alpha \vee A = \beta \vee A$, since otherwise we would have $\alpha \sim \beta \wedge (\alpha \vee A)$.

Let $C = t(\alpha/A)^{S(G)}$, $C' = \varphi\big(t(\alpha/A)\big)^{S(H)}$, and let $(C_\lambda)_{\lambda<\kappa}$ be a partition of C into non-empty subsets normal over B and realizing a single 1-type over B. For $\lambda < \kappa$, $\alpha_\lambda \in C_\lambda$, define $\beta_\lambda = \alpha_\lambda \vee B$ and $C'_\lambda = \varphi\big(t(\alpha_\lambda/B)\big)^{S(H)}$, $\beta'_\lambda = \varphi(\beta_\lambda)$.

By assumption, for every $\lambda < \mu < \kappa$ we have

$$\dim_{\langle A,\beta_\lambda\rangle} C_\lambda = \dim_{\langle A,\beta_\mu\rangle} C_\mu = \dim_{\langle A',\beta'_\lambda\rangle} C'_\lambda.$$

Assume that we have already extended φ from $B_\lambda = \langle B, \bigcup_{\mu<\lambda} C_\mu\rangle$ onto $B'_\lambda = \langle B', \bigcup_{\mu<\lambda} C'_\mu\rangle$. To extend φ from $B_{\lambda+1}$ onto $B'_{\lambda+1}$, it suffices to show that $\dim_{B_\lambda} C_\lambda = \dim_{B'_\lambda} C'_\lambda$. There are two cases to consider:

Case 1. α can be chosen so that $t(\alpha/\langle\beta\rangle)$ is minimal modular.

Then for every $\mu \neq \lambda$ we have $t(\alpha_\mu/\langle\beta_\mu\rangle) \perp t(\alpha_\lambda/\langle\beta_\lambda\rangle)$. By regularity and RK-minimality of $t(\alpha_\lambda/\langle\beta_\lambda\rangle)$, it follows that for any $\gamma_1, \dots, \gamma_n \in \bigcup_{\mu<\lambda} C_\mu$ which are independent over B, $t(\alpha_\lambda/\langle\beta_\lambda\rangle) \perp t(\gamma_1, \dots, \gamma_n/B)$. This implies that

$$\dim_{B_\lambda} C_\lambda = \dim_{\langle A,\beta_\lambda\rangle} C_\lambda = \dim_{B'_\lambda} C'_\lambda.$$

Case 2. Not case 1.

Then $\operatorname{Ker}\pi_{\alpha\beta}$ is abelian. Let $t(\varepsilon/\langle\eta\rangle)$ and $t(\varepsilon_\lambda/\langle\eta_\lambda\rangle)$ be the minimal modular types associated to $t(\alpha/\langle\beta\rangle)$ and $t(\alpha_\lambda/\langle\beta_\lambda\rangle)$ respectively.

Claim. $\dim_B C_\lambda = 1$.

Suppose that $\dim_{\langle A,\beta\rangle} t(\alpha/\langle A,\beta\rangle)^{S(G)} > 1$, and let $\alpha' \in t(\alpha/\langle A,\beta\rangle)^{S(G)}$ be independent from α over $\langle A,\beta\rangle$. By Lemma 5.3, $\langle\alpha,\alpha'\rangle$ contains a realization ε' of $t(\varepsilon/\langle\eta\rangle)$, and by independence of α and α' over $\langle A,\beta\rangle$, $\varepsilon' \notin \langle A,\beta\rangle$. Hence, because $\operatorname{Ker}\pi_{\varepsilon\eta}$ is the unique minimal normal subgroup of $[\varepsilon]$, $\varepsilon' \vee A = \eta \vee A$. By assumption, the realizations of the non-forking extensions of $t(\varepsilon/\langle\eta\rangle)$ to $\langle A,\eta\rangle$ are in B, and therefore $\varepsilon' \in B$.

Similarly, any element α'_λ of C_λ independent from α_λ over $\langle A,\beta_\lambda\rangle$ yields a realization ε'_λ of a non-forking extension of $t(\varepsilon_\lambda/\langle\eta_\lambda\rangle)$ to B. Since η_λ and η have the same type over A, $t(\varepsilon'_\lambda/A) = t(\varepsilon'/A)$, and therefore $\varepsilon'_\lambda \in B$. This gives $\dim_B C_\lambda = 1$. Since B' contains $\varphi\big(t(\varepsilon'/A)\big)^{S(H)}$, we obtain $\dim_{B'} C'_\lambda = 1$.

Furthermore, since $C_\lambda \subseteq \langle B,\alpha_\lambda\rangle$, we have either $B_\lambda \cap C_\lambda = \emptyset$, or $C_\lambda \subseteq B_\lambda$. If $C_\lambda \subseteq B_\lambda$, then $\varphi(\alpha_\lambda)$ realizes $\varphi\big(t(\alpha_\lambda/\langle\beta_\lambda\rangle)\big)$; since $\operatorname{Ker}\pi_{\alpha\beta}$ is the unique minimal normal subgroup of $[\alpha]$, $\varphi(\alpha_\lambda)$ realizes $\varphi\big(t(\alpha_\lambda/B)\big)$, i.e., $\alpha'_\lambda \in C'_\lambda$. Hence $C'_\lambda \subseteq B'_\lambda$.

By symmetry, $C'_\lambda \subseteq B'_\lambda$ implies $C_\lambda \subseteq B_\lambda$, and therefore $\dim_{B_\lambda} C_\lambda = \dim_{B'_\lambda} C'_\lambda$, which finishes the proof.

(6.2) We will now prove two results which will allow us to verify that structures we are interested in satisfy the hypotheses of the proposition.

LEMMA. *Let A be a small substructure of $S(G)$ and let $\alpha \in S(G)$. Then $\langle A,\alpha\rangle$ is small.*

Proof. Let $\beta = \alpha \vee A$; we may suppose that $\operatorname{Ker}\pi_{\alpha\beta}$ is the unique minimal normal subgroup of $[\alpha]$. Let $\gamma \in \langle A, \alpha\rangle \setminus A$ be of sort n, let $\delta = \gamma \vee A$ and let $\varepsilon \in A$ be maximal such that $\varepsilon \leq \beta \wedge \delta$ and $\alpha \wedge \varepsilon \leq \gamma$. If $\alpha \wedge \varepsilon \sim \gamma$ then ε is of sort n. If $\alpha \wedge \delta \not\sim \gamma$, then, by Lemma 4.4, $\operatorname{Ker}\pi_{\alpha\beta} \simeq \operatorname{Ker}\pi_{\varepsilon\gamma\wedge\beta}$ and therefore ε is of sort $m = n|[\alpha]|$. Thus $|\langle A, \alpha\rangle_n| \leq |A_m|$, which gives the result.

COROLLARY. *Let A be a substructure of $S(G) \models T_{IP}$, and let $\alpha, \beta \in S(G)$ be such that $\alpha < \beta \leq \alpha \vee A$ and $L(\alpha/\beta) = 1 = U(\alpha/\beta)$. Suppose that A is small or that $S(G)$ is $|A|^+$-saturated. Then* $\dim_{\langle A,\beta\rangle} t(\alpha/\langle A, \beta\rangle)^{S(G)} = |t(\alpha/\langle A, \beta\rangle)^{S(G)}|$.

Proof. When $t(\alpha/\langle\beta\rangle)$ has at least $|A|^+$ realizations in $S(G)$, this is clear. When A is small and $t(\alpha/\langle\beta\rangle)$ has only countably many realizations, observe that a small substructure of $S(G)$ contains only finitely many realizations of $t(\alpha/\langle\beta\rangle)$ and build a countably infinite sequence of realizations of $t(\alpha/\langle A, \beta\rangle)$ which are independent over $\langle A, \beta\rangle$.

(6.3) THEOREM. *Let $S(G) \models T_{IP}$, let κ be a cardinal. The following conditions are equivalent.*

(1) *$S(G)$ is κ-strongly homogeneous.*
(2) *$S(G)$ is κ-saturated, and for every α, β with $\alpha \leq \beta$ and $L(\alpha/\beta) = 1$, for every α', β' realizing $t(\alpha, \beta/\emptyset)$, $|t(\alpha/\langle\beta\rangle)^{S(G)}| = |t(\alpha'/\langle\beta'\rangle)^{S(G)}|$.*

Proof. (1) $\Rightarrow$ (2) is obvious, and (2) $\Rightarrow$ (1) follows from Proposition 6.1 and Corollary 6.2.

Remarks. (1) By Corollary 6.2, ω-strong homogeneity implies the following stronger property:
If A and A' are small substructures of $S(G)$ and φ is an isomorphism between A and A', then φ extends to an automorphism of $S(G)$.

(2) κ-strong homogeneity is equivalent to ω-strong homogeneity together with κ-saturation.

(3) The proof of 6.1 allows one to give invariants for ω-strongly homogeneous models of a theory T: consider the set $\mathcal{G}$ of types $p(x, y)$ over the empty set such that, whenever α, β realizes $p(x, y)$ then $t(\alpha/\langle\beta\rangle)$ is minimal modular and β is the identity element of $[\beta]$. Then each ω-strongly homogeneous model of T gives rise to a function from $\mathcal{G}$ to the class of infinite cardinals. Conversely, since distinct 2-types over the empty set give rise to orthogonal types, every such function originates from an ω-strongly homogeneous model of T.

(4) The proof of 6.1 shows that if $S(G)$ is ω-strongly homogeneous and N is a normal subgroup of G, then

$$N \text{ is characteristic} \iff S(G/N) \text{ is normal over } \emptyset.$$

(6.4) THEOREM. *Suppose that* $S(G) \models T_{IP}$ *is* κ*-strongly homogeneous, and let* A *be a substructure of* $S(G)$ *of size* $< \kappa$. *Let* N *be the closed normal subgroup of* G *kernel of the natural projection* $G \to G(A)$, *and let* U *be a characteristic subgroup of* N. *Then every automorphism of* G/U *lifts to an automorphism of* G.

Proof. Let $B = S(G/U)$; by dualizing it suffices to show that every automorphism φ of B extends to an automorphism of $S(G)$. Let φ be an automorphism of B. By Proposition 6.1 and Corollary 6.2, it suffices to show that B is normal over A and $\varphi(A)$.

Take $\alpha, \alpha' \in S(G)$ having the same type over A and assume that $\alpha \in B$. Because α and α' have the same type over A, $\langle A, \alpha\rangle$ and $\langle A, \alpha'\rangle$ are isomorphic, and have size less than κ. Let f: $\langle A, \alpha\rangle \to \langle A, \alpha'\rangle$ be an isomorphism which is the identity on A and sends α to α'. By κ-strong homogeneity, f extends to an automorphism g of $S(G)$. If ψ denotes the dual of g, then $\psi(N) = N$ because g is the identity on A, and therefore $\psi(U) = U$. Furthermore, if N_1 and N_2 are the kernels of the canonical projections π_α and $\pi_{\alpha'}$, then $g(\alpha) = \alpha'$ implies $\psi(N_1) = N_2$. Since $N_1 \supseteq U$, we have $N_2 \supseteq U$ and therefore $\alpha' \in B$.

Take α, α' realizing the same type over $\varphi(A)$ and suppose that $\alpha \in B$. Consider the type $\varphi^{-1}(t(\alpha'/\langle A, \varphi(A)\rangle))$. It is clearly consistent, and since $|\langle A, \varphi(A)\rangle| < \kappa$, it is realized by some element $\beta \in S(G)$. Then β realizes $t(\varphi^{-1}(\alpha)/A)$, and therefore $\beta \in B$ since $\varphi^{-1}(\alpha) \in B$ (using the normality of B over A). Also, $\varphi(\beta)$ realizes $t(\alpha'/A)$, which implies that $\alpha' \in B$.

Remarks. (1) This result was obtained by Mel'nikov [Me2] for U a characteristic subgroup of a free pro-$\mathcal{C}$-group.

(2) When $\kappa = \aleph_0$, the proof as given does not carry through to the case where A is small. Indeed, one can construct examples of two small isomorphic substructures generating a non-small substructure.

(6.5) As another application of Proposition 6.1, we show that substructures of ω-strongly homogeneous models have closed automorphism groups. The motivation behind this result was a question posed in Kueker-Steitz [KS]. Subsequently, Bouscaren and Laskowski [BL] showed that the result holds for superstable theories which are locally modular of finite rank. According to Laskowski, the proof given here generalizes in a straightforward manner to ω-stable $\aleph_0$-categorical theories, using the machinery developed these past years.

THEOREM. *Suppose that* $S(G) \models T_{IP}$ *is* ω*-strongly homogeneous. Let* $A \subseteq S(G)$, $\varphi \in \mathrm{Aut}(A)$ *and suppose that every restriction of* φ *to a finite subset of* A *extends to an automorphism of* $S(G)$ *sending* A *onto* A. *Then* φ *extends to an automorphism of* $S(G)$.

Proof. A routine argument (due to D. Macpherson) shows that A may be assumed algebraically closed: consider the family $\mathcal{F}$ of all partial isomorphisms ψ extending φ such that:

(a) $\operatorname{dom}\psi \subseteq \operatorname{acl}(A)$.
(b) Every restriction of ψ to a finite subset of $\operatorname{dom}\psi$ extends to an automorphism of $S(G)$ sending A onto A.

Under the natural ordering, this family is non-empty and inductive, and hence has a maximal element ψ. Suppose that $\operatorname{dom}\psi \neq \operatorname{acl}(A)$, and let $\alpha \in \operatorname{acl}(A) \setminus \operatorname{dom}\psi$. Let $A_0 \subseteq A$ be finite such that $\alpha \in \operatorname{acl}(A_0)$, and let $\beta_1, \dots, \beta_n$ be the realizations of $\varphi(t(\alpha/A_0))$. For every finite subset B of $\operatorname{dom}\psi$ containing A_0, $\psi|_B$ extends to an automorphism θ of $S(G)$ sending A onto A, and $\theta(\alpha) \in \{\beta_1, \dots, \beta_n\}$. It follows that for some i, $\psi \cup \{(\alpha, \beta_i)\}$ must have property (b). This contradicts the maximality of ψ, and therefore $\operatorname{dom}\psi = \operatorname{acl}(A)$; since every automorphism of $S(G)$ sending A onto A sends $\operatorname{acl}(A)$ onto $\operatorname{acl}(A)$, ψ satisfies the hypothesis of the theorem.

We will therefore assume that $A = \operatorname{acl}(A)$. Let $\alpha < \beta \leq \alpha \vee A$ be such that $L(\alpha/\beta) = U(\alpha/\beta) = 1$, and let α', β' realize $\varphi(t(\alpha, \beta/A))$. By Proposition 6.1, it suffices to show that

$$(*) \qquad \dim_{\langle A,\beta\rangle} t(\alpha/\langle A, \beta\rangle)^{S(G)} = \dim_{\langle A,\beta'\rangle} t(\alpha'/\langle A, \beta'\rangle)^{S(G)}.$$

First, suppose that $t(\alpha/\langle\beta\rangle)$ is minimal modular. If $\beta \in A$, then $L(\alpha/A) = 1$ and $\varphi(\beta) = \beta'$. By assumption, there is an automorphism ψ of $S(G)$ which sends A to A and agrees with φ on $\langle\beta\rangle$. Then $\psi\big(t(\alpha/\langle\beta\rangle)^{S(G)}\big) = t(\alpha'/\langle\beta'\rangle)^{S(G)}$ and ψ respects independence over A. Thus α, β, α' and β' satisfy $(*)$.

If $\beta \notin A$, then realizations of $t(\alpha/\langle\beta\rangle)$ which are independent over $\langle\beta\rangle$ remain independent over $\langle A, \beta\rangle$ (by 5.5), and therefore

$$\dim_{\langle A,\beta\rangle} t(\alpha/\langle\beta\rangle)^{S(G)} = \dim_{\langle\beta\rangle} t(\alpha/\langle\beta\rangle)^{S(G)}.$$

Similarly, $\beta' \notin A$ implies that $\dim_{\langle A,\beta'\rangle} t(\alpha'/\langle\beta'\rangle)^{S(G)} = \dim_{\langle\beta'\rangle} t(\alpha'/\langle\beta'\rangle)^{S(G)}$. By ω-strong homogeneity, $\dim_{\langle\beta\rangle} t(\alpha/\langle\beta\rangle) = \dim_{\langle\beta'\rangle} t(\alpha'/\langle\beta'\rangle)$, which gives $(*)$.

If $t(\alpha/\langle\beta\rangle)$ is not minimal modular, we let $t(\varepsilon/\langle\eta\rangle)$ be the minimal modular type associated to it. If $\operatorname{Ker}\pi_{\alpha\beta}$ is non-abelian, or if $t(\alpha/\langle\beta\rangle)$ is realized in $\langle A, \beta\rangle$, then $\dim_{\langle A,\beta\rangle} t(\alpha/\langle A, \beta\rangle)^{S(G)} = \dim_{\langle A,\beta\rangle} t(\varepsilon/\langle A, \eta\rangle)^{S(G)}$; if $\operatorname{Ker}\pi_{\alpha\beta}$ is abelian and $t(\alpha/\langle\beta\rangle)$ is not realized in $\langle A, \beta\rangle$, then $\dim_{\langle A,\beta\rangle} t(\alpha/\langle A, \beta\rangle)^{S(G)} = 1 + \dim_{\langle A,\beta\rangle} t(\varepsilon/\langle A, \eta\rangle)^{S(G)}$. Note that $t(\alpha/\langle\beta\rangle)$ is realized in $\langle A, \beta\rangle$ if and only if $t(\alpha'/\langle\beta'\rangle)$ is realized in $\langle A, \beta'\rangle$, because $\varphi(A) = A$ and (α', β') realises $\varphi(t(\alpha, \beta/A))$. Thus, since

$$\dim_{\langle A,\beta\rangle} t(\varepsilon/\langle A, \eta\rangle)^{S(G)} = \dim_{\langle A,\eta\rangle} t(\varepsilon/\langle A, \eta\rangle)^{S(G)} - \dim_{\langle A,\eta\rangle} t(\varepsilon/\langle A, \eta\rangle)^{\langle A,\beta\rangle},$$

and $\dim_{\langle A,\eta\rangle} t(\varepsilon/\langle A, \eta\rangle)^{\langle A,\beta\rangle}$ only depends on $t(\beta/A)$, the minimal modular case gives us the result.

(6.6) DUALIZATION OF THEOREM 6.5. *Let G be a profinite group having the property that any isomorphism between two of its finite quotients lifts to an automorphism of G. Let N be a closed normal subgroup of G and φ an automorphism of G/N having the following property:*

If U is an open normal subgroup of G containing N, and $\bar{\varphi}$: $G/U \to (G/N)/\varphi(U/N)$ is the isomorphism induced by φ, then $\bar{\varphi}$ lifts to an automorphism of G which sends N onto N.

Then φ can be lifted to an automorphism of G.

(6.7) We end this section with an example of a model of $\mathrm{Th}(S(\hat{F}_\omega))$ which is not ω-strongly homogeneous. This is part of a more general phenomenon: every multi-dimensional theory has such models; see [C] for more examples.

Choose any $\alpha \in S(\hat{F}_\omega)$ such for some $\beta > \alpha$, $\mathrm{Ker}\,\pi_{\alpha\beta}$ is the unique minimal normal subgroup of $[\alpha]$ and is non-abelian. Choose $\beta' \not\sim \beta$ and $\alpha' \in S(\hat{F}_\omega)$ realizing $t(\beta, \alpha/\emptyset)$. By Theorem 5.4, $t(\alpha/\langle\beta\rangle) \perp t(\alpha'/\langle\beta'\rangle)$, and therefore there is a model $S(G)$ of the elementary theory of $S(\hat{F}_\omega)$ which realizes $\aleph_1$ times $t(\alpha/\langle\beta\rangle)$ but only countably many times $t(\alpha'/\langle\beta'\rangle)$. Then $[\beta]$ and $[\beta']$ are isomorphic, but no automorphism of $S(G)$ sends $[\beta]$ to $[\beta']$.

7. Pro-p-groups and characteristic subgroups

Serre proved that projective pro-p-groups are free, and thus a projective pro-p-group is completely determined by its number of generators. In this section we prove an analogous result for pro-p-groups having IP.

(7.1) THEOREM. *Let G be a pro-p-group having IP. Then* $\mathrm{Th}(S(G))$ *is totally categorical.*

Proof. If G is finitely generated, then $S(G)$ is small and the result holds. Suppose therefore that G is not finitely generated, and let $\alpha < \beta$ and $\gamma \in S(G)$ be such that $L(\alpha/\beta) = 1$ and $[\gamma] \simeq \mathbb{Z}/p\mathbb{Z}$. Since $\mathrm{Ker}\,\pi_{\alpha\beta}$ is a minimal normal subgroup of the finite p-group $[\alpha]$, $\mathrm{Ker}\,\pi_{\alpha\beta}$ is central and isomorphic to $\mathbb{Z}/p\mathbb{Z}$. By 5.3, $|t(\alpha/\langle\beta\rangle)^{S(G)}| = |t(\gamma/\emptyset)^{S(G)}|$, which implies that $S(G)$ is saturated.

(7.2) THEOREM. *Let G and H be two pro-p-groups having IP, $H \neq (1)$, and let φ: $G \to H$ be an epimorphism. Then* $\mathrm{Ker}\,\varphi$ *is a characteristic subgroup of G if and only if $\varphi^{-1}(\Phi(H)) = \Phi(G)$ ($\Phi(G)$ denotes the Frattini subgroup $G^p[G, G]$ of G).*

Proof. By duality, we obtain an embedding $S\varphi$: $S(H) \to S(G)$, and we will identify $S(H)$ with its image by $S\varphi$ in $S(G)$, thus viewing φ as the canonical projection. Then

$$\varphi^{-1}(\Phi(H)) = \Phi(G) \iff \forall\alpha \in S(G),\ \big([\alpha] \simeq \mathbb{Z}/p\mathbb{Z} \Rightarrow \alpha \in S(H)\big).$$

Suppose first that $\mathrm{Ker}\,\varphi$ is a characteristic subgroup. Since H is non-trivial, there is $\alpha \in S(H)$ such that $[\alpha] \simeq \mathbb{Z}/p\mathbb{Z}$. By Remark 6.3 (4), $S(G)$ contains all realisations of $t(\alpha/\emptyset)$, which gives the result.

Suppose now that $\varphi^{-1}(\Phi(H)) = \Phi(G)$. We will show that $S(H)$ is normal over $\emptyset$. Let $\alpha \in S(H)$, $\alpha' \in S(G)$ such that $[\alpha] \simeq [\alpha']$, and suppose that we have proved the result for the types of elements which are $> \alpha$. Let $\beta > \alpha$ be such that $L(\alpha/\beta) = 1$, and let β' be such that $t(\alpha, \beta/\emptyset) = t(\alpha', \beta'/\emptyset)$. By induction hypothesis, $\beta' \in S(H)$; since $S(H) \models T_{IP}$, there is a realization $\alpha'' \in S(H)$ of $t(\alpha'/\langle\beta'\rangle)$. By the proof of Lemma 5.3, there is ε such that $\alpha'' \wedge \varepsilon = \alpha' \wedge \alpha''$ and $[\varepsilon] \simeq \mathbb{Z}/p\mathbb{Z}$. By hypothesis $\varepsilon \in S(H)$, which implies that $\alpha' \in S(H)$.

COROLLARY. *Let G be a pro-p-group having IP. Then H is isomorphic to the quotient of a free group by a characteristic subgroup.*

Proof. Since $G/\Phi(G)$ is isomorphic to a product of copies of $\mathbb{Z}/p\mathbb{Z}$, there exists a free pro-p-group F together with an epimorphism φ: $F \to G/\Phi(G)$ with kernel $\Phi(F)$. From the universal properties of F, φ can be lifted to an epimorphism ψ: $F \to G$. By the above, $\mathrm{Ker}\,\psi$ is characteristic.

This result provides a partial converse to a result of Haran and Lubotzky: they proved in [HL] that the quotient of a profinite group having IP by a characteristic subgroup has IP.

The fact that G is a pro-p-group plays an important role in the proof of Corollary 7.2. For a generalization to a non pro-p-group G, one needs to assume that $S(G)$ is saturated and that $\alpha \in \mathrm{acl}(\beta)$ implies $\beta \leq \alpha$ for every $\alpha, \beta \in S(G)$.

REFERENCES

[BL] E. Bouscaren and M.C. Laskowski, *S-homogeneity and automorphism groups*, J. Symbolic Logic **58** (1993), 1302–1322.

[C] Z. Chatzidakis, "Model theory of profinite groups having IP, III" in *Mathematical logic and theoretical computer science*, Kueker et al. ed., M. Dekker, New York, 1987.

[CDM] G. Cherlin, L. van den Dries and A. Macintyre, *The elementary theory of regularly closed fields*, preprint, 1980.

[E] Y. Eršov, *On the elementary theory of regularly closed fields*, Soviet Math. Dokl. **23** (1981), No 2, 259–262.

[Ha] M. Hall Jr., *Subgroups of finite index in free groups*, Canad. J. Math. **1** (1949), 187–190.

[HL] D. Haran and A. Lubotzky, *Embedding covers and the theory of Frobenius fields*, Israel J. Math. **41** (1982), 181–202.

[KS] D. Kueker and P. Steitz, *Saturated models of stable theories*, preprint, 1989.

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

[KK] G. Kreisel and J.-L. Krivine, *Eléments de logique mathématique*, Dunod, Paris, 1967.

[Me1] O.V. Mel'nikov, *Projective limits of free profinite groups* (in Russian, English summary), Dokl. Akad. Nauk. BSSR **24** (1980), No 11, 968–970, 1051.

[Me2] ———, *Characteristic subgroups and automorphisms of free profinite groups*, Mat. Zametki **31** (1982), No 3, 339–343, 473; English translation in Math. Notes **31** (82), No 3–4, 174–179.

[Ri] L. Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's Papers in Pure and Appl. Math., No 24, 1970.

UFR de Mathématiques, Case 7012, Université Paris 7, 75251 Paris Cedex 05, France
zoe@logique.jussieu.fr