The Elementary Theory of Regularly Closed Fields

by

Greg Cherlin* (Rutgers University)
Lou van den Dries* (Yale University)
Angus Macintyre* (Yale University)

Contents

---

* Partially supported by NSF research grants.

Introduction

In his 1968 paper [Ax] on the elementary theory of finite fields Ax isolated the following condition on a field K:

(*) Every absolutely irreducible affine variety defined over K has K-rational points.

Let us call K regularly closed (or RC-field) if K satisfies (*). (In §0 we will give reasons for this terminology.)

In a remarkable tour de force Ax proved three basic results:

(I) A field K is pseudo-finite, i.e., an infinite model of the theory of finite fields, if and only if K is a perfect RC-field with $G(K) \simeq \hat{\mathbb{Z}}$. (See §0 for the notations used.) (The proof combines ultra products, Weil's theorem on the Riemann hypothesis for curves over finite fields, and finally Cebotarev's density theorem to handle $\mathrm{char}(K) = 0$.)

(II) The elementary theory Th(K) of a perfect RC-field K with $G(K) \cong \hat{\mathbb{Z}}$ is completely determined by the isomorphism type of Abs(K), the algebraic closure in K of the prime field. (This in turn is determined by the set of $f(T) \in \mathbb{Z}[T]$ having a zero in K, so it is an elementary invariant.)

(III) A field L is isomorphic to Abs(K) for some perfect RC-field K with $G(K) \cong \hat{\mathbb{Z}}$ iff L is algebraic over its prime field and G(L) is pro-cyclic (i.e., topologically generated by one element).

(II) and (III) lead to a decision procedure for the theory of perfect RC-fields K with $G(K) \cong \hat{\mathbb{Z}}$ (they form an elementary class), and combining this with (I) Ax could give a decision procedure for the theory of finite fields, answering a problem posed by Tarski. (Actually, Ax's results are much more precise, see [Ax].)

We emphasize here that (I) represents the most interesting, number theoretic part of Ax's results, and that later work by Jarden demonstrates that (II) and (III) are largely independent of (I). (To be more precise, Ax's treatment of (III) in the characteristic 0 case still depended on Cebotarev's theorem, i.e. (III) was linked to (I), but Jarden showed that Hilbert's irreducibility theorem already suffices for (III)).

Later developments (by Jarden, Kiehne, Fried, Wheeler, Ersov and others) have concentrated on generalizing (parts of) (II) and (III) and the resulting decision procedures to other classes of RC-fields. Mostly the RC-fields were still supposed to be perfect, and restrictions were put on their absolute Galois groups. In this paper we study the model theoretic properties of RC-fields without such restrictions. In particular we obtain, what seem to us, satisfactory generalizations of (II) and (III) to arbitrary RC-fields. Before explaining these and other results, let us sketch the post-Ax developments, initiated by Jarden, which inspired our work.

Let K be a countable hilbertian field (e.g. $K = \mathbb{Q}$), and let $e \in \mathbb{N}$. Then for almost all $(\sigma_1,\ldots,\sigma_e) \in G(K)^e$ - almost all in the sense of the Haar measure on the compact group $G(K)$ - its fixed field. Fix $(\sigma_1,\ldots,\sigma_e)$,

is RC and has absolute Galois group free (as a profinite group) on $\sigma_1,\dots\sigma_e$, cf. [J1], [J2]. (For e = 1 this profinite group is $\cong \hat{\mathbb{Z}}$, and according to (I) it means that for almost all $\sigma \in G(\mathbb{Q})$ its fixed field is pseudo-finite, a surprising result at the time).

Fields K such that $G(K) \cong \hat{F}_e$, the free profinite group on e generators, are called e-free. In [J-K] Jarden and Kiehne generalize, for fixed e, properties (II) and (III) to perfect e-free RC-fields (for (II) we still have Abs(K) as the only elementary invariant, in (III) one replaces rank $(G(L)) \leq 1$ by rank $(G(L)) \leq e$), and derive the decidability of their theory. These generalizations required new techniques, since Ax's arguments depend on the commutativity of the absolute Galois group involved. Besides the use of Jarden's probabilistic result mentioned above, there are three key ideas in their proof. The first, relatively easy one, is the observation:

(a) A profinite group is $\cong \hat{F}_e$ iff its finite homomorphic images are exactly the finite groups of rank $\leq e$. Using this and Galois theory one can write down sentences about a field K expressing that $G(K) \cong \hat{F}_e$.

Their second, most crucial tool, is:

(b) The "Embedding Lemma" which (for perfect RC-fields) replaces the conventional back and forth method for constructing isomorphisms between fields by a dual method for constructing isomorphisms between profinite groups.

Finally, they depend on:

(c) A lifting property of finite groups discovered by Gaschütz allows to carry out this dualized back and forth method in the case $G(K) \cong (\hat{F}_e)$.

In our generalizations of (II) and (III) to arbitrary RC-fields we use Jarden's probabilistic result, in (3.5), (4.3) and (6.2), and also develop as tools natural versions of (a), (b), and (c) for arbitrary RC-fields.

Concerning (a): we construct a language to express certain properties of profinite groups by so called cosentences, e.g. $G \cong \hat{F}_e$ can be expressed by a countable list of cosentences about G. The underlying (co)model theory of this language is not a conventional first-order one. Let us stress here that it is entirely natural and has been used implicitly by earlier workers in the model theory of fields. In many ways it has properties dual to model theory for fields, e.g. the role of embeddings between fields corresponds to those of epimorphisms between profinite groups. (The crucial example which led us to the idea of a comodel theory is Iwasawa's theorem characterizing $\hat{F}_\omega$ as the unique profinite group with a countable basis, a certain lifting property ("ω-cohomogeneity") and all finite groups as homomorphic images; we realized that its proof was the exact dual of Cantor's proof that a countable ω-homogeneous locally finite algebra is uniquely determined by the finite algebras embeddable in it.)

The "comodel theory" of $G(K)$ is interpretable in the 1st order theory of K (K any field) and our comodel theory is maximal with this property cf. (2.9). Sections 1 and 2 are devoted to this comodel theory—see [Ch-vdD-M] for

abrief sketch—, and can be read independently of the rest of the paper. We expect further applications to the model theory of fields.

Section 3 generalizes the Embedding Lemma to not necessarily perfect RC-fields (e.g. separably closed fields are RC, by [L, p. 76], but not perfect, unless algebraically closed). Tamagawa gave us essential help in this part.

To generalize (II) to RC-fields we combine the generalized Embedding Lemma with the main result of comodel theory, and obtain a complete list of elementary invariants for arbitrary RC-fields, cf. (3.4). To get all possibilities for these invariants for RC-fields we need the notion of projective profinite group. The first clue to this is in Ax's paper [Ax]. He proved that if K is a perfect RC-field, then $G(K)$ is of cohomological dimension ≤ 1. The profinite groups with this property are exactly the projective profinite groups as follows from [G]. Conversely, all projective groups occur as $G(K)$, K a (perfect) RC-field, see [Lu-vdD].

Here we improve this last remark and obtain the natural generalization of (III) to arbitrary RC-fields.

The most important elementary invariant of an RC-field is the cotheory of its absolute Galois group. If the absolute Galois group has the so called Iwasawa property cf. (2.10), we call the field an Iwasawa field. Iwasawa fields form an elementary class and include the e-free fields (by Gaschütz), the ω-free fields studied in [J3] (by Iwasawa's theorem referred to above), and many more, by results of Mel'nikov on the structure of normal subgroups of free profinite groups [M]. In §4 we generalize most results of Jarden-

Kiehne to Iwasawa RC-fields, and reduce the decision problem for this class to a decision problem on finite groups. (Lubotsky and Haran, and Eršov in the mean time gave a solution to this problem.) An accidental by product of all this is an example of a decidable field which is a finite extension of an undecidable field, see 4.4.

The properties of the projective cover of a finite group are the key to the other decidability and undecidability results (there are also connections with work of Wheeler though he never mentions projective covers). In §5 we study the projective cover and use it in §6 to prove decidability of the theory of RC-fields with absolute Galois group of rank $\leq e$, for any given $e \in \mathbb{N}$. (Again we reduce it first to a decision problem on finite groups.) In §7 we use projective covers to interpret the (undecidable) theory of graphs in the cotheory of projective profinite groups. The undecidability of the theory of RC-fields is an immediate consequence.

We also attend to questions of model completeness and quantifier elimination (in appropriate languages), see (4.2).

In the last section, §8, we make some remarks on comodel theory, a subject which seems deserving further development.

We feel that with this paper the main questions about the model theory of RC-fields have been answered. Duret [Du] showed that stable RC-fields are separably closed. In another paper [vdD-M] Van den Dries and Macintyre will

discuss the (dismal) situation concerning prime model extensions (even for pseudo-finite fields). As an indication of the abundance of RC-fields, let us mention here that algebraic extensions of RC-fields are RC, see [J1], [T], that there exist two decidable ω-free RC-fields algebraic over $\mathbb{Q}$ with intersection $\mathbb{Q}$, and that there is even a descending sequence of such fields with intersection $\mathbb{Q}$, see [vdD-S].

We gratefully acknowledge our debt to the work of the authors quoted above. During our research we got valuable stimulus from Denef, Lubotsky, McKenna, Poizat and Sabbagh, whom we heartily thank. During the last few months of writing, we got essential help from Zoe Chatzidakis, who helped us reconstruct forgotten proofs, and advanced the general theory considerably. Our greatest debt is to Tauneo Tamagawa, who worked out the relevant inseparable descent for us, thereby opening the imperfect case to our methods.

A final remark on the organization of the paper: for the reader's convenience we included a section 0 stating the definitions of the main notions and establishing standard notations used later on in the paper without further comment.

§0. Conventions and Notations

(0.0) $\omega = \mathbb{N} = \{0,1,2,3,\ldots\}$; e,k,l,m,n stand for members of ω.

(0.1) Profinite Groups. General reference: [R].

A profinite group is a topological group which is Hausdorff, totally disconnected and compact; equivalently: a topological group which is the projective limit of discrete finite groups.

Unless we indicate otherwise the letters Γ, G, H, J will always stand for profinite groups. We write $G \to H$ to indicate a continuous group homomorphism of G into H. The category of profinite groups has these maps as morphisms from G to H. It is important that epis in this category are the surjective group homomorphisms, by [Do]. In §2 we will also deal with the category PROFIN which has the same objects but only the as morphisms.

$\mathrm{Im}(G)$ is the class of finite groups F for which there is an epi $G \to F$. The profinite completion $\hat{F}$ of a group F is defined as the profinite group $\varprojlim F_{/N}$, N ranging over the normal subgroups of finite index of F; in particular $\hat{F}_e$ is the profinite completion of the free group F_e on e generators, $\hat{F}_1 = \hat{\mathbb{Z}}$. Equivalently, $\hat{F}_e$ is the free profinite group on e generators, cf. [R]. However, abusing this notation in accordance with established habits we write $\hat{F}_\omega$ to denote the restricted free profinite group on $\aleph_0$ generators, cf. [Lu-vdD, (1.6)], (which is not the profinite completion of F_ω, the free group on ω). The rank of G, rk(G), is the minimum cardinality of subsets of G generating a dense subgroup. (For finite groups this is the minimum cardinality of a generating set.)

(0.2) Fields and Galois Groups. General references: [L] and [R].

K, L will always denote fields. An absolute number of K is an element of K algebraic over the prime field; Abs(K) is the subfield of K consisting of the absolute numbers of K. $K_s, \tilde{K}$ are the separable, respectively the algebraic closure of K. An embedding $K \to L$ is called regular if L is a regular extension of its image, cf. [L].

An absolutely irreducible (affine) variety defined over K is the set of zeros in $\tilde{K}^n$ of an absolutely prime ideal of $K[X_1,\ldots,X_n]$, i.e. a prime ideal generating a prime ideal in $\tilde{K}[X_1,\ldots,X_n]$.

Following [E] we call K regularly closed (or RC) if each absolutely irreducible variety defined over K has a point with coordinates in K; see (3.2) for equivalent definitions. These fields have also been called pseudo-algebraically closed (PAC) by various authors, but in view of [Wh] this may cause confusion.

It is well known (but not trivial) that the class of RC-fields is elementary, in fact, a field K is RC iff each absolutely irreducible $f(X,Y) \in K[X,Y]$ has infinitely many zeros in K^2.

For a normal extension L of K we denote by G(L/K) the (Galois) group of automorphisms of L fixing K (pointwise), equipped with the Krull topology. (A typical neighborhood of the identity is the set of automorphisms fixing pointwise a given finite subset of L.) It is a profinite group; if $L = \tilde{K}$ we call it the absolute Galois group of K and write G(K). Similarly we write $G_s(K)$ for $G(K_s/K)$, and the restriction may $G(K) \to G_s(K)$ is an isomorphism of profinite groups, so in general there is no harm in identifying the two groups (but see §1).

If L/K is algebraic, then the degree $[L:K]$ is taken as a supernatural number $[R]$, which equals $\dim_k L$ iff this dimension is finite.

§1. Galois theory and interpretability.

(1.1) For any field K, let K_s be the separable algebraic closure of K and let $G_s(K)$ be the profinite group of all automorphisms of K_s over K. A good reference for profinite groups and Galois theory is [R].

Under the Galois duality, given by $L \mapsto G_s(L)$, the following objects are in 1-1 correspondence:

(a) fields L with $K \subset L \subset K_s$, and closed subgroups of $G_s(K)$;

(b) L as above, but also normal over K, and closed normal subgroups of $G_s(K)$;

(c) L as in (a), with $[L:K] = m < \omega$, and open subgroups of $G_s(K)$ of index m;

(d) L as in (b), with $[L:K] = m < \omega$, and open normal subgroups of $G_s(K)$ of index m.

(1.2) Coding finite extensions of K in K.

As is well-known, m-dimensional algebras A over K, i.e., m-dimensional K-linear spaces A equipped with a K-bilinear map $A \times A \to A$, can be parametrized by K^{m^3}, as follows. Select a basis $b_1,\ldots,b_m$ of A, and define c_{ijk} (structure constants) in K by

$$b_i b_j = \sum_{k=1}^{m} c_{ijk}\, b_k.$$

Now, for each m, we fix the basis $b_1,\ldots,b_m$ of K^m by

$b_i = (0,\ldots,1,0,\ldots,0)$

i^{th} place.

Then a point $(c_{ijk})_{i,j,k<m} = \vec{c}$ in K^{m^3} uniquely determines an algebra $A\vec{c}$, m-dimensional over K.

Lemma 1: The $\vec{c}$ such that $A\vec{c}$ is associative form the set of zeros in K^{m^3} of a system of polynomial equations over $\mathbb{Z}$.

Proof: Trivial. ∎

Lemma 2: The $\vec{c}$ such that $A\vec{c}$ is a field form a first-order definable set in K^{m^3}.

Proof: Elementary. ∎

Whenever $A\vec{c}$ is a field with unit $1_{A\vec{c}}$, we construe K as embedded in $A\vec{c}$ via $k \mapsto k.1_{A\vec{c}}$.

Lemma 3: The $\vec{c}$ such that $A\vec{c}$ is a field separable over K form a first-order definable subset of K^{m^3}.

Proof: Elementary. ∎

Lemma 4: The $\vec{c}$ such that $A\vec{c}$ is a field normal over K form a first-order definable subset of K^{m^3}.

Proof: Elementary, e.g. via the splitting field criterion, noting that one need consider only polynomials of degree $\leq m$. ∎

Lemma 5: The $\vec{c}$ such that $A\vec{c}$ is a field Galois over K form a first-order definable subset of K^{m^3}.

Proof: By lemmas 3 and 4.

■

Now we come to the key point, comparing $A\vec{c}$ and $A\vec{d}$ when $\vec{c} \in K^{m^3}$ and $\vec{d} \in K^{n^3}$. We are interested in embeddings of $A\vec{c}$ in $A\vec{d}$ (and in particular in automorphisms of $A\vec{c}$ over K). Such an embedding can exist only if $m \leq n$, and will then be given by a K-linear transformation $T : K^m \to K^n$, satisfying certain compatibility conditions vis-a-vis $\vec{c}$ and $\vec{d}$. Precisely, T is given by an $n \times m$ matrix $\vec{t} = (t_{\ell k})$ with entries in K, and

$$T(b_i\, b_j) = T(b_i)\, T(b_j),\ 1 \leq i, j \leq m.$$

That T should be 1-1 can now be expressed by requiring rank $(t_{\ell_k}) = m$.

Clearly $T(b_i b_j) = T(b_i)\, T(b_j)$, $1 \leq i, j \leq m$, translates into a conjunction of $m^2.n$ polynomial equations $(H)(\vec{c},\vec{d},\vec{t})$ in the variables $\vec{c},\vec{d},\vec{t}$ with coefficients in $\mathbb{Z}$. This proves:

Lemma 6: The $(\vec{c},\vec{d})$ such that $A\vec{c}$, $A\vec{d}$ are fields over K and $A\vec{c}$ is K-embeddable in $A\vec{d}$ form a first-order definable subset of $K^{m^3} \times K^{n^3}$.

Of most importance to us is the case $m = n$ of the above. Recalling that composition of linear maps $K^m \to K^m$ corresponds to multiplication of their matrices, we easily deduce:

Lemma 7: For each finite group G, the $\vec{c}$ such that $A\vec{c}$ is a field and $\mathrm{Aut}(A\vec{c}|K) \cong G$ form a first-order definable subset of K^{m^3}.

More generally:

Lemma 8: For each finite group G, the $(\vec{c},\vec{d})$ such that $A\vec{c}$ and $A\vec{d}$ are fields (over K) so that $\mathrm{Aut}(A\vec{d}|A\vec{c}) \cong G$, form a first-order definable subset of $K^{m^3} \times K^{n^3}$.

Important note. In each lemma in the subsection, the definition of the appropriate first-order definable set is independent of K, and can be effectively constructed from m,n,G.

§2. The Cologic for Profinite Groups.

(2.1) Let PROFIN be the category of profinite groups with the epis, i.e., the continuous surjective group homomorphisms, as morphisms. We will develop a model theory for PROFIN.

First we define auxiliary first-order structures dual to profinite groups. The basic idea is simple. A profinite group is an inverse limit of finite groups. There is a standard method [C-K] for making a (category-theoretic) diagram of first-order structures into a first-order structure. Modified to the present situation this leads to the following.

Definition: An inverse system (of groups) is a structure $\langle S, \leq, C, P\rangle$ where

(i) $\leq$ is a preorder on S; it has the unqiue largest element;

(ii) C is a subset of S^2;

(iii) P is a subset of S^3;

(iv) [Let $\approx$ be the equivalence relation on S induced by $\leq$, $[\alpha]$ the equivalence class of $\alpha \in S$ in $S/\approx$, and $\preceq$ the induced partial order on $S/\approx$.] $\leq$ is directed downwards;

(v) $P \subset \bigcup_{\alpha} [\alpha]^3$, and on each $[\alpha]$ P is the graph of a binary operation making $[\alpha]$ into a group $[\![\alpha]\!]$;

(vi) $C \subset \bigcup_{\alpha\leq\beta} [\alpha] \times [\beta]$ and on $[\alpha] \times [\beta]$ C is the graph of a morphism $\pi_{\alpha\beta}$ of $[\![\alpha]\!]$ onto $[\![\beta]\!]$;

(vii) $\pi_{\alpha\alpha} = 1_{[\alpha]}$, and if $\alpha \leq \beta \leq \gamma$, then $\pi_{\alpha\gamma} = \pi_{\beta\gamma} \circ \pi_{\alpha\beta}$.

Let L_0 be the first-order language for such structures. Clearly the class of inverse systems is finitely axiomatizable in L_0.

Now, for reasons to appear later, we adjoin to L_0 unary predicates R_n $(n \in \omega)$ to get a language L.

Definition: A stratified inverse system (of groups) is a structure $\langle S, \leq, C, P, R_n\ (n \in \omega)\rangle$, where

(i) $\langle S, \leq, C, P\rangle$ is an inverse system of groups;

(ii) $R_n = \{\alpha : [\alpha]$ has cardinal $\leq n\}$.

Clearly the class of stratified inverse systems is L-axiomatizable.

Next we add a more stringent condition.

Definition: A complete system (of groups) is a stratified inverse system such that if $\gamma \in R_n$ $(n \in \omega)$ and N is a normal subgroup of $[\![\gamma]\!]$, then there is a δ, unique up to $\approx$, with $\gamma \leq \delta$ and $N = \ker \pi_{\gamma\delta}$. It must also satisfy the following sentence: $R_n(x) \wedge R_n(y) \rightarrow \exists z\, R_{n^2}(z) \wedge z \leq x \wedge z \leq y$.

Note that the class of complete systems is L-axiomatizable. Finally,

Definition: A stratified inverse system is ranked if $S = \bigcup_n R_n$, i.e., if each $[\alpha]$ is finite.

Clearly ranked is $L_{\omega_1,\omega}$-axiomatizable. Let CRS be the category of complete ranked systems, with the L-embeddings as morphisms. We now establish the duality between PROFIN and CRS.

(2.2) Let G be a profinite group. We construct an object $S(G)$ of CRS, thus $S(G)$ is $\langle S,\leq,C,P,R_n (n \in \omega)\rangle$, where the ingrediants are defined as follows. $S = \bigcup_N G/N$, where N ranges over all open normal subgroups of G. (G/N is the set G/N). It is technically important to note that $G/N_1 \cap G/N_2 = \phi$ unless $N_1 = N_2$.

Define $\leq$ on S by: $g\,N \leq h\,M \leftrightarrow N \subset M$.

Define C by:

$$C(gN,hM) \leftrightarrow N \subset M \text{ and } gM = hM.$$

Define P by:

$$P(g_1N_1,g_2N_2,g_3N_3) \leftrightarrow N_1 = N_2 = N_3 \text{ and } g_1g_2N_1 = g_3N_1.$$

Define R_n by:

$$gN \in R_n \leftrightarrow G/N \text{ has cardinality } \leq n.$$

Clearly P describes multiplication in each G/N, and C the canonical maps $G/N \to G/M$ for $N \subset M$.

Evidently $S(G)$ is a complete ranked system.

S on morphisms. Let $\varphi : G \to H$ be a morphism in PROFIN (recall φ is surjective). We must define $S(\varphi)$ as an embedding of $S(H)$ into $S(G)$. This is described by: $S(\varphi)(hN) = g\varphi^{-1}(N)$, where N is open normal in H, $h \in H$ and $g \in G$ satisfies $\varphi(g) = h$.

Clearly $S(\varphi)$ is well-defined, 1-1 and respects $\leq$. Note that $S(\varphi)(hN) = \varphi^{-1}(hN)$.).

The basic point is that $S(\varphi)$ restricted to the subset H/N of $S(H)$ gives the isomorphism $H/N \cong G/\varphi^{-1}(N)$ induced by φ. This easily implies that $S(\varphi)$ is an L-embedding.

S is a contravariant functor from PROFIN into CRS.

(This is immediate from $S(\varphi)(hN) = \varphi^{-1}(hN)$.)

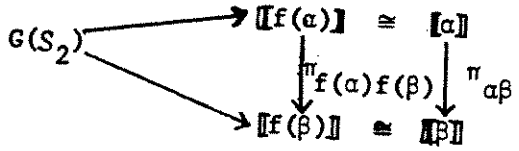
The functor G. Let $S = \langle S, \leq, C, P, R_n (n \in \omega) \rangle$ be a complete ranked system. We construct a profinite group $G(S)$. Let I be $S/\approx$, partially ordered by the converse of $\trianglelefteq$. Let $G_i = [\![\alpha]\!]$, where $i = [\alpha] \in I$, and for $i = [\alpha] \trianglelefteq [\beta] = j$, i.e. $i \geq j$ in I, let $p_{ij} : G_i \to G_j$ be $\pi_{\alpha\beta}$. Then $\langle G_i, p_{ij} \rangle_{i \geq j}$ is a projective system of finite groups.

Let $G(S)$ be the projective limit (identified as a closed subgroup of $\prod_i G_i$).

G on maps. Let $f : S_1 \to S_2$ be an L-embedding of complete ranked systems. We want to define a morphism $G(f) : G(S_1) \to G(S_2)$ in PROFIN.

Note that f respects $\approx$, so for α in S_1 the image of $[\alpha]$ is included in $[f(\alpha)]$. But since f respects the R_n, f restricts to a bijection of $[\alpha]$ onto $[f(\alpha)]$. Since f respects P, it induces an isomorphism $[\![\alpha]\!] \cong [\![f(\alpha)]\!]$.

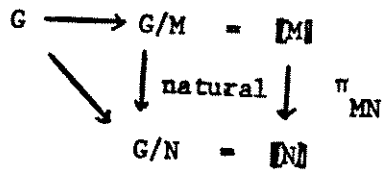
For $\alpha \leq \beta$ in S_1 we have a diagram



which commutes because f respects C. Hence these diagrams induce a morphism $G(f) : G(S_2) \to G(S_1) = \varprojlim [\![\alpha]\!]$.

Functoriality of G. A simple computation shows that G is a contravariant functor from CRS into PROFIN.

The Natural Isomorphisms. We compare first (for G a profinite group) G and $G(S(G))$. We have a commutative diagram



for $M \subset N$ open normal in G. These diagrams induce an obvious isomorphism $\theta_G : G \cong G(S(G)) = \varprojlim [\![M]\!]$, and the family $\langle \theta_G \rangle_{G \in \text{PROFIN}}$ is a natural

isomorphism between the functors 1_{PROFIN} and GS.

Next we compare S and $S(G(S))$, S a complete ranked system. This is the first place where completeness is used. Let $S = \langle S, \leq, C, P, R_n (n \in \omega) \rangle$. We define

$$\psi_S : S \to S(G(S)).$$

Let $\alpha \in S$ and consider $[\![\alpha]\!]$. Let N_α be the kernel of the natural $G(S) \twoheadrightarrow [\![\alpha]\!]$. N_α is open normal in $G(S)$. $\psi_S(\alpha)$ should be an element of $G(S)/N_\alpha$. Which one?

Clearly the one corresponding to $\alpha \in [\![\alpha]\!]$ under the <u>canonical</u> isomorphism $G(S)/N_\alpha \cong [\![\alpha]\!]$.

So ψ_S is certainly a set map from S to $S(G(S))$. One checks easily that ψ_S is an S-embedding. To get ψ_S surjective one needs the completeness condition. We leave this as a simple exercise. Hence $\langle \psi_S \rangle$ gives a natural isomorphism between the functors 1_{CRS} and SG.

It is readily checked, and important, that, for profinite G, the maps

$$S(\theta_G): SGS(G) \to S(G) \quad \text{and}$$
$$\psi_{S(G)}: S(G) \to SGS(G)$$

are mutually inverse.

(2.3) We now use the preceding duality to get a model theory.

Co-ultraproducts. Let $(G_i)_{i\in I}$ be a family of profinite groups. Let D be an ultrafilter on I. Form the L-structure

$$\prod_{i\in I} S(G_i)/D.$$

This structure is a complete stratified inverse system but is not necessarily ranked. There is however, a natural notion of ranked part.

Definition: Let $S = \langle S,\leq,C,P,R_n (n \in \omega)\rangle$ be a stratified inverse system. We define its ranked part S^o as the substructure of S with universe $S \cap (\cup R_n)$.

So S^o is a ranked stratified inverse system, in particular $\Pi^o S(G_i)/D$, defined as $(\Pi S(G_i)/D)^o$, is in CRS.

Now we look for a Łoś Theorem. This involves working with a fragment of the logic L. The set of bounded L-formulas is defined as the smallest set of L-formulas containing the atomic formulas, closed under connectives, and closed under

$$\Phi \mapsto \exists v(R_n(v) \wedge \Phi) \quad (n \in \omega,\ v \text{ a variable}).$$

Lemma 9. Let S be a stratified inverse system and $\Phi(v_1,\ldots,v_n)$ a bounded L-formula, $\alpha_1,\ldots,\alpha_n \in |S^o|$. Then
$S \models \Phi(\alpha_1,\ldots,\alpha_n) \Leftrightarrow S^o \models \Phi(\alpha_1,\ldots,\alpha_n)$.

Proof: By induction on the complexity of Φ . ∎

An immediate consequence of lemma 9 and Łoś'Theorem is:

Lemma 10: For each bounded L-formula $\Phi(v_1,\ldots,v_n)$, and all $f_1,\ldots,f_n \in \Pi S(G_i)$ with $f_1/D,\ldots,f_n/D$ in $\Pi^o S(G_i)/D$:

$$\Pi^o S(G_i)/D \models \Phi(f_1/D,\ldots,f_n/D)$$
$$\Leftrightarrow$$
$$\{i \in I : S(G_i) \models \Phi(f_1(i),\ldots,f_n(i))\} \in D.$$

This prompts the following definitions.

Definitions:

(a) A b-elementary map of L-structures is an embedding between L-structures preserving bounded L-formulas.

(b) The co-ultraproduct

$$\Pi^o G_i/D \text{ is defined as } G(\Pi^o S(G_i)/D).$$

When all $G_i = G$ we write $\overset{\circ}{G}{}^I/D$, and call this the co-ultrapower.

The diagonal $\Delta : S(G) \to S(G)^I/D$ sends $S(G)$ into the ranked part of $S(G)^I/D$ and so induces $G(\Delta) : \overset{\circ}{G}{}^I/D \to G(S(G))$, and identifying $G(S(G))$ with G via θ_G, this gives the codiagonal map

$$\nabla : \overset{\circ}{G}{}^I/D \to G.$$

By the last lemma, Δ is b-elementary from $S(G)$ to the ranked part of $S(G)^I/D$. Therefore, from a heuristic point of view, ∇ seems a good example of a coelementary map. So

Definition: An epi $\varphi : G \to H$ is coelementary if $S(\varphi)$ is b-elementary.

Lemma 11: If $(G_i, \varphi_{ij})_{i \geq j}$ is an inverse system of profinite groups such such that all φ_{ij} are coelementary, then each induced map $\varphi_i : \varprojlim G_i \to G_i$ is coelementary.

Proof: It is easy to prove by induction on the complexity of bounded L-formulas that if $(S_i, f_{ij})_{i \leq j}$ is a direct system of L-structures and all f_{ij} are b-elementary, then each induced embedding $f_i : S_i \to \varinjlim S_i$ is b-elementary.

Now dualize. ∎

Functoriality of co-ultraproduct. The preceding constructions act on morphisms as follows. Let $\varphi_i : G_i \to H_i$ $(i \in I)$ be morphisms in PROFIN. These induce $S(\varphi_i) : S(H_i) \to S(G_i)$, whence

$$S(\varphi_i)/D : \Pi S(H_i)/D \to \Pi S(G_i)/D \quad ,$$

and the latter clearly restricts to an embedding of the respective ranked parts. Applying the functor G to this, one gets

$$G(\, S(\varphi_i)/D) : \Pi^{\circ} G_i/D \to \Pi^{\circ} H_i/D \quad .$$

We denote this morphism (in PROFIN) by $\Pi^{\circ}\varphi_i/D$. In the special case when each φ_i is $\varphi : G \to H$, we get a morphism written as φ^{*I}/D.

This makes ${}^{\circ}I/_D$ a functor PROFIN$^{-} \to$ PROFIN, and ∇ gives a natural transformation from ${}^{\circ}I/_D$ to the identity, dual to the situation for I/D and Δ in first-order logic.

(2.4) Coformulas and Cosatisfaction.

We are taking here a utilitarian approach to setting up a cologic for profinite groups. We are of course aware that most of what we do can be done for profinite algebras. We believe that a more abstract category-theoretic approach to coformulas and cosatisfaction is possible and desirable, but we leave that for another occasion.

Definition: A coformula (for profinite groups) is a bounded L-formula

For an L-structure S we have the usual notion of L_S, L extended by constants for S. S is then construed as an L_S-structure. We have the obvious notion of bounded L_S-formulas.

Definition: (G profinite) A coformula over G is a bounded $L_{S(G)}$-formula. A cosentence (resp. cosentence over G) is a coformula (resp. coformula over G) which is a sentence.

Definition: Let $\Phi(v_1,\ldots,v_n)$ be a coformula over G, and let $\gamma_1,\ldots,\gamma_n \in S(G)$. G cosatisfies $\Phi(\gamma_1,\ldots,\gamma_n)$ (written $G \dashv \Phi(\gamma_1,\ldots,\gamma_n)$) iff $S(G) \models \Phi(\gamma_1,\ldots,\gamma_n)$.

The reader should observe that the "coelements" in this theory are cosets.

Definition: The cotheory of G (written $\mathrm{Coth}(G)$) is the set of all cosentences Φ such that $G \dashv \Phi$. $G \equiv^{o} H$ (G is coequivalent with H) if $\mathrm{Coth}(G) = \mathrm{Coth}(H)$.

Note that our previous definition of coelementary morphism can now be expressed as follows:

An epi $\varphi : G \to H$ is coelementary iff for all coformulas $\Phi(v_1,\ldots,v_n)$ and all open cosets $\gamma_1,\ldots,\gamma_n$ of H (i.e., cosets of open normal subgroups of H) we have

$$H \dashv \Phi(\gamma_1,\ldots,\gamma_n) \Leftrightarrow G \dashv \Phi(\varphi^{-1}(\gamma_1),\ldots,\varphi^{-1}(\gamma_n)).$$

(2.5) Co-types and Cosaturation. The definitions here are slightly less routine.

Definition: A set Σ of coformulas over G is ranked if for every variable v occurring free in some member of Σ there is an $n \in \omega$ such that the coformula $R_n(v)$ is in Σ.

Definition: Let Σ be a set of coformulas over G, with V as its set of free variables. A function $f : V \to$ open cosets of G is said to realize Σ in G if for every $\Phi(v_1,\ldots,v_n)$ in Σ we have $G \dashv \Phi(f(v_1),\ldots,f(v_n))$. Σ is realized in G if some f realizes Σ.

Definition: A V-type over G is a ranked set Σ of coformulas such that V includes the set of free variables of Σ and every finite subset of Σ is realized in G.

Finally,

Definition: (i) G is κ-cosaturated if every V-type over G of cardinal $\leq \kappa$ is realized in G.

(ii) G is cosaturated if G is κ-cosaturated where κ is the cardinal of the set of open cosets of G.

The explanation of the last clause is that the cardinal of $S(G)$ is the cardinal of the set of open cosets of G (and if G is infinite is the cardinal of the set of normal open subgroups of G).

Isomorphism of Cosaturated G. We come now to a theorem which is the dual of a basic theorem in model theory [C-K], and is of theoretical importance for the model theory of fields.

Lemma 12: Suppose κ is infinite and G_1, G_2 are κ-cosaturated. Consider a diagram in PROFIN

$$\begin{array}{ccc} G_1 & & G_2 \\ {\scriptstyle\theta_1}\downarrow & \overset{\varphi}{\underset{\sim}{\longrightarrow}} & \downarrow{\scriptstyle\theta_2} \\ H_1 & & H_2 \end{array}$$

where i) each H_i has $<\kappa$ open normal subgroups

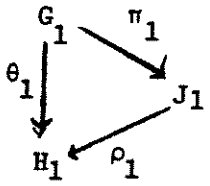
ii) for all coformulas $\Phi(v_1,\ldots,v_n)$ and all open cosets $\gamma_1,\ldots,\gamma_n$ of H_1

$G_1 \models \Phi(\theta_1^{-1}(\gamma_1),\ldots,\theta_1^{-1}(\gamma_n)) \leftrightarrow G_2 \models \Phi(\theta_2^{-1}(\varphi(\gamma_1)),\ldots,\theta_2^{-1}(\varphi(\gamma_n)))$.

(If this condition holds we write

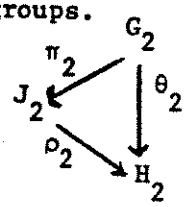
$(G_1,\theta_1) \equiv^{o}_{\varphi} (G_2,\theta_2)$.)

Suppose one has a commuting diagram

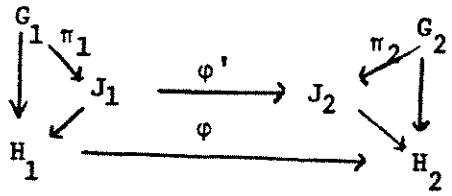


where J_1 has $<\kappa$ normal open subgroups.

Then there is a commuting diagram



and $\varphi' : J_1 \tilde{\to} J_2$ so that the following commutes:



and such that $(G_1,\pi_1) \equiv^{o}_{\varphi'} (G_2,\pi_2)$.

Proof: Let V be a set of variables and f a bijection of V onto the set of open cosets of J_1.

Let Σ be the set of all coformulas (over G_1 in the free variables V) $\Phi(\theta_1^{-1}(\gamma_1),\ldots,\theta_1^{-1}(\gamma_k), v_1,\ldots,v_n)$ where $\gamma_1,\ldots,\gamma_k$ are open cosets of H_1 and $G_1 \models (\theta^{-1}(\gamma_1),\ldots,\theta^{-1}(\gamma_k), \pi_1^{-1}(f(v_1),\ldots,\pi_1^{-1}(f(v_n)))$.

(We are looking at the "cotype" of J_1 over H_1 in G_1.) Σ is of course ranked, and realized in G_1.

Now let Σ^{φ} be the set of all coformulas

$\Phi(\theta_2^{-1}(\varphi(\gamma_1)),\ldots,\theta_2^{-1}(\varphi(\gamma_k)), v_1,\ldots,v_n)$ such that $\Phi(\theta_1^{-1}(\gamma_1),\ldots,\theta_1^{-1}(\gamma_k),v_1,\ldots,v_n)$ is in Σ. Σ^φ is ranked.

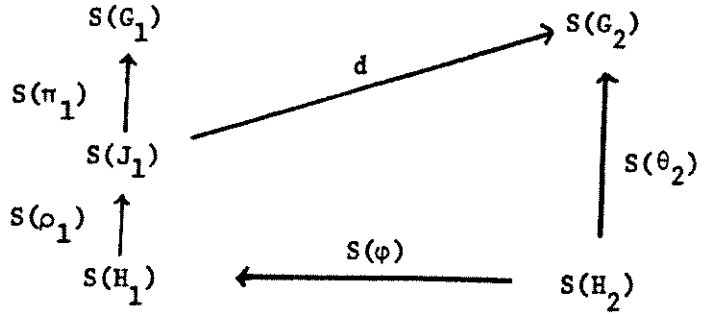
We claim Σ^φ is a V-type over G_2.

Let Σ_0 be a finite subset of Σ. Σ_0 involves only free variables in a finite subset V_0. For v in V_0, select $n(v)$ so that $R_{n(v)}(v)$ is in Σ. Then

$$G_1 \models \exists \vec{v} \left(\bigwedge R_{n(v)}(v) \wedge \bigwedge \Sigma_0\right)$$

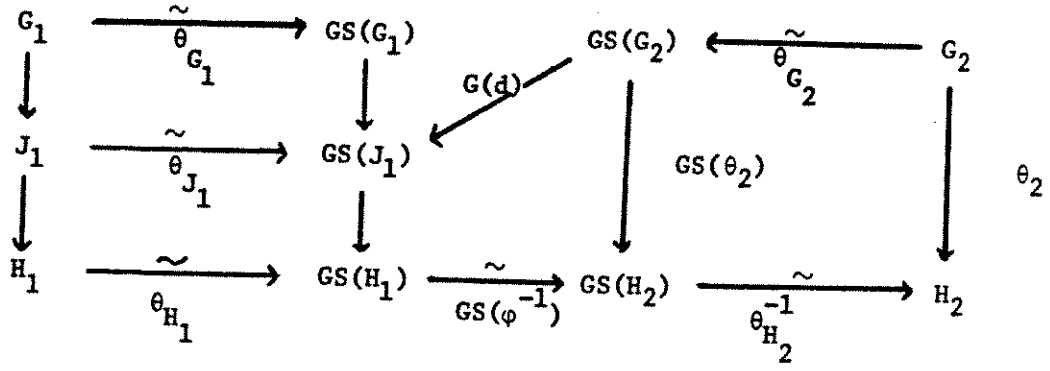
where $\vec{v}$ consists of the variables of V_0. So by (ii) $G_2 \models \exists v(\bigwedge R_{n(v)}(v) \wedge \bigwedge \Sigma_o^\varphi)$. So Σ^φ is a V-type over G_2. Σ^φ has cardinal $<\kappa$, hence is realized in G_2, say by $g: V \to$ set of open cosets of G_2.

What does g give us? Precisely, an L-structure embedding $d: S(J_1) \to S(G_2)$ so that the following commutes:



($d(\gamma) = g(v)$, if $f(v) = \gamma \in S(J_1)$.)

Now we apply the functor G to the above and take account of the natural isomorphism between GS and the identity. We get a commuting diagram:



Note that the bottom line represents $\varphi : H_1 \xrightarrow{\sim} H_2$, by naturality.

So our problem is solved by taking J_2 as $GS(J_1)$, π_2 as $G(d) \circ \theta_{G_2}$, ρ_2 as $\theta_{H_2}^{-1} \circ GS(\varphi^{-1}) \circ GS(\rho_1)$, and φ' as θ_{J_1}.

That $(G_1,\pi_1) \equiv^{o}_{\varphi} (G_2,\pi_2)$ holds amoints to the following. We know by construction that for any coformula $\Phi(v_1,\ldots,v_n)$ and open cosets $\gamma_1,\ldots,\gamma_n$ of J_1:

$$G_1 \models \Phi(\pi_1^{-1}(\gamma_1),\ldots,\pi_1^{-1}(\gamma_n)) \leftrightarrow G_2 \models \Phi(d(\gamma_1),\ldots,d(\gamma_n)),$$

and we want to replace the last condition by

$$G_2 \models \Phi(\pi_2^{-1}\varphi'(\gamma_1),\ldots,\pi_2^{-1}(\varphi'(\gamma_n)))$$

i.e.

$$G_2 \models \Phi(S(\varphi')^{-1}\pi_2)(\gamma_1),\ldots,S((\varphi')^{-1}\pi_2)\gamma_n)).$$

From the definitions of π_2 and φ' it follows easily that $S((\varphi')^{-1}\pi_2) = d$. (Write $SG(d) = \psi_{S(G_2)} d \psi^{-1}_{S(J_1)}$, and use the remark at the end of (2.2).)

This proves the lemma.

■

We can now formulate the main theorem.

Theorem 13. Let G_1 and G_2 be cosaturated, with the same number of open normal subgroups. Suppose we have a diagram in PROFIN

$$\begin{array}{ccc} G_1 & & G_2 \\ {\scriptstyle\theta_1}\downarrow & & \downarrow{\scriptstyle\theta_2} \\ H_1 & \xrightarrow[\varphi]{\sim} & H_2 \end{array}$$

where H_i has fewer open subgroups then G_i and $(G_1,\theta_1) \equiv^{\circ}_{\varphi} (G_2,\theta_2)$. Then there exists $\varphi' : G_1 \xrightarrow{\sim} G_2$ such that

$$\begin{array}{ccc} G_1 & \xrightarrow{\varphi'} & G_2 \\ \downarrow & & \downarrow \\ H_1 & \xrightarrow{\varphi} & H_2 \end{array}$$

commutes. (φ can be lifted to an isomorphism $G_1 \cong G_2$.)

Proof: Use the lemma to construct φ' by a back and forth projective limit argument.

■

In first order logic one has the basic result [C-K] relating saturation to universality and homogeneity. The dual will be quite evident to anyone who has mastered the preceding proof. Nevertheless it is convenient to set down the appropriate definitions and note the main result.

Definition. The cocardinal of G is the cardinal of $S(G)$.

Definition. G is κ-couniversal of for every $H \equiv^{o} G$ of cocardinal $<\kappa$ there is a coelementary $G \twoheadrightarrow H$.

Definition. G is κ-cohomogeneous if every diagram

$$\begin{array}{ccc} & & G \\ & & \downarrow \\ H_2 & \twoheadrightarrow & H_1 \end{array}$$

with H_2 of cocardinal κ, the vertical maps coelementary, and such that there exists a coelementary $G \twoheadrightarrow H_2$, can be completed to a commuting diagram by a coelementary $G \twoheadrightarrow H_2$.

Now one easily gets the following addendum to Theorem 13.

Theorem 13A: $(\kappa \geq \aleph_0)$. G is κ-cosaturated iff G is κ-couniversal and κ-cohomogeneous.

(2.6) Lowenheim-Skolem Phenomena

We shall need two duals of basic theorems.

Theorem 14: If for some n G has infinitely many open subgroups of index n, then for each $\kappa \geq$ cocardinal of G there exists coelementary $H \twoheadrightarrow G$ with $\kappa =$ cocardinal of H.

Before we prove this, let us note that each open subgroup of index n of a profinite group G contains an open normal subgroup of index $\leq n!$. This implies that if G is infinite, then the number of open subgroups equals the number of normal open subgroups. It also shows that, under the hypothesis of the theorem, there exists n such that G has infinitely many normal open subgroups of index n.

Proof: Our hypothesis implies that for some n the R_n of $S(G)$ is infinite. So by upward Löwenheim-Skolem and reduction there is a b-elementary $f : S(G) \to S$, S in CRS, S of cardinal κ. Applying G we obtain coelementary

$$G(f) : G(S) \to GS(G) \cong G,$$

and $G(S)$ has exactly κ open subgroups.

■

For the downward version we first define cocountable as: has only countably many open subgroups.

Theorem 15: For any G there is cocountable H and a coelementary $G \to H$.

Proof: As above we get H having $\leq \aleph_0$ open subgroups, whence H is cocountable.

In passing, we see that the dual of finite is having only finitely many open subgroups of each index. Groups with this property are called small. We shall come back to them in (2.10).

We add a word of clarification concerning the notions cocountable and separable. Evidently cocountable implies separable. However, the converse fails. An example is the unrestricted profinite completion $G[\ R\ ]$ of F_ω. This is of course separable, since F_ω is countable. It is a good exercise (after reading Proposition 23) to show that G has cocardinal $2^{\aleph_0}$.

(2.7) Isomorphic coelementary liftings

In first-order model theory, using the methods of Jónsson-Morley-Vaught [C-K] one proves that elementary equivalent structures have isomorphic elementary extensions. Dualizing appropriately, one easily proves:

Theorem 16: $G \equiv^{o} H$ iff there are coelementary epi's $G_1 \to G$ and $H_1 \to H$ with $G_1 \cong H_1$.

(2.8) From fields to groups

Let K be a field. A basic fact is that the cotheory of $G(K)$ is interpretable in K. Precisely,

Lemma 17: There is a recursive map $\hat{}$ from cosentences to sentences of field theory so that for each cosentence Φ : $G(K) \dashv \Phi \Leftrightarrow K \models \hat{\Phi}$.

Proof: Clear from section 1. Related is:

Lemma 18: (a) If K is κ-saturated, $G(K)$ is κ-cosaturated.

(b) If $K \prec L$, then the restriction $G(L) \to G(K)$ is coelementary.

Proof: Clear from the definitions and section 1.

Lemma 19: Let D be an ultrafilter on the index set I and let K_i, $i \in I$, be fields. Then $G(\Pi K_i/D)$ is canonically isomorphic to $\Pi^{o} G(K_i)/D$.

Proof: This is clear from the following well-known observations:

(A) A finite Galois extension of $\Pi K_i/D$ of dimension n can be naturally identified with some $\Pi L_i/D$, where L_i is a Galois extension of K_i, which is for almost all $i \in I$ of dimension n over K_i.

(B) In the above $G(\Pi L_i/D \mid \Pi K_i/D)$ is naturally isomorphic to $\Pi G(L_i|K_i)/D$.

■

(2.9) The Maximality Theorem

Here we offer a foundational theorem expressing that as far as model theory of fields is concerned our comodel theory is optimal.

Theorem 20: Let F be a class of objects, and $\dashv^*$ a relation between profinite groups and elements μ of F satisfying:

i) $(G \cong H$ and $G \dashv^* \mu) \Rightarrow H \dashv^* \mu$;

ii) for every μ there exists μ^*, a sentence of field theory, such that for all fields K : $K \models \mu^* \Rightarrow G(K) \dashv^* \mu$.

Then we have for any fields K_1 and K_2: if $G(K_1) \equiv^0 G(K_2)$, then for all μ: $G(K_1) \dashv^* \mu \Leftrightarrow G(K_2) \dashv^* \mu$.

Proof: Suppose K_1, K_2 and μ give a counterexample, so $G(K_1) \equiv^0 G(K_2)$, $K_1 \models \mu^*$ and $K_2 \models \neg(\mu^*)$, say. A limit argument as in Lemma 12 will give elementary extensions K_1^* of K_1 and K_2^* of K_2 such that $G(K_1^*) \cong G(K_2^*)$. So $G(K_1) \dashv^* \mu \Rightarrow G(K_2) \dashv^* \mu$. But $K_1 \models \mu^*$ and $K_2 \models \neg(\mu^*)$, hence $G(K_1) \dashv^* \mu$ and not $G(K_2) \dashv^* \mu$, contradiction.

This theorem, with lemma 17 shows that our comodeltheory is the maximal one interpretable in field theory.

(2.10) Coelementary classes

Before turning to RC-fields in the next section, we consider several special classes $\mathcal{C}$ of profinite groups. $\mathcal{C}$ will be respectively:

(a) the class of projective groups;

(b) the class of profinite groups satisfying Iwasawa's condition;

(c) the class of profinite groups isomorphic to a fixed small G;

(d) the class of profinite groups of rank $\leq e$ for a fixed $e \in \mathbb{N}$.

It turns out that each of these classes is coelementary, i.e. is the class of profinite groups cosatisfying a fixed set Σ of cosentences. From lemma 17 it follows that the class of fields K with $G(K) \neq \Sigma$ is elementary.

Projective Profinite Groups

A profinite group G is called projective if every diagram

$$\begin{array}{ccc} & & G \\ & & \downarrow \\ B & \to & A \end{array}$$

where $B \to A$ is an epi between profinite groups, can be completed by a $G \to B$ to a commutative diagram.

Proposition 21. The class of projective profinite groups is coelementary.

Proof: A projective limit argument, cf. [G, p.157], shows that G is projective iff in the above diagrams one only considers finite groups A,B. It is no loss of generality to restrict further to the case that $G \to A$ is

an epi, in fact a canonical map $G \xrightarrow{\pi} G/M$, M open normal in G. So to show that G is projective it suffices to complete diagrams

$$\begin{array}{ccc} & & G \\ & & \downarrow \pi \\ B & \xrightarrow{\alpha} & G/M \end{array} \qquad (*)$$

with M open normal in G, B finite.

It is clear that for given $n \in \mathbb{N}$ we have the equivalence:

each diagram $(*)$ with $\#(B) \leq n$ can be completed

$\Leftrightarrow$

for each open $M \lhd G$ and each epi $\alpha : B \to G/M$ with $\#(B) \leq n$ there is open $N \lhd G$, $N \subset M$ and an embedding $G/N \to B$ such that the composition $G/N \to B \xrightarrow{\alpha} G/M$ is the canonical map.

We leave it to the reader to check that the second half of the equivalence can be said (or cosaid) by a cosentence $Pr(n)$. Hence G is projective iff $G \models Pr(n)$, for all $n \in \mathbb{N}$.

■

The Iwasawa Property

Recall that $Im(G)$ is the class of finite groups isomorphic with some G/M, M open normal in G. In [I, §2] Iwasawa isolated a condition which turns out to be the dual of ω-homogeneity (in Jónsson's sense).

Definition: A profinite group G has the Iwasawa property (IP) if every diagram

$$\begin{array}{ccc} & & G \\ & & \downarrow \\ B & \to & A \end{array}$$

, where both maps are epis and $B \in Im(G)$, can be completed by an epi $G \to B$ to a commuting diagram. It is easily verified that G has

IP iff for each isomorphism $G/M_1 \cong G/M_2$, M_1 and M_2 open normal in G, and for each open normal $N_1 \subset M_1$ there exists open normal $N_2 \subset M_2$ such that α lifts to an isomorphism $G/N_1 \cong G/N_2$.

This leads immediately to:

Proposition 22. The class of profinite groups with IP is coelementary.

Bearing in mind our remark about IP and ω-homogeneity, one expects:

Proposition 23. Suppose G_1 and G_2 are cocountable, with IP, and $\mathrm{Im}(G_1) = \mathrm{Im}(G_2)$. Then any isomorphism $G_1/M_1 \cong G_2/M_2$, M_1 open normal in G_1 and M_2 open normal in G_2, lifts to an isomorphism $G_1 \cong G_2$.

Proof: See Iwasawa [I, §2], or dualize the back and forth argument. ∎

Corollary 24. The isomorphism-type of a cocountable G with IP is determined by Im(G).

Proof: Take $M_1 = G_1$ and $M_2 = G_2$ in the proposition. ∎

Corollary 25. The cotheory of any G with IP is determined by Im(G).

Proof: Immediate from corollary 24 and Theorem 15. ∎

When we deal later with RC-fields K with $G(K)$ having IP, the following considerations will be important. Let us say that G has IP_κ if every diagram

$$\begin{array}{ccc} & & G \\ & & \downarrow \\ B & \to & A \end{array}$$

where both maps are epis, B has less than κ open subgroups, and for which there exists an epi $G \to B$ can be completed to a commuting diagram by an epi $G \to B$.

Lemma 26 (a): If G is κ-cosaturated and has IP, then G has IP_κ.
(b) Suppose G_1 and G_2 have IP_κ, κ infinite, and $\mathrm{Im}(G_1) = \mathrm{Im}(G_2)$. Suppose one has epis $G_1 \to H_1$, $G_2 \to H_2$, and an isomorphism $\phi : H_1 \cong H_2$. Suppose H_1 is of cocardinal $< \kappa$. Then $(G_1, \theta_1) \overset{o}{\equiv}_\phi (G_2, \theta_2)$.

Proof (a): (Sketch) Dualize, and use [M] to get a back and forth system "over $S(\phi)$".

■

Examples: Jarden-Kiehne [J-K] and Jarden [J3] consider only perfect RC-fields K with $G(K) \cong \hat{F}_e$ and $G(K) \equiv \hat{F}_\omega$. That $\hat{F}_e$ has IP is proved in [J-K] using a result of Gaschutz. That $\hat{F}_\omega$ has IP is due to Iwasawa, [I, §2]. Note that these profinite groups are also projective.

A rich source of projective profinite groups with IP is due to Mel'nikov [M]: he showed that all closed normal subgroups of free profinite groups of rank >1 are among them. Closed normal subgroups of free profinite groups of rank >1 have moreover the remarkable property that, while

often not free themselves, all their proper open subgroups are free (as profinite groups), see [M] and [Lu-vd D].

In (7.2) we give an example of a projective profinite group (of finite rank) which does not have IP. Finite simple groups are examples of profinite groups with IP which are not projective.

Axiomatizing small G

Recall from (2.6) that 'small' (having only finitely many open subgroups of each index) is the dual of finite. Reinforcing this analogy are the following facts, proved by Schuppar in [S], for small G and arbitrary H:

1. Each epi $G \to G$ is an iso.
2. $\mathrm{Im}(G) \supset \mathrm{Im}(H)$ iff there exists an epi $G \to H$.
3. $\mathrm{Im}(G) = \mathrm{Im}(H)$ iff $G \cong H$ (immediate from 1. and 2.).

Proposition 27: Let G be small. The class of all $H \cong G$ is coelementary.

Proof: Immediate from fact 3. above. ∎

Profinite groups of finite rank

Proposition 28: Let $e \in \mathbb{N}$. The class of profinite groups of rank $\leq e$ is coelementary.

Proof: An easy projective limit argument shows:

$\mathrm{rk}(G) \leq e \Leftrightarrow$ each $A \in \mathrm{Im}(G)$ can be generated by $\leq e$ elements.

∎

Remarks: (i) It is well known that finitely generated profinite groups are small.

(ii) The class of profinite groups of rank =e is not coelementary, for $e \geq 1$. This is an instructive exercise.

(2.11) See 40 (a).

§3. The Embedding Lemma and elementary invariants for RC Fields.

(3.1) The main novelty of this section is a systematic development of the model theory of RC fields which are not necessarily perfect. With the exception of Eršov [E2] and Wheeler [Wh], previous work was restricted to the perfect case. Wheeler's definition of PAC-fields allows imperfect fields K but only those with $[K : K^p] = p$, $\mathrm{char}(K) = p > 0$. In writing our paper in its present generality we had access to Eršov's paper, which has no proofs and is apparently done under special hypothesis (namely Iwasawa Galois groups). It is mainly because of the kind assistance of Tamagawa that we have been able to proceed with perfect (or imperfect?) generality.

(3.2) Recall that a field K is regularly closed iff

(a) each absolutely prime ideal of $K[X]$, $X = (X_1,\ldots,X_n)$, has a K-rational zero.

It is routine to show that condition (a) is equivalent to each of the following:

(b) for each domain A which is finitely generated as K-algebra and regular over K there is a K-algebra morphism $A \to K$;

(2.11) The following will be needed later in lemmas 31 and 36.

Lemma 28a: Let M_1, M_2 be open normal subgroups of G_1, G_2 and ϕ an isomorphism $G_2/M_2 \cong G_1/M_1$ (inducing an isomorphism $S(\phi) : S(G_1/M_1) \xrightarrow{\sim} S(G_2/M_2)$. Suppose for all coformulas ψ and all cosets $\alpha_1,\ldots,\alpha_n$ of M_1 in G_1 we have:

$$G_1 \models \psi(\alpha_1,\ldots,\alpha_n) \leftrightarrow G_2 \models \psi(S(\phi)(\alpha_1),\ldots,S(\phi)(\alpha_n)).$$

Then for all coformulas $\psi(v_1,\ldots,v_n)$ and all $\beta_1,\ldots,\beta_n$ in $S(G_1/M_1)$ (which is a substructure of $S(G_1)$):

$$G_1 \models \psi(\beta_1,\ldots,\beta_n) \leftrightarrow G_2 \models \psi(S(\phi)(\beta_1),\ldots,S(\phi)(\beta_n))$$

Proof: The point is that each $\beta \in S(G_1/M_1)$ is definable in $S(G_1/M_1)$ from finitely many cosets $\alpha_1,\ldots,\alpha_k$ of M_1 by a coformula $\theta(v, \alpha_1,\ldots,\alpha_k)$ and that then $S(\phi)(\beta)$ will then be definable by the coformula $\theta(v, S(\phi)(\alpha_1),\ldots,S(\phi)(\alpha_n))$ in $S(G_2/M_2)$.

Let the natural map $G_1/M_1 \to [\beta]$ have kernel $\{\alpha_1,\ldots,\alpha_{k-1}\}$(cosets of M_1 in G_1), and let α_k be a coset of M, mapped onto β by $G_1/M_1 \to [\beta]$. Then β is the unique element of $S(G_1/M_1)$ such that $\alpha_k \leq \beta$, $\pi_{\alpha_k}(\alpha_k) = \beta$, and $\alpha_1,\ldots,\alpha_{k-1}$ are exactly the elements of $S(G_1/M_1)$ mapped by $\pi_{\alpha_k}\beta$ to the identity element of $[\beta]$. (Note: all this takes place inside $S(G_1/M_1)$ which is crucial.)

■

(c) K is existentially closed in each regular field extension.
(The basic fact one needs is that a prime ideal of K[X] is absolutely prime iff K[X]/I is regular over K, cf. [L, p. 71]).

Condition (c) suggests Robinson's Test. Later we refine it to get model completeness results.

(3.3) Our initial model-theoretic analysis of RC fields will use the technique of isomorphisms of saturated models. As usual, we require a lemma to give us the main step in a back and forth argument. For perfect RC fields, this lemma is the Embedding Lemma of Jarden-Kiehne [J-K]. To extend this to the general case we need some preliminary definitions and will quote a result of Tamagawa.

If A is a domain of characteristic $p > 0$, we define A^p as its subdomain of p^{th} powers. (If A is a field, so is A^p.) Suppose A has fraction field L. We call a family $(\alpha_i)_{i \in I}$ of elements of A p-independent in A if it is p-independent in L. See [Bo,p.133] for the basic material, and [L] for the following fact which we will use:

A domain A containing a field K is regular over K iff
(i) K is relatively algebraically closed in A;
(ii) K has p-basis remaining p-independent in A (if char(K) = p > 0).

Tamagawa proved the following on request from us.

Suppose K is RC of characteristic $p > 0$. Let A be a domain finitely generated as K-algebra and regular over K. Let $S \subset A$ be finite of

cardinality $\leq \#$ (p-basis of K) and p-independent in A. Then there exists a K-algebra morphism $f : A \to K$ such that the family $(f(s))_{s \in S}$ is p-independent in K.

See [T] for a proof. Now we transcribe Tamagawa's result to the κ-saturated case.

Lemma 29: Suppose K is RC of characteristic $p > 0$ and κ-saturated, $\kappa > \aleph_0$. Let A be a domain generated as K-algebra by $< \kappa$ elements and regular over K. Let $S \subset A$ be p-independent in A, and of cardinality $\leq \#$ (p-basis of K) in case $[K : K^p] < \infty$. Then there is a K-algebra morphism $f : A \to K$ such that the family $(f(s))_{s \in S}$ is p-independent in K.

Proof: Trivial, using Tamagawa's result quoted above.

■

Now we can generalize the Embedding Lemma of Jarden-Kiehne [J-K]. It's importance is that it reduces field-theoretic embedding problems to group-theoretic lifting ("co-embedding") problems.

Lemma 30: Let E/L, F/M be two regular field extensions of characteristic p. Suppose

(a) F is RC;

(b) F is $\#(E)^+$-saturated;

(c) if $p > 0$ and $[F : F^p] < \infty$, then $[E : E^p] \leq [F : F^p]$;

(d) Φ_0 is an isomorphism $\tilde{L} \cong \tilde{M}$ with $\Phi_0(L) = M$;

(e) $\phi : G(F) \to G(E)$ is an epi such that

$$\begin{array}{ccc} G(E) & \longleftarrow & G(F) \\ \downarrow & & \downarrow \\ G(L) & \underset{\hat{\Phi}_0}{\longleftarrow} & G(M) \end{array}$$

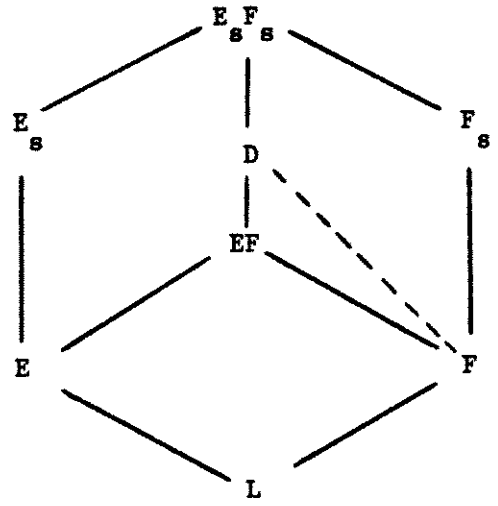
commutes, where $\hat{\Phi}_0$ is the isomorphism induced by Φ_0, and the vertical maps are restrictions.

Then Φ_0 extends to an embedding $\Phi : \tilde{E} \to \tilde{F}$ such that $\Phi(E) \subset F$, $\Phi((\phi\sigma)(x)) = \sigma(\Phi(x))$ for all $\sigma \in G_F$ and $x \in \tilde{E}$, and F is regular over its subfield $\Phi(E)$.

Proof: (following [J-K] as much as possible).

Without loss of generality we may assume that $L = M$ and that Φ_0 and $\hat{\Phi}_0$ are the identity. As E and F are regular over L we may also assume that not only E and F are linearly disjoint over L but also $\tilde{E}$ and $\tilde{F}$ over $\tilde{L}$ (in a common extension of $\tilde{E}$, $\tilde{F}$). Hence the map $x \otimes y \mapsto xy : \tilde{E} \otimes_{\tilde{L}} \tilde{F} \to \widetilde{EF}$ is an embedding. It follows that every $\sigma \in G(\tilde{F}/F)$ can be uniquely extended to $\tilde{\sigma} \in G(\widetilde{EF}/EF)$ with $\tilde{\sigma}x = (\phi\sigma)(x)$ if $x \in \tilde{E}$, $= \sigma(x)$ if $x \in \tilde{F}$, since $(\phi\sigma)(x) = x$ for $x \in \tilde{L}$. The map $\sigma \mapsto \tilde{\sigma}$ defines an injective morphism $G(\tilde{F}/F) \to G(\widetilde{EF}/EF)$ which restricts to an injective morphism $G(F_s/F) \to G(E_sF_s/EF)$. This last map has left inverse the natural restriction $G(E_sF_s/EF) \to G(F_s/F)$.

Let D = fixed field of the image of $G(F_s/F)$ in $G(E_sF_s/EF)$. So we have an isomorphism $G(E_sF_s/D) \cong G(F_s/F)$ given by restriction. It follows that $D \cap F_s = F$ and $DF_s = E_sF_s$. (1)



We claim that D/F is regular. (2)

D/F is certainly separable because D/EF and EF/F are separable. Also F is relatively algebraically closed in D; otherwise there is $f \in (\widetilde{F} \setminus F) \cap D$, but then f is separable algebraic over F, so $f \in F_s \cap D = F$, and we have a contradiction. The claim is proved. Now $\widetilde{E} = E_s E^{p^{-\infty}}$ (put $p^{-\infty} = 1$ if $p = 0$), so by (1) we get $\widetilde{E} \subset D^{p^{-\infty}} \widetilde{F}$, hence:

$$\widetilde{E} \subset \widetilde{E}\widetilde{F} = D^{p^{-\infty}} \widetilde{F} = D^{p^{-\infty}}[\widetilde{F}] = \widetilde{F}[D^{p^{-\infty}}] \qquad (3)$$

Take a subset D_0 of D of cardinal $< \kappa = \#(E)^+$ such that $E \subset D_0^{p^{-\infty}}$ $(= \{x^{p^{-n}} \mid x \in D_0, n \in \omega\})$ and $\widetilde{E} \subset \widetilde{F}[D_0^{p^{-\infty}}]$.

Let S be a p-basis of E. Because $F(D_0)/E$ is separable (D/EF and EF/E are separable), the set S is still p-independent in $F[D_0]$. $F[D_0]/F$ is regular by (2), so we may conclude from (b) and lemma 29 : there is an F-algebra morphism $\psi: F[D_0] \to F$ such that $(\psi(s))_{s \in S}$ is p-independent in F. Now $F(D_0) \subset D$ and $\widetilde{F}$ are linearly disjoint over F

by (2), so ψ can be extended to an $\widetilde{F}$-algebra morphism $\widetilde{\psi} : \widetilde{F}[D_0] \to \widetilde{F}$, which uniquely extends to an $\widetilde{F}$-algebra morphism $\widetilde{F}[D_0^{p^{-\infty}}] \to \widetilde{F}$, also denoted by $\widetilde{\psi}$.

Our definitions imply that

$$\widetilde{\psi}(\widetilde{\sigma}x) = \sigma\widetilde{\psi}(x) \qquad (4)$$

for every $\sigma \in G(\widetilde{F}/F)$ and each $x \in \widetilde{F} \cup D_0$, hence for each $x \in \widetilde{E}$. Let $\Phi : \widetilde{E} \to \widetilde{F}$ be the restriction of $\widetilde{\psi}$. Then $\Phi(E) \subset F$, $\Phi((\phi\sigma)(x)) = \sigma(\Phi x)$ for all $\sigma \in G(\widetilde{F}/F)$ and $x \in \widetilde{E}$.

It remains to show that F is regular over $\Phi(E)$. $F/\Phi(E)$ is separable because $(\Phi(s))_{s \in S}$ is a p-basis of $\Phi(E)$ which is p-independent in F. Now let $x \in \widetilde{E}$ and $\Phi(x) \in F$, i.e. $\Phi(x) \in \Phi(\widetilde{E}) \cap F$. Then $\Phi((\phi\sigma)(x) = \sigma(\Phi x) = \Phi x$ for all $\sigma \in G(\widetilde{F}/F)$, i.e. $(\phi\sigma)(x) = x$ for all $\sigma \in G(\widetilde{F}/F)$, hence by (e): $\tau(x) = x$ for all $\tau \in G(\widetilde{E}/E)$, which implies $x \in E^{p^{-\infty}}$. We have proved that $\Phi(\widetilde{E}) \cap F = (\Phi E)^{p^{-\infty}} \cap F$ which together with the separability of $F/\Phi(E)$ implies that $\Phi(E)$ is algebraically closed in F, whence $F/\Phi(E)$ is regular.

■

(3.4) Elementary equivalence of RC fields

Recall from Lemma 12 that if $\theta_i : G_i \to H_i$ are epis $(i = 1,2)$ and $\varphi : H_1 \cong H_2$, then we write $(G_1,\theta_1) \overset{\circ}{\equiv}_\varphi (G_2,\theta_2)$ (and say that (G_1,θ_1) and (G_2,θ_2) are coelementary equivalent over φ) if for all open cosets $\gamma_1,\ldots,\gamma_n$ of H_1 and coformulas $\psi(v_1,\ldots,v_n)$ we have:

$$G_1 \models \psi(\theta_1^{-1}(\gamma_1),\ldots,\theta_1^{-1}(\gamma_n)) \leftrightarrow G_2 \models \psi(\theta_2^{-1}(\varphi(\gamma_1)),\ldots,\theta_2^{-1}(\varphi(\gamma_n))).$$

The following lemma will be useful later on. Its straightforward proof is left to the reader.

Lemma 31: Let θ_i, G_i, H_i $(i = 1,2)$ be as above, and let N be a collection of open normal subgroups of H_1 which is cofinal in the sense that each open normal subgroup of H_1 includes one from N. Then $(G_1,\theta_1) \overset{\circ}{\equiv}_\varphi (G_2,\theta_2)$ iff for all coformulas $\psi(v_1,\ldots,v_n)$, $N \in N$ and cosets $\gamma_1,\ldots,\gamma_n$ of N we have:

$$G_1 \models \psi(\theta_1^{-1}\gamma_1,\ldots,\theta_1^{-1}\gamma_n) \leftrightarrow G_2 \models \psi(\theta_2^{-1}\varphi\gamma_1,\ldots,\theta_2^{-1}\varphi\gamma_n) .$$

A regular embedding $f : K \to L$ of fields, together with an extension of f to an embedding $\tilde{K} \to \tilde{L}$ (also denoted by f) induces an epi $\hat{f} : G(L) \to G(K)$.

Two special cases we often deal with are:

(1) f is an isomorphism $\tilde{K} \cong \tilde{L}$ mapping K onto L. Then obviously $\hat{f}$ is an isomorphism of $G(L)$ onto $G(K)$.

(2) L is a regular extension of K, f is the inclusion $K \hookrightarrow L$; then we take for $\tilde{K}$ the algebraic closure of K inside $\tilde{L}$ and let f also stand for the inclusion $\tilde{K} \hookrightarrow \tilde{L}$. $\hat{f}$ is then the restriction $G(L) \to G(K)$.

For the next lemma, recall that K is a regular extension of $Abs(K)$.

Lemma 32: Suppose $K \equiv L$. Let i,j be the inclusions $Abs(K) \hookrightarrow K$ and $Abs(L) \hookrightarrow L$ inducing epis $\hat{i} : G(K) \to G(Abs(K))$ and $\hat{j} : G(L) \to G(Abs(L))$.

Then there is an isomorphism $f : \tilde{Abs}(L) \simeq \tilde{Abs}(K)$ mapping $Abs(L)$ onto $Abs(K)$ such that $(G(K),\hat{i}) \overset{o}{\equiv}_{\hat{f}} (G(L),\hat{j})$.

Proof: Take an isomorphism f^* of an elementary extension L^* of L onto an elementary extension K^* of K. Extend f^* to an isomorphism also denoted by f^*, of $\tilde{L}^*$ onto $\tilde{K}^*$. According to our convention above we take $\tilde{Abs}(L) \subset \tilde{L} \subset \tilde{L}^*$, and similarly for K. Let $f = f^* | \tilde{Abs}(L)$. Clearly f maps $\tilde{Abs}(L)$ onto $\tilde{Abs}(K)$ and $Abs(L)$ onto $Abs(K)$. We now have the commuting diagram

$$\begin{array}{ccc} G(K^*) & \xrightarrow[\hat{f}^*]{\sim} & G(L^*) \\ \downarrow & & \downarrow \\ G(K) & & G(L) \\ \hat{i}\downarrow & & \downarrow\hat{j} \\ G(AbsK) & \xrightarrow[\hat{f}]{\sim} & G(AbsL) \end{array}$$

where $G(K^*) \to G(K)$ and $G(L^*) \to G(L)$ are coelementary. The result is now immediate.

■

This lemma gives a necessary condition for elementary equivalence of two fields. It is remarkable that, modulo one obvious elementary invariant, this condition is also sufficient in the case of RC-fields. The one extra invariant we need is the degree of imperfectness (of K) which is defined as the supernatural number $[K:K^p] \in \{1,p,p^2,\ldots,p^\infty\}$ if $\mathrm{char}(K) = p > 0$ and as 1 if $\mathrm{char}(K) = 0$.

The following result generalizes to RC-fields Eršov's theorem [E1] that two separably closed fields are elementarily equivalent iff they have the same characteristic and the same degree of imperfectness.

Proposition 33: Suppose K,L are RC-fields. Let i,j be as in the previous lemma. Then $K \equiv L$ iff and only if K and L have the same degree of imperfectness and there is an isomorphism $f : \widetilde{Abs}(L) \xrightarrow{\sim} \widetilde{Abs}(K)$ mapping Abs(L) onto Abs(K) such that $(G(K),\hat{i}) \overset{0}{\equiv}_{\hat{f}} (G(L),\hat{j})$.

Proof: The previous lemma gives one direction. For the converse we assume that K and L have the same degree of imperfectness and that f has the stated property. We can assume without loss of generality that K,L are ω_1-saturated, and so that G(K) and G(L) are ω_1-cosaturated. We prove $K \equiv L$ by constructing a Karp morphism ("back and forth system") consisting of triples (g,M,N) with the following property (*):

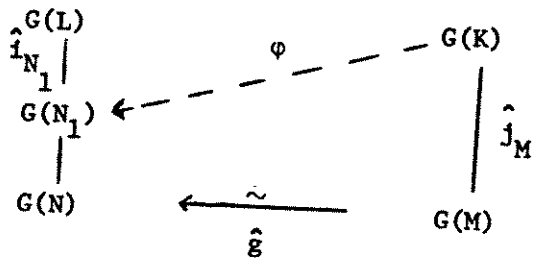
(*) K,L are regular extensions of their countable subfields M,N respectively and g is an isomorphism $\widetilde{N} \to \widetilde{M}$ mapping N onto M such that, with i_M, j_N the inclusions $M \hookrightarrow K$, $N \hookrightarrow L$:

$$(G(K),\hat{i}_M) \overset{0}{\equiv}_{\hat{g}} (G(L),\hat{j}_N) .$$

Note that (f, Abs(K), Abs(L)) satisfies (*).

To conclude the proof we need only show that if (g,M,N) satisfies (*) and A is a countable subset of L, then there is a triple (g_1,M_1,N_1) satisfying (*) with $M_1 \supset M$, $N_1 \supset N$, g_1 extending g and $A \subset N_1$.

For N_1 we take any countable elementary subfield of L containing N and A. Then $L|N_1$ is regular. Consider



By lemma 12 (or rather its proof) there is an epi $\varphi : G(K) \to G(N_1)$ making the diagram commute and such that for all coformulas $\Phi(v_1,\ldots,v_k)$ and open cosets $\gamma_1,\ldots,\gamma_k$ of $G(N_1)$:

(1) $$G(L) \models \Phi(\hat{i}_{N_1}^{-1}(\gamma_1),\ldots,\hat{i}_{N_1}^{-1}(\gamma_k)) \leftrightarrow G(K) \models \Phi(\varphi^{-1}\gamma_1,\ldots,\varphi^{-1}(\gamma_k))$$

Now we apply the generalized Embedding Lemma (lemma 30) and get an extension of g to an embedding $g_1 : \tilde{N}_1 \to \tilde{K}$ restricting to a regular embedding $N_1 \to K$, such that, putting $M_1 = g_1(N_1)$ we have: $\varphi = \hat{g}_1 \circ \hat{i}_{M_1}$.

Now it follows from (1) that (g_1,M_1,N_1) satisfies (*).

■

The following is similar, and we omit the proof.

Theorem 34: Suppose $K \subset L$, K and L are RC-fields.

Then $K \prec L$ if and only if

(i) L is a regular extension of K;

(ii) K and L have the same degree of imperfectness;

(iii) the restriction map $G(L) \to G(K)$ is coelementary.

The following special case seems particularly interesting. Denef pointed out that for perfect K and L it is concealed in Theorem 3.2 of [J-K].

Corollary 35: Suppose the RC-field L is a regular extension of the RC-field K and $\hat{i} : G(L) \to G(K)$ is an isomorphism. Then $K \prec L$ if and only if K and L have the same degree of imperfectness.

We know a short alternative proof of this bypassing the Embedding Lemma and using projectivity of $G(K)$ and $G(L)$, but will not give it here.

The existence of an isomorphism f as in proposition 33 is a global condition. We now prove it equivalent to a set of local conditions, more precisely we want elementary invariants such that if K and L agree on these invariants then an isomorphism f as in proposition 33 exists.

For that we need a slight elaboration of the interpretation of Galois theory in field theory of §1.

For each finite Galois extension of a prime field P we fix a monic irreducible polynomial $q(X) \in P[X]$ such that the extension is generated over P by a root of q (hence by any of its roots); we write this extension as P_q. Let $[P_q:P] = n$ $(= \deg q)$. We then fix a sequence of polynomials $r_1(X),\ldots,r_n(X)$, all of degree $< n$, in $P[X]$, such that $r_1(\delta),\ldots,r_n(\delta)$ are the n distinct roots of $q(X)$ in P_q, where δ is one of the roots of q. (This does not depend on the choice of δ.) In the following q and $r_1,\ldots,r_n$ will always be used in this sense.

Let K be any field $\supset P$. For a finite Galois extension F over K we identify, as usual the members of $G(F|K)$ with the cosets of $G(F)$ in $G(K)$. (Note that $G(F)$ is an open normal subgroup of $G(K)$). Here $\sigma\, G(F)$ is identified with $\sigma|F$ for $\sigma \in G(K)$.

Consider now the special case $F = K.P_q$. Given a root δ of $q(X)$ in $\tilde{K}$ we have $F = K(\delta)$ and a member σ of $G(F|K)$ is determined by the unique polynomial $r_i(X)$ such that $\sigma(\delta) = r_i(\delta)$. So we now have a 1-1 map from the cosets of $G(F)$ in $G(K)$ into $\{r_1,\ldots,r_n\}$: $\sigma\, G(F)$ corresponds to r_i where $\sigma(\delta) = r_i(\delta)$. (This correspondence depends on the choice of δ.) Now let $\Phi(v_1,\ldots,v_k)$ be any coformula and $\bar{r}$ be any finite sequence $(r_{i_1},\ldots,r_{i_k})$, $1 \le i_j \le n$. From these data we can construct a <u>sentence</u> $\Phi_q(\bar{r})$ in the language of fields such that for each field $K \supset P$ we have:

$$K \models \Phi_q(\bar{r}) \leftrightarrow$$

there is a root δ of $q(X)$ in $\tilde{K}$ such that $G(K) \models \Phi(N_1,\ldots,N_k)$, where $N_1,\ldots,N_k$ are the cosets of $G(K(\delta))$ in $G(K)$ corresponding to automorphisms $\sigma_1,\ldots,\sigma_k$ of $K(\delta)$ over K with $\sigma_1(\delta) = r_{i_1}(\delta),\ldots,\sigma_k(\delta) = r_{i_k}(\delta)$.

(Note that we can take $\Phi_q(\bar{r}) = \hat{\Phi}$ if $k = 0$.)

Now we can state and prove:

Lemma 36: Let $K \supset P$, $L \supset P$ and let i,j be the natural inclusions $Abs(K) \hookrightarrow K$, $Abs(L) \hookrightarrow L$. Then the following are equivalent:

(1) There is an isomorphism $f : \widetilde{Abs}(L) \cong \widetilde{Abs}(K)$ mapping $Abs(L)$ onto $Abs(K)$ such that $(G(K), \hat{i}) \overset{\circ}{\cong}_{f} (G(L), \hat{j})$.

(2) $K \models \Phi_q(\bar{r}) \Leftrightarrow L \models \Phi_q(\bar{r})$, for all Φ, q, $\bar{r}$ as above.

Proof: (1) $\Rightarrow$ (2) follows in a straightforward way from the definitions.

(2) $\Rightarrow$ (1): the construction of f comes from a projective limit argument. First some preliminaries.

The finite Galois extensions P_q of P occur both as subfields of $\widetilde{K}$ and of $\widetilde{L}$. To distinguish we write $P_{q,K}$ if P_q occurs in the first role and $P_{q,L}$ if it occurs in the second role. An isomorphism $\mu: P_{q,K} \cong P_{q,L}$ induces an isomorphism $\sigma \to \sigma^{\mu}$ of $G(P_{q,K}|P)$ onto $G(P_{q,L}|P)$ given by $\sigma^{\mu} = \mu\sigma\mu^{-1}$. If μ maps $K \cap P_{q,K}$ onto $L \cap P_{q,L}$, then $\sigma \to \sigma^{\mu}$ maps $G(P_{q,K}|P_{q,K} \cap K)$ onto $G(P_{q,L}|P_{q,L} \cap L)$. Now $G(K \cdot P_{q,K}|K) \cong G(P_{q,K}|P_{q,K} \cap K)$ by restriction, hence we obtain an isomorphism of $G(K \cdot P_{q,K}|K)$ onto $G(L \cdot P_{q,L}|L)$ which we also denote by $\sigma \to \sigma^{\mu}$.

After these preliminaries we can define for each finite Galois extension $P_q|P$: the (finite) set $M(q)$ consists of all automorphisms $\mu: P_{q,K} \overset{\sim}{\to} P_{q,L}$ mapping $P_{q,K} \cap K$ onto $P_{q,L} \cap L$ such that $G(K) \models \Phi(\gamma_1,\ldots,\gamma_k) \Leftrightarrow G(L) \models \Phi(\gamma_1^{\mu},\ldots,\gamma_k^{\mu})$ for all coformulas $\Phi(v_1,\ldots,v_k)$ and $\gamma_1,\ldots,\gamma_k \in G(K \cdot P_{q,K}|K)$. (Here the γ_i and γ_i^{μ} are identified as usual with open cosets in $G(K)$ and $G(L)$.) We order the q's by putting $q_1 \geq q_2$ if $P_{q_1} \supset P_{q_2}$ (inside $\widetilde{P}$). Then the q's are

directed upwards, and if $q_1 \geq q_2$, restriction defines a map $M(q_1) \to M(q_2)$. (This depends on a general comodel theoretic lemma, the formulation and proof of which we leave to the reader). So the $M(q)$'s form a projective system of finite sets, and if each $M(q) \neq \emptyset$, then $\lim_{\leftarrow} M(q) \neq \emptyset$. An element of $\lim_{\leftarrow} M(q)$ determines an isomorphism of $\widetilde{Abs}(K)$ onto $\widetilde{Abs}(L)$ sending $Abs(K)$ onto $Abs(L)$. Writing f for the inverse isomorphism it follows easily from lemma 31 that

$$(G(K), \hat{i}) \cong \hat{f}(G(L), \hat{j}) .$$

So we are reduced to showing $M(q) \neq \emptyset$, q given. For a coformula $\Phi = \Phi(v_1,\ldots,v_k)$ we let $M(q,\Phi)$ consist of all $\mu : P_{q,K} \xrightarrow{\sim} P_{q,L}$ mapping $P_{q,K} \cap K$ onto $P_{q,L} \cap L$ such that

$$G(K) \models \Phi(\gamma_1,\ldots,\gamma_k) \Leftrightarrow G(L) \models \Phi(\gamma_1^{\mu},\ldots,\gamma_k^{\mu})$$

for all $\gamma_1,\ldots,\gamma_k \in G(K\,P_{q,K}|K)$. So the intersection of all $M(q,\Phi)$ equals $M(q)$. Now each $M(q,\Phi)$ is finite, hence to show that $M(q) \neq \emptyset$ it suffices to show that $M(q, \Phi_1) \cap \ldots \cap M(q,\Phi_\ell) \neq \emptyset$ for any coformulas $\Phi_1,\ldots,\Phi_\ell$. Let $\Phi_i = \Phi_i(v_1,\ldots,v_k)$, $i = 1,\ldots,$. Let $r_1,\ldots,r_n$ be the sequence of polynomials associated to q, where $n = \deg q = [P_q : P]$. Fix a root δ of $q(X)$ in $\widetilde{K}$. Suppose $[K(\delta):K] = m \leq n$, and write $\sigma_1,\ldots,\sigma_m$ for the m distinct automorphisms of $K(\delta)$ over K. For simplicity of notation we assume $\sigma_1(\delta) = r_1(\delta),\ldots,\sigma_m(\delta) = r_m(\delta)$. (In general we have $\sigma_1(\delta) = r_{i_1}(\delta),\ldots,\sigma_m(\delta) = r_{i_m}(\delta)$, but this would force us leter on into awkward subsubindices.) Construct a coformula $\psi(v_1,\ldots,v_m)$ such that for each G: $G \models \psi(\gamma_1,\ldots,\gamma_m) \Leftrightarrow \gamma_1,\ldots,\gamma_m$ are the m cosets of an open normal subgroup of index m in G. Hence we have $G(K) \models \psi(\sigma_1,\ldots,\sigma_m)$.

Let I be the set of all sequences $i = (i_1,\ldots,i_k)$ with $1 \le i_1 \le m,\ldots,1 \le i_k \le m$, and for $1 \le j \le \ell$ let $A(j)$, be the set of all $i = (i_1,\ldots,i_k) \in I$ with $G(K) \models \Phi_j(\sigma_{i_1},\ldots,\sigma_{i_k})$, and let $B(j) = I \backslash A(j)$. Then we define the coformula $\Phi^*(v_1,\ldots,v_m)$ as the conjunction of $\psi(v_1,\ldots,v_m)$ with the ℓ coformulas

$$\bigwedge_{i\in A(j)} \Phi_j(v_{i_1},\ldots,v_{i_k}) \wedge \bigwedge_{i\in B(j)} \neg\Phi_j(v_{i_1},\ldots,v_{i_k}) \ , \ j = 1,\ldots,\ell \ .$$

Then $G(K) \models \Phi^*(\sigma_1,\ldots,\sigma_m)$, by construction of Φ^*, hence $K \models \Phi_q^*(r_1,\ldots,r_m)$ by definition. The hypothesis (2) of the lemma implies that $L \models \Phi_q^*(r_1,\ldots,r_m)$. By definition of $\Phi_q^*(r_1,\ldots,r_m)$ this gives the existence of a root ε of $q(X)$ in $\tilde{L}$ such that:

(a) $L(\varepsilon)$ has exactly m automorphisms $\tau_1,\ldots,\tau_m$ over L given by $\tau_1(\varepsilon) = r_1(\varepsilon),\ldots,\tau_m(\varepsilon) = r_m(\varepsilon)$. (This comes from ψ .)

(b) $G(L) \models \Phi_j(\tau_{i_1},\ldots,\tau_{i_k})$ for all $j = 1,\ldots,\ell$ and $i = (i_1,\ldots,i_k) \in A(j)$, and $G(L) \models \neg\Phi_j(\tau_{i_1},\ldots,\tau_{i_k})$ for all $j = 1,\ldots,\ell$ and $i = (i_1,\ldots,i_k) \in B(j)$.

Define $\mu: P_{q,K} \xrightarrow{\sim} P_{q,L}$ by $\mu(\delta) = \varepsilon$. From (a) we get $\mu(P_{q,K} \cap K) = P_{q,L} \cap L$ and $\tau_i = \sigma_i^{\mu}$. Together with (b) this implies $\mu \in M(q,\Phi_1) \cap \ldots \cap M(q,\Phi_\ell)$, and the nonemptiness of the last set was what we were out to prove. ∎

The following corollary gives a complete list of elementary invariants for RC-fields.

Corollary 37: Let K, L be two RC-fields. Then $K \equiv L$ iff:

(a) K and L have the same characteristic (say with prime field P);

(b) K and L have the same degree of imperfectness;

(c) K and L satisfy the same sentences $\Phi_q(\bar{r})$, where $\Phi = \Phi(v_1,\ldots,v_k)$ ranges over the coformulas, q (with associated sequence $r_1,\ldots,r_n$) over the polynomials in P[X] defining the finite Galois extensions of P, and $\bar{r}$ over the finite sequences $(r_{i_1},\ldots,r_{i_k})$.

Proof: Combine Proposition 33 and the previous lemma. ∎

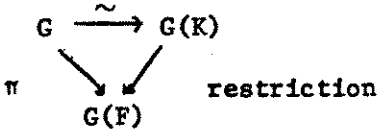
Clearly condition (c) is the most significant one. It is quite possible that (c) in its present formulation is not optimal. In the next section we give an improvement for Iwasawa RC-fields. In §6 we give a similar improvement for RC-fields with small absolute Galois group.

(3.5) Galois theoretic constraints on RC-field extensions

Corollary 37 says roughly that the elementary theory of an RC-field K is completely determined by the characteristic of K, its degree of imperfectness and the cotheory of $G(K)$ with suitably distinguished image $G(Abs(K))$.

Therefore it is natural to consider the following problem. *Let F be a field algebraic over its prime field, G a profinite group and $\pi: G \to G(F)$ an epi.*

When does there exist an RC-field extension K of F with $Abs(K) = F$ and an isomorphism $G \xrightarrow{\sim} G(K)$ such that the diagram



commutes?

The answer is given in the following proposition, which improves a result in [Lu-vdD].

Proposition 38: *An RC-field extension K as required exists if and only if G is projective. In that case K can be taken to have any degree of imperfectness compatible with char(F).*

Remark. Compatibility with char(F) means of course that if $char(F) = 0$, then the degree of imperfectness of K is 1, while if $char(F) = p > 0$, then K can have any degree of imperfectness p^n, $n = 0,1,2,\ldots,\infty$.

First a lemma.

Lemma 39: There exists a countable RC-field extension L of F such that $Abs(L) = F$ and $G(L) \cong \hat{F}_\omega$. L can be taken to have any degree of imperfectness compatible with $char(F)$.

Proof: Take a purely transcendental extension F' of F of transcendence degree $\aleph_0$. So F' is a countable hilbertian field. Therefore we have, by [J1], [J2], for each $e \in \mathbb{N}$: Fix $(\sigma_1,\ldots,\sigma_e)$ is an e-free RC-field for almost all $(\sigma_1,\ldots,\sigma_e) \in G_s(F')^e$. In particular, given any finite Galois extension $F(\delta)|F$ and any $e \geq \mathrm{rk}\ G(F(\delta)|F)$ we can take $\sigma_1,\ldots,\sigma_e$ in $G_s(F')$ such that Fix $(\sigma_1,\ldots,\sigma_e)$ is e-free and RC, and the $\sigma_i|F(\delta)$ generate $G(F(\delta)|F)$. Note that then $\mathrm{Fix}(\sigma_1,\ldots,\sigma_e)$ is linearly disjoint from $F(\delta)$ over F and, as a separable extension of F', has degree of imperfectness p^∞, if $\mathrm{char}(F) = p > 0$.

Now $G(\mathrm{Fix}(\sigma_1,\ldots,\sigma_e)) \cong \hat{F}_e$, $\mathrm{Im}(\hat{F}_e)$ = all finite groups of rank $\leq e$, and $\hat{F}_e$ has IP, see [J-K].

Therefore the compactness theorem, followed by an application of the downward Skolem-Lowenheim theorem, gives the existence of a countable RC-field extension L of F such that:

(1) L is linearly disjoint over F from each finite Galois extension of F;

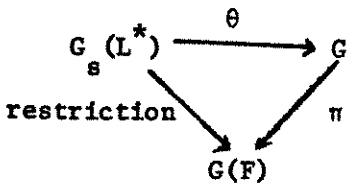
(2) $\mathrm{Im}(G(L))$ = all finite groups, $G(L)$ has IP;

(3) L has degree of imperfectness p^∞, if $\mathrm{char}(F) = p > 0$.

Now (1) implies that $\mathrm{Abs}(L) = F$, (2) gives that $G(L) \cong \hat{F}_\omega$, by Corollary 24, and (3) implies that replacing L by a suitable purely inseparable extension, we get an RC-field of the right degree of imperfectness, without changing $\mathrm{Abs}(L)$ or $G(L)$.

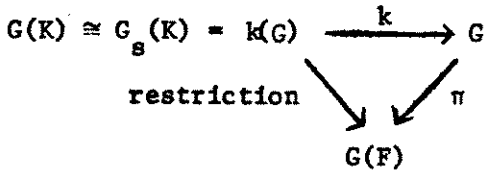
■

Proof of Proposition 38: That $G(K)$ is projective if K is RC, goes back to Ax and Gruenberg, see [Lu-vdD, p. 44]. Suppose now that G is projective. Take a field L as in the previous lemma. Let κ be an infinite cardinal such that G has cocardinality $<\kappa$. Take a κ-saturated elementary extension L^* of L. $G_s(L^*)(\cong G(L^*))$ is then κ-cosaturated and $\mathrm{Coth}(G_s(L^*)) = \mathrm{Coth}(\hat{F}_\omega)$. Using Theorem 13A it follows that there exists an epi $G_s(L^*) \to G$. Now $G_s(L^*)$ has IP_κ by lemma 26, so there is even an epi $\theta : G_s(L^*) \to G$ such that



commutes. As G is projective, there exists $k : G \to G_s(L^*)$ splitting θ. Let $K \subset L_s^*$ be the fixed field of $k(G)$.

Then we have a commuting diagram



We still have that $\mathrm{Abs}(K) = F$, since the restriction map $G_s(L^*) \to G(F)$ maps $G_s(K)$ onto $G(F)$. Finally, $K|L^*$ is separable algebraic, hence has the same degree of imperfectness as L.

■

§4. The case of Iwasawa RC-fields

(4.1) The classification of Iwasawa RC-fields turns out to be easier and more satisfactory then the general case. Recall that an Iwasawa field is a field whose absolute Galois group has IP, see (2.10).

Theorem 40. Let K, L be Iwasawa RC-fields. Then $K \equiv L$ if and only if

(i) $\mathrm{Abs}(K) \cong \mathrm{Abs}(L)$,

(ii) K and L have the same degree of imperfectness.

(iii) $\mathrm{Im}\ (G(K)) = \mathrm{Im}(G(L))$.

Note: This theorem, for perfect K and L, was obtained independently and by different methods, by Fried-Haran-Jarden [F-H-J], who write Frobenius for Iwasawa. There is also overlap with results announced by Ersov in [E2] and elaborated in [E3].

Proof: Necessity is clear.

Sufficiently. We shall apply proposition 33. Without loss of generality, assume that K and L are $\aleph_1$-saturated; so G(K) and G(L) have $\mathrm{IP}_{\aleph_1}$, by lemmas 18 and 26. Take any isomorphism $f : \tilde{\mathrm{Abs}}(L) \cong \tilde{\mathrm{Abs}}(K)$ mapping Abs(L) onto Abs(K), and consider the diagram

$$\begin{array}{ccc} G(K) & & G(L) \\ {\scriptstyle \hat{i}}\downarrow & & \downarrow{\scriptstyle \hat{j}} \\ G(\mathrm{Abs}(K)) & \xrightarrow[\hat{f}]{\sim} & G(\mathrm{Abs}(L)) \end{array}$$

Use (iii) and apply Lemma 26(b) to get $(G(K), \hat{i}) \overset{b}{\equiv} \hat{f}(G(L), \hat{j})$. Now use (ii) and apply proposition 33 to get $K \equiv L$.

■

Note that proposition 38 takes care of constraints between the elementary invariants.

(4.2) Quantifier elimination and model completeness for Iwasawa RC-fields

We have a very satisfactory quantifier elimination for perfect Iwasawa RC-fields, in a language which we will call the "Galois formalism". For imperfect Iwasawa RC-fields we only have a model completeness result.

Definition: The Galois formalism is the language of rings $\{0,1,+,.,-\}$ expanded by an n-ary predicate S_n, for each $n \geq 2$, and a 0-place predicate I_G, for each isomorphism type G of finite groups.

Definition: pIRC is the theory of perfect Iwasawa RC-fields in the Galais formalism, where the new predicates are defined as follows: a perfect Iwasawa RC-field K has the unique expansion K to a model of pIRC by putting: $K \models S_n(c_1,\ldots,c_n) \longleftrightarrow \exists x(x^n + c_1x^{n-1} + \ldots + c_n = 0)$, and $K \models I_G \leftrightarrow K$ has a Galois extension L with $G(L|K)$ of isomorphism type G.

So if $K \subset L$ and K, L have expansions K, L to models of pIRC, then $K \subset L$ if and only if K is algebraically closed in L and $Im(G(K)) = Im(G(L))$.

Theorem 41. pIRC admits quantifier elimination.

Proof: By Shoenfield's criterion [Sh] it suffices to prove the following: Suppose $f : L \cong M$ is an isomorphism between countable fields and L, M are relatively algebraically closed in extension fields E, F respectively, which are perfect Iwasawa RC and such that $ImG(E) = ImG(F)$, E is countable and F is $\aleph_1$-saturated. Then f extends to an isomorphism of E onto a relatively algebraically closed subfield of F. ∎

To prove this we involve the embedding lemma, and as we are in the perfect case the Jarden-Kiehne version suffices here. We first extend f to an isomorphism, also denoted f, on $\tilde{L}$ onto $\tilde{M}$, so we have a diagram

$$\begin{array}{ccc} G(E) & & G(F) \\ \downarrow & \overset{\hat{f}}{\underset{\sim}{\longleftarrow}} & \downarrow \\ G(L) & & G(M) \end{array}$$

According to the embedding lemma we only have to find an epi $G(F) \to G(E)$ which makes the diagram commutative. There certainly is an epi $G(F) \to G(E)$, because $G(F)$ is $\aleph_1$-couniversal, (lemmas 18 and Theorem 13A) and $G(E)$ is cocountable and $G(E) \equiv G(F)$ (corollary 25). Since $G(F)$ has $IP_{\aleph_1}$ (lemma 26), we may conclude that an epi as required exists. ∎

We now extend the Galois formalism by m-ary predicates $Q_{m,p}$ ($m \geq 1$, p a prime) and let IRC be the theory of Iwasawa RC-fields in this extended Galois formalism with the same defining axioms for the S_n and I_G as before and with $K \models Q_{m,p}(c_1,\ldots,c_m)$ ⇔ the underlying field K of K is characteristic p and $c_1,\ldots,c_m$ are p-independent in K. For $m \in \{1,2,\ldots\} \cup \{\infty\}$ and p a prime we let

$IRC_{m,p} = IRC \cup \{\exists x_1,\ldots,x_m Q_{m,p}(x_1,\ldots,x_m) \wedge \neg(\exists x_1,\ldots,x_m,x_{m+1} Q_{m+1,p}(x_1,\ldots,x_{m+1}))\}$ if m is finite, $IRC_{\infty,p} = IRC \cup \{\exists x_1,\ldots,x_k\, Q_{k,p}(x_1,\ldots,x_k) \mid k = 1,2,\ldots\}$. So $IRC_{m,p}$ is the theory of Iwasawa RC-fields with degree of imperfectness p^m. We now generalize Ersov's model completeness theorem for separably closed fields in [E1].

Proposition 42. $IRC_{m,p}$ is model complete.

Proof: Suppose K and L are models of $IRC_{m,p}$ with underlying fields K, L. Then $K \subset L$ means that L is a regular extension of K, K and L have the same degree of imperfectness, and $ImG(K) = ImG(L)$. Then $K \prec L$ follows immediately from theorem 34 and a minor extension of Corollary 25.

■

Remark. Wood indicated in [Wo] a 'weak' theory $T_{m,p}$ which has as model completion the theory $\bar{T}_{m,p}$ of separably closed fields of degree of imperfectness p^m (in the language of rings with the $Q_{m,p}$'s and the above defining axioms). But $T_{m,p}$ is not universal, and, stronger even, $\bar{T}_{m,p}$ does not admit quantifier elimination. Therefore, neither does $IRC_{m,p}$.

(4.3) A reduction of the decision problem for Iwasawa RC-fields

Theorem 43. The decision problem for the theory of Iwasawa RC-fields is Turing-reducible to the problem of deciding, for any given finite groups $A_1,\ldots,A_m$, $B_1,\ldots,B_n$, whether there is a projective G with IP such that $A_i \in Im(G)$ for $i = 1,\ldots,m$, $B_j \notin Im(G)$ for $j = 1,\ldots,n$.

Remarks. (1) We did not solve the decision problem for finite groups mentioned in the theorem. However, Lubotzky and Haran recently did, see [L-H]. Hence the theory of Iwasawa RC-fields is decidable.

(2) In the proof of the theorem we shall freely use that one can effectively carry out certain algorithms in, and effectively decide certain questions on, finite extensions of prime fields. This kind of effective algebra is by now well established, and the reader will find enough detail in [vd W, p. 79], [Ra, p. 352], [vdD, fact 4].

Proof of the theorem: As the theory of Iwasawa RC-fields is recursively axiomatized, its set LC of logical consequences is recursively enumerable (r.e. for short). So it suffices to show that the set $\overline{LC}$ of sentences which are not true in some Iwasawa RC-field is r.e. relative to the decision problem for finite groups mentioned in the theorem. We shall do this by means of the elementary invariants provided by theorem 40.

Take a sentence $\phi \in \overline{LC}$, so there is an Iwasawa RC-field K with $K \models \neg\phi$. Now, by theorem 40, the complete theory Th(K) is axiomatized by the sentences saying what the characteristic and degree of imperfectness of K are, which monic polynomials in $Z[T]$ have and which do not have a root in K, and which finite groups do, and which do not occur as Galois groups over K. (Of course, the last part only refers to the isomorphism types of the finite groups.)

So $\phi \in \overline{LC}$ means that ϕ is a logical consequences of a finite subset of such an axiomatization. Roughly then, to obtain the relative r.e. ness of $\overline{LC}$, we need only decide, relative to the finite groups problem, whether a given finite set of sentences of a special kind, is true in some Iwasawa RC-field. More precisely:

Let a finite Galois extension P_q of a prime field P be given (meaning: the characteristic p of P and the defining polynomial q(X) of P_q are given, see (3.4)). Let also a subfield F of P_q be specified, say by a polynomial $r(X) \in P[X]$ with $F = P(r(\delta))$, δ a root of q(X). (Of course, r(X) determines F only up to isomorphism inside P_q, but that is good enough, we note that one can determine effectively $G(P_q|F)$ as a permutation group on

the roots of $q(x)$.) Let also a supernatural number d be given, where $d = 1$ if $p = 0$, and $d \in \{1, p, p^2, \ldots, p^\infty\}$ if $p > 0$. Finally, let finite groups $A_1, \ldots, A_m$, $B_1, \ldots, B_n$ be given.

We want to decide, relative to the decision problem for finite groups mentioned in the theorem, whether there is an Iwasawa RC-field $K \supset P$ with $K \cap P_{q,K} = F$, which has degree of imperfectness d and $A_i \in \mathrm{Im}(G(K))$ for $i = 1, \ldots, m$, $B_j \notin \mathrm{Im}(G(K))$ for $j = 1, \ldots, n$.

The following claim clearly provides such a relativized decision method.

Claim. Such a K exists if and only if there is projective G with IP and with $G(P_q|F) \in \mathrm{Im}(G)$, $A_i \in \mathrm{Im}(G)$ for $i = 1, \ldots, m$, and $B_j \notin \mathrm{Im}(G)$ for $j = 1, \ldots, n$.

One direction is obvious: if such a K exists, then $G = G(K)$ has the required properties. Conversely, let G be projective with IP and

× $G(P_q|F) \in \mathrm{Im}(G)$, $A_i \in \mathrm{Im}(G)$ for $i = 1, \ldots, m$ and $B_j \notin \mathrm{Im}(G)$ for $j = 1, \ldots, n$.

We now use an argument similar to the proof of proposition 38: take an infinite cardinal κ such that G has cocardinality $< \kappa$ and take an RC-field $L^* \supset P$ with $\mathrm{Abs}(L^*) = F$, such that L^* has degree of imperfectness d, and $G(L^*)$ is κ-cosaturated and has the same cotheory as $\hat{F}_\omega$. Now we may consider P_q as a subfield of L_s^*, which gives us a surjective restriction map $G_s(L^*) \to G(P_q|F)$. By the assumptions on G there is also an epi $\pi: G \to G(P_q|F)$. Proceeding as in the proof of proposition 38 we get an epi $\theta: G_s(L^*) \to G$ such that $\pi\theta =$ restriction : $G_s(L^*) \to G(P_q|F)$. As G is projective, there is a

splitting $k : G \to G_s(L^*)$ of θ. Taking $K \subset L_s^*$ as the fixed field of $k(G)$, the usual arguments show that $K \cap P_q = F$, K is RC, K has degree of imperfectness d, and $G(K) \cong G$. So K satisfies all requirements.

(4.4) The preceding results, together with some work of Melnikov [M], give the following outlandish:

Example: There is an undecidable field K such that all proper finite extensions L of K are isomorphic, and decidable.

Construction: Let f be a nonrecursive function from the set of finite simple nonabelian groups to ω. By Melnikov, there is a closed normal subgroup N of $\hat{F}_\omega$ such that for any S $f(S)$ is the largest k such that S^k is a continuous image of N. By interpretability, any field K with $G(K) \cong N$ is undecidable.

Let K_0 be any RC-field with $G(K_0) \cong \hat{F}_\omega$, and $Abs(K_0) \cong \tilde{Q}$. Any extension L of K_0 has $Abs(L) \cong \tilde{Q}$. Let K be the algebraic extension of K_0 with $G(K) \cong N$. Then K is undecidable.

By [M], if M is a proper open subgroup of N, $M \cong \hat{F}_\omega$. Suppose L is the fixed field of M. Then L is RC, $G(L) \cong \hat{F}_\omega$, and $Abs(L) \cong$ So by Theorem 40, and L is decidable!

Finally, to make all these L isomorphic, we should choose K more carefully. Replace K by a countable recursively saturated $K^* \equiv K$, and one easily proves that all proper finite extensions of K^* are isomorphic and decidable.

■

§5. Projective Covers

(5.1) The material in this section is essential for the decidability and undecidability results of Sections 6, 7. It seems to us interesting beyond our present setting.

We developed (as did Ersov independently in [E-F]) some properties of projective covers of profinite groups. After the appearance of [Ch-vdD-M] Tony Hager pointed out to us that the basic existence and uniqueness (of projective covers of profinite groups) is due to Banaschewski [B]. As our proofs turned out to the simpler than those in [B] and [E-F] we give here a new and selfcontained treatment. Subsections (5.1) and (5.2) are sufficient for the undecidability result of §7, subsection (5.3) is included for its own interest, and subsection (5.4) is only needed for the decidability result in §6.

Definition: An essential epi is $\phi: G \to H$ such that there is no proper closed subgroup G_0 of G with $\phi(G_0) = H$.

Lemma 45: Suppose $\phi: G \to H$ is an essential epi and $\psi: \Gamma \to H$ is an epi with Γ projective. Then there is an epi $\gamma: \Gamma \to G$ with $\psi = \phi\gamma$.

Proof: Each $\gamma: \Gamma \to G$ such that $\psi = \phi\gamma$ is obviously surjective. ∎

Definition: A projective cover of H is an essential epi $G \to H$ such that G is projective.

If $G \to H$ is a projective cover of H we often write $P(H)$ for G and also call $P(H)$ the projective cover of H. This is justified by the following.

Lemma 46: (Banaschewski) Every profinite group H has a projective cover unique up to isomorphism.

Proof: Let F be a free profinite group and $\phi: F \to H$ an epi. By Zorn's lemma there is a minimal closed subgroup P of F such that $\phi(P) = H$. Now P is projective by [G], hence $\phi|P : P \to H$ is a projective cover.

Suppose $\phi_1 : P_1 \to H$ and $\phi_2 : P_2 \to H$ are projective covers of H. By the previous lemma there is an epi $\pi: P_1 \to P_2$ such that $\phi_2\pi = \phi_1$. Because P_2 is projective, π has a splitting $\theta : P_2 \to P_1$, i.e. $\pi\theta = 1_{P_2}$. Then $\phi_1\theta = \phi_2\pi\theta = \phi_2$, so $\phi_1(\theta(P_2)) = \phi_2(P_2) = H$, so $\theta(P_2) = P_1$ because ϕ_1 is an essential epi. Hence $\theta : P_2 \to P_1$ is an isomorphism such that $\phi_1\theta = \phi_2$.

■

(5.2) More Specific Results

Lemma 47: $rk(P(H)) = rk(H)$.

Proof: Clearly, $rk(H) \leq rk(P(H))$. If $\phi: P(H) \to H$ is a projective cover, and X generates H topologically, then there is a subset Y of $P(H)$ which ϕ maps 1-1 onto X. Y generates topologically a closed subgroup of $P(H)$ which ϕ maps onto H, and by minimality this closed subgroup must equal $P(H)$. Hence $rk(P(H)) \leq rk(H)$.

■

The next lemma leads to a decidability result.

Lemma 48: A finite group Γ is in $Im(P(H))$ iff there is a Δ in $Im(H)$ and an essential epi $\Gamma \to \Delta$.

Proof: Sufficiency: Suppose Δ is in $Im(H)$ and $\Gamma \to \Delta$ is an essential epi. Because $P(H)$ is projective there is $\theta: P(H) \to P(\Gamma)$ making the diagram

$$\begin{array}{ccc} P(H) & \xrightarrow{\theta} & P(\Gamma) \\ \downarrow & & \downarrow \pi \\ H & \longrightarrow & \Gamma \end{array} \qquad (\pi : P(\Gamma) \to \Gamma \text{ the projective cover of } \Gamma)$$

commutative. $\pi\theta(P(H))$ must be all of Γ . (Otherwise it maps onto a proper subgroup of Γ, contradiction.) Hence $\Gamma \in Im(P(H))$.

Necessity: Suppose $\phi: P(H) \to \Gamma$ is an epi, Γ a finite group. Let $p : P(H) \to H$ be the projective cover of H, so $p(\ker(\phi))$ is a closed normal subgroup of H, hence p induces a commutative diagram

$$\begin{array}{ccc} P(H) & \xrightarrow{\phi} & \Gamma \\ p \downarrow & & \downarrow \theta \\ H & \xrightarrow{\text{natural}} & H/p(\ker\theta) = \Delta \end{array} \qquad (\theta \text{ is an epi.})$$

We need only show that θ is an essential epi (take $\Delta = H/p(\ker\phi)$). Let Γ_1 be any subgroup of Γ with $\theta(\Gamma_1) = \Delta$. We first show that $\ker\phi.\phi^{-1}(\Gamma_1) = P(H)$.

Let $h \in H$, so $h \bmod p(\ker\phi) = \theta\phi(x)$ for some $x \in \phi^{-1}(\Gamma_1)$, .i.e. $h \bmod p(\ker\phi) = p(x) \bmod p(\ker\phi)$, so $h \in p(\ker\phi.\phi^{-1}(\Gamma_1))$, and we have

proved that $p(\ker\phi.\phi^{-1}(\Gamma_1)) = H$. As p is essential this gives $\ker\phi\ .\phi^{-1}(\Gamma_1) = P(H)$. Applying ϕ to this gives $\Gamma_1 = \Gamma$.

■

(5.3) Applications and examples

The first application combines projective covers and smallness.

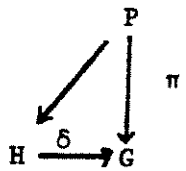
Corollary 49: Suppose G is a finitely generated profinite group with projective cover $\pi: P \to G$. Then each epi $P \to G$ is a projective cover of G.

Proof: Given an epi $p : P \to G$ there is by lemma 45 an epi $\gamma: P \to P$ with $p = \pi\gamma$. By lemma 47, P is finitely generated, hence small, therefore γ is an isomorphism, cf. (2.10).

■

The next result is somewhat stronger.

Corollary 50: Suppose G is finitely generated and has projective cover $\pi : P \to G$. Let $\delta: H \to G$ be an epi. Then each epi $P \to H$ is a projective cover of H, and if there is such an epi, there is one which makes the diagram



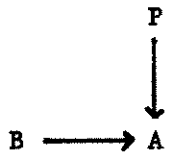
commutative.

Proof: Let $p : P \to H$ be any epi. Then $\delta p : P \to G$ is an epi, hence a projective cover by the previous corollary. So there is an automorphism of P such that $\delta p\mu = \pi$. Then $p\mu$ completes the diagram above. Moreover, as δp is a projective cover, p must be an essential epi, so p is a projective cover of H.

■

Projective covers of finite groups satisfy a weak form of the Iwasawa property:

Corollary 51: Let G be a finite group with projective cover P. Then each diagram



where both maps are epi's, $B \in \mathrm{Im}(P)$ and $G \in \mathrm{Im}(A)$, can be completed by an epi $P \to B$ to a commuting diagram.

Proof: Note that $G \in \mathrm{Im}(A)$ implies, by the previous corollary, that the epi $P \to A$ is a projective cover. Now apply again corollary 50.

■

Corollary 52: The projective cover of a finite simple group has IP.

Proof: Let P be the projective cover of a finite simple group S. Lemma 48 implies that for each $A \in \mathrm{Im}(P)$ we have either $A = 1$ or $S \in \mathrm{Im}(A)$. Now apply the previous corollary.

■

Remark. In [L-H] this last result has been generalized to: the projective cover of a f.g. G with IP has IP.

The following result is related to the decision procedure in §6.

Corollary 53: There is an algorithm which, given any finite groups $A_1,\ldots,A_m$, $B_1,\ldots,B_n$, decides whether there is a projective profinite group P such that $A_i \in \mathrm{Im}(P)$ for $i = 1,\ldots,m$ and $B_j \notin \mathrm{Im}(P)$ for $j = 1,\ldots,n$.

Proof: Let G be any profinite group. Then epis $G \to A_i$, $i = 1,\ldots,m$, induced a morphism $G \to A_1 x \ldots x A_m$ with image of a subgroup A of $A_1 x \ldots x A_m$ which is mapped onto A_i by each projection $A_1 x \ldots x A_m \to A_i$. Now, given finite groups $A_1,\ldots,A_m$, we list the (finitely many) subgroups A of $A_1 x \ldots x A_m$ which are mapped onto A_i by each projection $A_1 x \ldots x A_m \to A_i$. Clearly, for any G we have $A_1,\ldots,A_m \in \mathrm{Im}(G)$ if and only if there is such a subgroup A with $A \in \mathrm{Im}(G)$. This reduces our decision problem to the case $m = 1$.

So let finite groups $A, B_1,\ldots,B_n$ be given. If there is a projective profinite group P with $A \in \mathrm{Im}(P)$, $B_j \notin \mathrm{Im}(P)$ for $j = 1,\ldots,n$, then, because an epi $P \to A$ factors as $P \to P(A) \to A$ (both maps being epis, $P(A) \to A$ a projective cover), we must have $B_j \notin \mathrm{Im}(P(A))$, $j = 1,\ldots,n$. So a necessary and sufficient condition for the existence of such a P is that $B_j \notin \mathrm{Im}(P(A))$, $j = 1,\ldots,n$, which, according to lemma 48, is equivalent to: there is no $\Delta \in \mathrm{Im}(A)$ with an essential epi onto any B_j. Whether this last condition holds, can obviously be verified in a finite number of steps.

■

Corollary 54: If P is the projective cover of G, then the primes dividing the supernatural order of P are exactly those which divide the supernatural order of G.

Proof: Let $\mathfrak{X}$ be the class of finite groups with orders divisible only by primes dividing the supernatural order of G. So G is a pro-$\mathfrak{X}$-group, and there is an epi from $\mathfrak{X}$-projective group onto G, see [G, p. 158]. But each $\mathfrak{X}$-projective group is projective, by [G, Theorem 1]. Hence the projective cover of G is a pro-$\mathfrak{X}$- group.

■

Example: the projective cover of a finitely generated pro-nilpotent group.

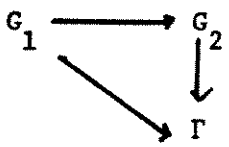
Let G be a pro-nilpotent group of rank e, so $G = \prod_{p\in I} G_p$, where I is the set of primes dividing the supernatural order of G, and G_p is the p-Sylow subgroup of G. Let $rk(G_p) = e_p$, so $1 \le e_p \le e$. Take for such $p \in I$ an epi $\hat{F}_p(e_p) \to G_p$, where $\hat{F}_p(e_p)$ is the free pro-p group on e_p generators. We claim that the induced map $\prod_{p\in I} \hat{F}_p(e_p) \to \prod_{p\in I} G_p = G$ is a projective cover of G.

Notice first that by the corollary above and lemma 45 the projective cover of G_p is a pro-p group of rank e_p, hence isomorphic to $\hat{F}_p(e_p)$ (because projective pro-p groups are free pro-p groups, cf. [G]). By corollary 40 it follows that each epi $\hat{F}_p(e_p) \to G_p$ is a projective cover. By Galois cohomology $\prod_{p\in I} \hat{F}_p(e_p)$ is of cohomological dimension 1, hance projective, by [G], and it is easy to see that the map $\prod_{p\in I} \hat{F}_p(e_p) \to G$ is essential. Our claim is proved.

(5.4) Relativized profinite groups

For our decision method in Section 6 we need a generalization of the algorithm of corollary 53. The best way to state this generalization is to consider profinite groups over a fixed profinite group.

Fix a profinite group Γ. A profinite group over Γ is by definition an epi $G \to \Gamma$ where G is profinite. The profinite groups over Γ form a category: a morphism of $G_1 \to \Gamma$ into $G_2 \to \Gamma$ is determined by a morphism $G_1 \to G_2$ such that the diagram



commutes.

(It follows that such a morphism is an epi in the category of profinite groups over Γ if and only if $G_1 \to G_2$ is an epi.) For simplicity of notation, let us write $\widetilde{G}$ for a profinite group over Γ of the form $G \to \Gamma$.

We define an essential epi $G_1 \to G_2$ to be an epi $G_1 \to G_2$ such that there is no proper closed subgroup H of G_1 such that the composition $H \to G_1 \to G_2$ is an epi.

A projective cover of $\widetilde{G}$ is by definition a projective object P in the category of profinite groups over Γ, together with an essential epi $\widetilde{P} \to \widetilde{G}$.

It is easy to show that each $\widetilde{G} = (G \to F)$ has a projective cover: take any projective cover $\pi: P \to G$ of G and let $\widetilde{P}$ be the composition $P \xrightarrow{\pi} G \to F$. Then P, together with the morphism $\widetilde{P} \xrightarrow{\pi} \widetilde{G}$ is a projective cover of $\widetilde{G}$.

Moreover, if $\widetilde{P}_1 \xrightarrow{\pi_1} \widetilde{G}$ and $P_2 \xrightarrow{\pi_2} \widetilde{G}_2$ are two projective covers of $\widetilde{G}$, then there is an isomorphism $\theta: \widetilde{P}_2 \xrightarrow{\sim} \widetilde{P}_1$ such that $\pi_1\theta = \pi_2$. (Uniqueness, same proof as in (5.1).)

Suppose now that Γ is finite. Call $\widetilde{H} = (H \to \Gamma)$ finite if H is finite and define $\mathrm{Im}(\widetilde{G})$ = the class of all finite $\widetilde{H}$ for which there exists an epi $\widetilde{G} \to \widetilde{H}$.

The analogue of lemma 48 holds, and is proved in the same way.

Lemma 55: Let Γ be finite, and $P(\mathcal{G})$ projective cover of $\mathcal{G}$. Then a finite $\mathcal{H}$ belongs to $\mathrm{Im}(P(\mathcal{G}))$ if and only if there is $\mathcal{A} \in \mathrm{Im}(\mathcal{G})$ and an essential epi $\mathcal{H} \to \mathcal{A}$.

Corollary 56. There is an algorithm which, given any $e \in \mathbb{N}$, any finite group Γ and any finite groups $A_1,\ldots,A_m$, $B_1,\ldots,B_n$ over Γ, decides whether there is a projective profinite group $\tilde{P} = (P \to \Gamma)$ over Γ with $rk(P) \leq e$, such that $\tilde{A}_i \in Im(\tilde{P})$ for $i = 1,\ldots,m$, $B_j \notin Im(\tilde{P})$ for $j = 1,\ldots,n$.

The proof is similar to the proof of corollary 53. The algorithm above is crucial for the decision procedure in the next section.

§6

DECIDABILITY

(6.1) Elementary invariants for RC-fields of finite corank

A field K is called of corank e if G(K) has rank e. We shall prove that the theory of RC-fields of corank $\leq$ e is decidable. First, we improve corollary 37 for those RC-fields which have small absolute Galois group.

Let us fix for the moment a prime field P and a finite Galois extension P_q of P. (The notations are those preceding lemma 36). Recall that we associated to the polynomial q(X) a sequence of polynomials $r_1, \ldots, r_n$, where n = deg q(X). $(r_1(\delta), \ldots, r_n(\delta)$ are the n roots of q(X) if δ is one of them.) Let us write S_q for the symmetric group on $r_1, \ldots, r_n$. Given a field $K \supset P$ and a Galois extension F of K containing a root δ of q(X) we define a morphism

$\pi_\delta : G(F|K) \longrightarrow S_q$, by

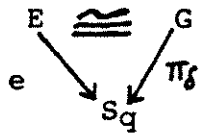
$\pi_\delta(\sigma)(r_i) = r_j$ iff $\sigma(r_i(\delta)) = r_j(\delta)$.

(π_δ just describes how each σ permutes the roots of q(X); note that the image of π_δ is isomorphic to $G(P_q.K|K)$.)

Now we fix <u>one</u> representative from each isomorphism type E of <u>finite</u> groups, and indicate this representative also by E (for simplicity). Given such an E and a morphism e: $E \longrightarrow S_q$ we can construct a sentence $\theta_q(e,E)$ such that for each field $K \supset P$ the following holds:

$K \models \theta_q(e,E)$ $\iff$ There is a Galois extension F of K containing a root δ of q(X), and an isomorphism

$E \cong G(F|K)$ such that the diagram



commutes.

Now we can formulate the following variation on lemma 36.

Lemma 57

Let $K \supset P$, $L \supset P$ and let i,j be the natural inclusions $Abs(K) \hookrightarrow K$, $Abs(L) \hookrightarrow L$. Assume that G(K) or G(L) is small. Then the following are equivalent:

(1) There exists an isomorphism f: $\widetilde{Abs}(L) \cong \widetilde{Abs}(K)$ mapping Abs (L) onto Abs (K) such that $(G(K),\hat{i}) \overset{\hat{f}}{\cong} (G(L),\hat{j})$;

(2) $K \models \theta_q(e,E) \iff L \models \theta_q(e,E)$, for all q, E, e as above.

Proof (1) $\Longrightarrow$ (2) is just a consequence of lemma 36, and the fact that one can take each $\theta_q(e,E)$ of the form $\Phi_q(r_1, \ldots, r_n)$. (This fact can be established by a tedious but straightforward argument, which we leave to the reader.)

Now assume (2). By a projective limit argument we shall construct an isomorphism f: $\widetilde{Abs}(L) \cong \widetilde{Abs}(K)$ mapping Abs (L) onto Abs (K), together with an isomorphism $\phi : G(K) \cong G(L)$, such that the diagram

$$\begin{array}{ccc} G(K) & \xrightarrow{\phi} & G(L) \\ {\scriptstyle \hat{i}}\downarrow & & \downarrow{\scriptstyle \hat{j}} \\ G(Abs\ K) & \xrightarrow[\hat{f}]{} & G(Abs\ L) \end{array}$$

commutes. This statement clearly implies (1). In the construction of f and ϕ we will freely use the notations $P_{q,K}$, $P_{q,L}$, σ^μ introduced in the proof of lemma 36.

For each finite Galois extension F of K and each q with $F \supset K.P_{q,K}$ we define M(F,q) as the set of all triples (F', ϕ, μ) such that F' is a finite Galois extension of L with $F' \supset L.P_{q,L}$, ϕ is an isomorphism $G(F|K) \cong G(F'|L)$ and μ is an isomorphism $P_{q,K} \cong P_{q,L}$ mapping $K \cap P_{q,K}$ onto $L \cap P_{q,L}$, with the property that the diagram

$$\begin{array}{ccc} G(F|K) & \xrightarrow{\phi} & G(F'|L) \\ \downarrow & & \downarrow \\ G(K.P_{q,K}|K) & \longrightarrow & G(L.P_{q,L}|L) \\ \sigma & \longmapsto & \sigma^{\mu} \end{array}$$

commutes.

Claim 1 $M(F,q) \neq \emptyset$

To prove this, choose a root δ of q(X) in F and an isomorphism p: $E \cong G(F|K)$, where E is the representative of the isomorphism type of G(F|K). Then there is a unique morphism e: $E \longrightarrow S_q$ such that $\pi_\delta \circ p = e$. So we have $K \models \theta_q(e,E)$, hence $L \models \theta_q(e,E)$. This means that there is a Galois extension F' of L, a root δ' of q(X) in F' and an isomorphism p': $E \cong G(F'|L)$ such that $\pi_{\delta'} \circ p' = e$. Now we put $\phi = p' \circ p^{-1}$ (so ϕ is an isomorphism of G(F|K) onto G(F'|L)), and define μ: $P_{q,K} \xrightarrow{\sim} P_{q,L}$ by $\mu(\delta) = \delta'$, and a straightforward computation gives $(F', \phi, \mu) \in M(F,q)$.

Claim 2 $Im(G(K)) = Im(G(L))$

If $E \in Im(G(K))$, say $E \cong G(F|K)$, then $M(F,q) \neq \emptyset$ (for q such that $P_q = P$, say) immediately gives $E \in Im(G(L))$, so $Im(G(K)) \subset Im(G(L))$, and by symmetry, we get equality.

Claim 3 $M(F,q)$ is finite.

From claim 2, the hypothesis, and Schuppar's result on small profinite groups in [S], we get that $G(K)$ and $G(L)$ are both small, and claim 3 follows immediately.

Now we put $(F_1,q_1) \geq (F_2,q_2)$ if $F_1 \supset F_2$ and $P_{q1} \supset P_{q2}$. It is easy to see that the (F,q)'s (with F a finite Galois extension of K containing a root of $q(X)$) are directed upwards, and that if $(F_1,q_1) \geq (F_2,q_2)$, then there is a canonical map $M(F_1,q_1) \longrightarrow M(F_2,q_2)$. So the $M(F,q)$'s form a projective system of finite non-empty sets (by the claims above), so $\varprojlim M(F,q) \neq \emptyset$. Now an element of $\varprojlim M(F,q)$ determines first of all an isomorphism $\phi : G(K) \xrightarrow{\sim} G(L)$ (by claim 2 and smallness), and secondly an isomorphism $\mu : \widetilde{Abs}(K) \xrightarrow{\sim} Abs(L)$ mapping $Abs(K)$ onto $Abs(L)$ such that the diagram

$$\begin{array}{ccc} G(K) & \xrightarrow{\phi} & G(L) \\ \downarrow \hat{i} & & \downarrow \hat{j} \\ G(Abs\ K) & \longrightarrow & G(Abs\ L) \\ \sigma & \longmapsto & \sigma^{\mu} \end{array}$$

commutes. Now just take $f = \mu^{-1}$. ∎

Corollary 58 Let $K \supset P$, $L \supset P$ be two RC-fields and assume that $G(K)$ or $G(L)$ is small. Then $K \equiv L$ if and only if K and L have the same degree of imperfectness, and for all q, E, e as above:

$K \models \theta_q(e,E) \iff L \models \theta_q(e,E)$.

Proof Combine Proposition 33 and the previous lemma. ∎

For our decision procedure in (6.2) we shall need the somewhat technical lemma 59 below. In the following Galois extensions

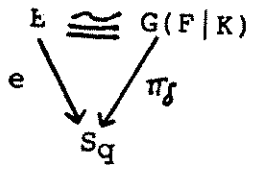
of a field K are always taken inside a fixed algebraic closure $\tilde{K}$ of K.

Definition

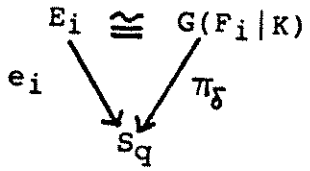
Given a Galois extension P_q of a prime field P, representatives E, E_1, . . ., E_n, and morphisms e: $E \longrightarrow S_q$, e_i: $E_i \longrightarrow S_q$, i = 1, . . ., n, all with the same image in S_q, we let $\theta_q(e,E|e_1,E_1; \ldots; e_n, E_n)$ be a sentence of field theory such that for each field $K \supset P$ we have:

$$K \models \theta_q(e,E|e_1,E_1; \ldots; e_n, E_n)$$
$$\Longleftrightarrow$$

there is a root δ of q(X) (in $\tilde{K}$) and a Galois extension F of K containing δ and an isomorphism $E \cong G(F|K)$ such that the diagram



commutes, and such that, for each i = 1, . . ., n, there is no Galois extension $F_i|K$ containing δ with an isomorphism $E_i \cong G(F_i|K)$ making



commutative.

Remark Note that $\theta_q(e,E) \wedge \neg\theta_q(e_1,E_1) \wedge \ldots \wedge \neg\theta_q(e_n, E_n)$ implies $\theta_q(e,E|e_1, E_1; \ldots; e_n, E_n)$, for fields $\supset P$. Note also

that we have an effective method which, given $q(X)$, $e : E \to S_q$ and the $e_i : E_i \to S_q$ $(i = 1,\ldots,n)$ as above, constructs the sentence $\theta_q(e, E|e_1, E_1;\ldots;e_n, E_n)$.

Lemma 59. Suppose $K \supset P$ and $K \models \tau$, where τ is a conjunction $\theta_{q(1)}(e(1), E(1)) \wedge \ldots \wedge \theta_{q(k)}(e(k), E(k)) \wedge \neg\theta_{q(k+1)}(e(k+1), E(k+1)) \wedge \ldots \wedge \neg\theta_{q(k+\ell)}(e(k+\ell), E(k+\ell))$. Then there is a sentence $\sigma = \theta_q(e, E|e_1, E_1;\ldots;e_n, E_n)$ as defined above, such that $K \models \sigma$ and $\sigma \to \tau$ holds in all fields $\supset P$.

Proof(i): Let P_q be the splitting field of the $q(j)$, $j = 1,\ldots,k+\ell$, with q irreducible over P, and consider P_q and the $P_{q(j)}$ as subfields of $\tilde{K}$. Choose for each $j = 1,\ldots,k$ a Galois extension $F(j)|K$, and isomorphism $E(j) \cong G(F(j)|K)$ and a root $\delta(j)$ of $q(j)(X)$ such that the diagram

$$\begin{array}{ccc} E(j) & \cong & G(F(j)|K) \\ & {\scriptstyle e(j)}\searrow \quad \swarrow{\scriptstyle \pi_{\delta(j)}} & \\ & S_{q(j)} & \end{array}$$

commutes.

Choose for F any finite Galois extension of K containing $F(1),\ldots,F(k)$, and take a root δ of $q(X)$, an isomorphism $E \cong G(F|K)$ and a morphism $e : E \to S_q$ making the diagram

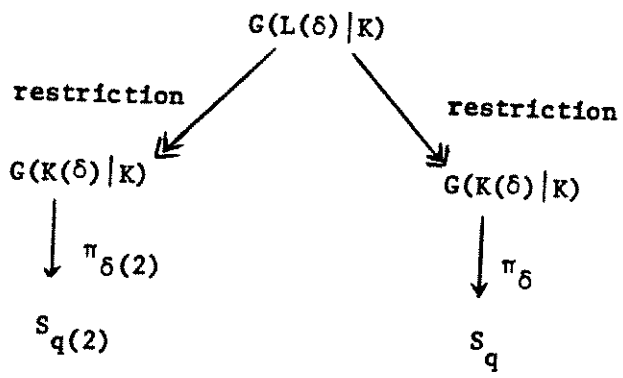
$$\begin{array}{ccc} E & \cong & G(F|K) \\ & {\scriptstyle e}\searrow \quad \swarrow{\scriptstyle \pi_{\delta}} & \\ & S_q & \end{array}$$

commutative.

Then $K \models \theta_q(e,E)$ and it is easy to see that the implication $\theta_q(e,E) \to (\theta_{q(1)}(e(1), E(1)) \wedge \ldots \wedge \theta_{q(k)}(e(k), E(k)))$ holds in all fields $\supset P$.

(ii) By (i) we can assume without loss of generality that $k = 1$. Moreover, if δ is a root of $q(1)$, then $q(2),\ldots,q(\ell+1)$ split in $P(\delta)$.

Now look for example at the condition $\theta_{q(2)}(e(2), E(2))$. Select a root $\delta(2)$ of $q(2)$ in $P(\delta)$. Suppose L is a Galois extension of K containing $\delta(2)$. We have



and we want to fill in $S_q \overset{\alpha}{\to} S_{q(2)}$ to make this commute.

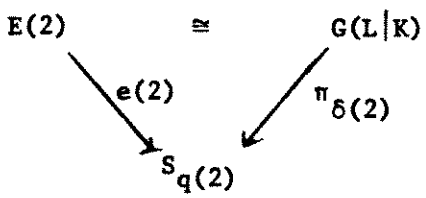
Let m = degree $(q(1))$,

n = degree $(q(2))$.

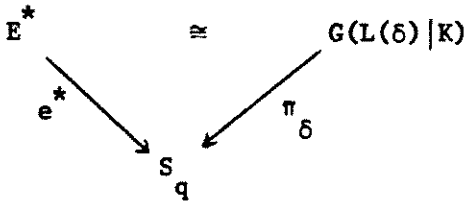
Let $r_1^{(1)},\ldots,r_m^{(1)}$ and $r_1^{(2)},\ldots,r_n^{(2)}$ be the polynomials corresponding to $q(1)$, $q(2)$ respectively. Now $\delta(2)$ can be written as $R(\delta)$ for some $R \in P[x]$. Now we define $\alpha : S_q \to S_{q(2)}$ by:

$r^{(2)}_{\alpha(\pi)(i)}(\delta(2)) = R(r^{(1)}_{\pi(j)}(\delta))$ if $r^{(2)}_i(\delta(2)) = R(r^{(1)}_j(\delta))$. We leave to the reader the verification that α is well-defined, independent of R, and works.

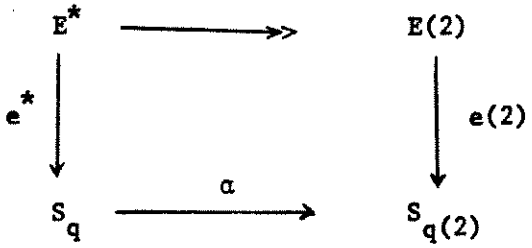
Now suppose we have a commuting



Using the preceding paragraph this readily gives

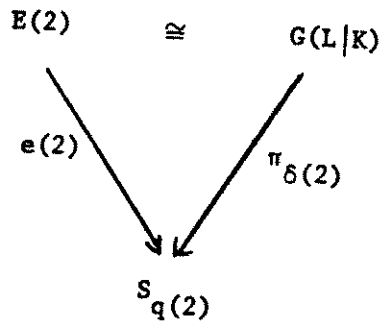


where αe^* covers e(2), i.e.



commutes. Note that α depends only on δ and R, and is uniquely determined by them. Call such an α <u>suitable</u>.

Suppose conversely we have E^*, e^* and suitable α with commuting diagrams as above. Then it is simple to get a commuting



This shows that there is some E^*, e^* such that

$$K \models \theta_{q(1)}(e^*,E^*)$$

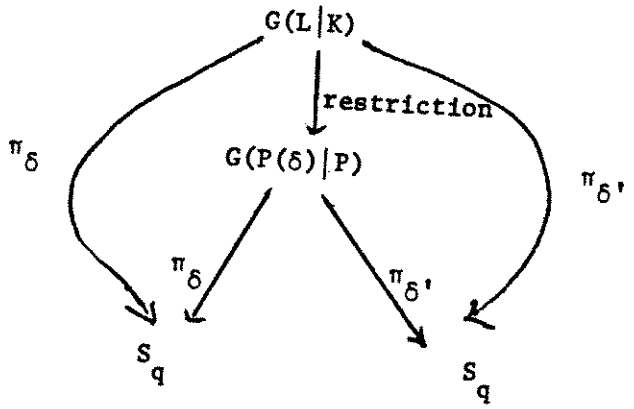
and

$$\theta_{q(1)}(e^*,E^*) \rightarrow \neg\theta_{q(2)}(e(2),E(2))$$

holds in all extensions of P.

So now without loss of generality we can assume $q(1) = q(2) = \cdots = q(\ell+1) = q$.

(iii) Finally we must consider the relation between π_δ and $\pi_{\delta'}$ for different roots δ,δ' of q. Suppose L is a Galois extension of K containing δ (equivalently, δ'). Then π_δ, $\pi_{\delta'}$ are best represented via



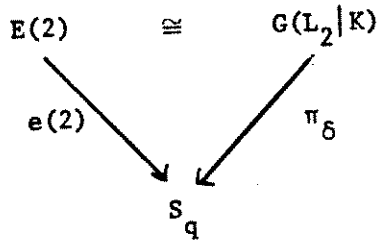
(We do not bother to make our notation reflect L).

Now it can be easily checked that if $\gamma \in G(P(\delta)|P)$ and $\delta' = \gamma(\delta)$ then

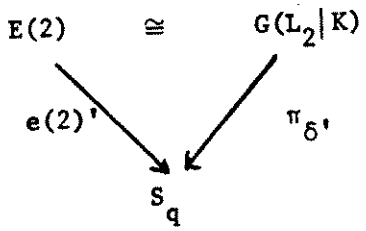
$$\pi_{\delta'}(\sigma) = \pi_{\delta}(\gamma)^{-1}\pi_{\delta}(\sigma)\pi_{\delta}(\gamma)$$

for all $\sigma \in G(P(\delta)|P)$. And of course, since q is irreducible over P, there is a γ with $\delta' = \gamma(\delta)$. So $\pi_{\delta'}$ and π_{δ} are conjugate.

So now suppose there is no L_2 Galois over K, containing δ, with commuting



Let $e(2)'(g) = \pi_{\delta}(\delta)^{-1}e(2)(g)\pi_{\delta}(\gamma)$, for $g \in E(2)$. Then by the preceding analysis there is no L_2 with commuting



We write $e(2)' = e(2)^{\gamma}$, in an obvious notation, and call $e(2)^{\gamma}$ a conjugate of $e(2)$. So now at last we see that

(i) $$K \models \theta_q(e(1),E(1)|e(2),E(2);\ldots;e(r),E(r))$$

where $\{e(2),\ldots,e(r)\}$

$= \{e(j)^{\gamma}: 2 \leq j \leq \ell + 1,\ \gamma \in G(P(\delta)|P)\}$;

(ii) if σ is the above θ_q, then $\sigma \to \tau$ holds in all fields $\supset P$.

This completes the proof. □

(6.2) Theorem 60: The theory of RC-fields of corank $\leq e$ is decidable, for each $e \in \mathbb{N}$.

Remarks:

(1) In contrast, in section 7 we shall see that the theory of RC-fields of finite corank is undecidable. Let us also note that the statement of Theorem 60 remains true if we prescribe the characteristic, and any degree of imperfectness compatible with the characteristic. (This is clear from the proof.)

(2) We shall follow the pattern of the proof of Theorem 43. Again, we tacitly assume that certain algebraic objects (such as a finite Galois extension of a prime field) are effectively presented (say, by giving the characteristic of the prime field P, the defining polynomial $q(X) \in P[X]$, with its associated sequence $r_1,\ldots,r_n$), and that certain algebraic operations in and on such objects are given by effective constructions. It would be painful to spell out exactly what is needed in this respect, and the proof makes it clear anyway.

Proof: Let $e \in \mathbb{N}$ be given. We only have to show that the set of sentences which are false in some RC-field of corank $\leq e$ is recursively enumerable. Now, the complete theory of an RC-field K of corank $\leq e$ is, besides by the axioms for RC-fields, axiomatized by the sentences saying what the characteristic and degree of imperfectness of K are, and by the sentences $\theta_q(e,E)$ and $\neg\theta_q(e,E)$ which hold in K. (By Corollary 58.) By Lemma 59 every finite set of sentences of the forms $\theta_q(e,E)$, $\neg\theta_q(e,E)$ can be replaced by one sentence of the form $\theta_q(e,E|e_1,\bar{E}_1;\ldots;e_n,E_n)$.

Now, by the same argument as in the proof of Theorem 43, we are led to consider a situation of the following type: A finite Galois

extension P_q of a prime field P, of characteristic p, is given, and a supernatural number d, where $d = 1$ if $p = 0$, and $d \in \{1, p, p^2, \ldots, p^\infty\}$ if $p > 0$. Further morphisms $e: E \to S_q$, $e_i: E_i \to S_q$, $i=1,\ldots,n$, are given, all with the same image $\Gamma \subset S_q$. (*)

It suffices to produce an algorithm which from such data (*) computes an answer to the question whether or not there is an RC-field $K \supset P$ of degree of imperfectness d, satisfying $\theta_q(e, E | e_1, E_1; \ldots; e_n, E_n)$. (**)

Now, if such a K exists, then, for $L = K \cap P_q$ and a suitable root δ of $q(X)$ we have $\Gamma \cong G(K(\delta)|K) \cong G(P_q|L)$, and in view of the nature of these isomorphisms we see that the embedding $\pi_\delta: G(P_q|L) \to S_q$ has image Γ. Let us denote the epis $E \to \Gamma$, $E_i \to \Gamma$ induced by e, e_i by $\tilde{E}$, $\tilde{E}_i$ $(i=1,\ldots,n)$.

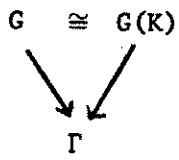
Claim: A field K as described in (**) exists, if and only if there is a subfield L of P_q such that $\pi_\delta: G(P_q|L) \to S_q$ has image Γ, for a suitable root δ of $q(X)$, and there is a projective profinite group $\tilde{G}$ over Γ with $\tilde{E} \in \mathrm{Im}(\tilde{G})$ and $\tilde{E}_i \notin \mathrm{Im}(\tilde{G})$, for $i=1,\ldots,n$.

If the claim is true, we have an algorithm as required in (**): by checking the subgroups of $G(P_q|P)$ given as a permutation group on the roots of q we can decide whether a field L exists, and by Corollary 56 we can decide effectively whether $\tilde{G}$ exists.

One direction of the claimed equivalence is easy: if K exists, just take $L = P_q \cap K$ and $\tilde{G}$ = the epi $(G(K) \to \Gamma)$, induced by a suitable $\pi_\delta: G(F|K) \to S_q$ as described in the definition of $\theta_q(e, E | e_1, E_1; \ldots; e_n, E_n)$.

Now for the other direction: let π_δ map $G(P_q|L)$ onto $\Gamma \subset S_q$, where δ is a root of $q(X)$ and L a subfield of P_q. Let $\tilde{G} = (G \to \Gamma)$

be a projective profinite group over Γ with $\widetilde{E} \in \mathrm{Im}(\widetilde{G})$, $\widetilde{E}_i \notin \mathrm{Im}(\widetilde{G})$ for $i=1,\ldots,n$. Just as in the proof of Theorem 43 we find an RC-field $K \supset P_q$, of degree of imperfectness d, with $K \cap P_q = L$, such that for some isomorphism $G \cong G(K)$ we have a commuting diagram



From the properties of $\widetilde{G}$ it is clear that $K \models \theta_q(e,E|e_1,E_1;\ldots;e_n,E_n)$.

§7. Undecidability

(7.1) We shall prove that the cotheory of projective profinite groups is undecidable. This will give the undecidability of the theory of RC-fields, via interpretability. This was proved independently by Ersov.

(7.2) We first give an example to show that there are projective profinite groups which do not have the Iwasawa property.

Example: Let q be an odd prime and Dq the dihedral group generated by α,β with relations $\alpha^2 = 1$, $\beta^q = 1$, $\alpha^{-1}\beta\alpha = \beta^{-1}$.

Dq has $2q$ elements and cannot be written non-trivially as a direct product.

Let $H = Dq \times \mathbb{F}_2$ ($\mathbb{F}_2$ the group of 2 elements). Identify Dq and $\mathbb{F}_2$ as subgroups of H. Let N_1 and N_2 be respectively Dq and $\langle\beta\rangle \times \mathbb{F}_2$. Both are normal in H with quotient isomorphic to $\mathbb{F}_2$. However there is no normal subgroup M_1 of H with $M_1 \subset N_1$ and $H/M \cong Dq$, whereas $M_2 = \mathbb{F}_2 \subset N_2$ and $H/M_2 \cong Dq$.

We claim that the projective cover $P(H)$ does not have IP. For, consider

$$\begin{array}{ccc} & & P(H) \\ & & \downarrow p \\ & & H \\ & & \downarrow \text{natural} \\ H/M_2 & \xrightarrow{\text{natural}} & H/N_2 \cong H/N_1 \end{array}$$

Suppose this can be completed by an epi $\gamma: P(H) \to H/M_2$ to a commutative diagram. Let $K = \text{kernel}(\gamma)$. Then the induced epi $P(H)/K \to H/p(K)$ is essential, see the proof of the 2nd part of Lemma 48. But $P(H)/K \cong H/M_2 \cong Dq$, and the only essential epi's with domain Dq are

isomorphisms. So $H/p(K) \cong Dq$. On the other hand, $K \subset p^{-1}(N_1)$, so $p(K) \subset N_1$, contradiction.

Our undecidability proof will be an elaboration of the above.

(7.3) Coding graphs

A graph is simply a set together with an irreflexive symmetric binary relation on it. A basic undecidability result [ELTT] says that the theory of graphs is recursively inseparable from the set of sentences refutable in some finite graph.

We give a construction $G \to \Gamma(G)$ which to any profinite G assigns a graph $\Gamma(G)$ (whose underlying set may be empty). We show that every graph is isomorphic to a $\Gamma(G)$, G projective. $\Gamma(G)$ will be interpretable in the cotheory of G, whence our undecidability results.

Fix distinct odd primes p, q. The underlying set of $\Gamma(G)$ is the set of open normal N with $G/N \cong Dp$. Dote that for such N there is unique open normal $M \supset N$ with $G/M \cong \mathbb{F}_2$, and we indicate this M in the following as N'. We define a relation R on $\Gamma(G)$ thus: $R(N_1,N_2)$ iff $N_1 \neq N_2$ and there exists normal open $M \supset N_1' \cap N_2'$ with $G/M \cong \mathbb{F}_2$, such that there is open normal $N \subset M$ with $G/N \cong Dq$.

Evidently, $(\Gamma(G),R)$ is a graph, possibly empty. By $\Gamma(G)$ we normally understand the graph. The proof of the next 2 lemmas is clear.

Lemma 61: There is a single cosentence expressing that $\Gamma(G) \neq \emptyset$.

Lemma 62: If $\Gamma(G) \neq \emptyset$, then the 1st order theory of $\Gamma(G)$ is interpretable in the cotheory of G.

Now a nice use of projective covers.

Lemma 63: $\Gamma(G) \cong \Gamma(P(G))$.

Proof: The essential point is that $\mathbb{F}_2$, Dp and Dq have no nontrivial essential epis from them.

Let $p:P(G) \to G$ be the projective cover, and H open normal in P(G), with $P(G)/H \cong$ one of $\mathbb{F}_2$, Dp, Dq. Since the induced epi $P(G)/H \to G/p(H)$ is essential (see the proof part of the 2nd part of Lemma 48), we have $G/p(H) \cong P(G)/H$. Hence $H = p^{-1}(p(H))$ (since $G/N \cong P(G)/p^{-1}(N)$ for each open normal N in G).

So $\Gamma(G)$ and $\Gamma(P(G))$ are naturally isomorphic as sets, via $N \to p^{-1}(N)$, and it is easy to see that this map is also an isomorphism of $\Gamma(G)$ and $\Gamma(P(G))$ as graphs.□ We define $\Gamma(G)$ also for a (discrete) group G: in the definition of $\Gamma(G)$ we simply replace "normal open subgroup" by "normal subgroup of finite index". Now the subgroups of finite index of a group G are in a natural 1-1 correspondence with the open subgroups of its profinite completion $\hat{G} = \varprojlim G/N$, N ranging over the normal subgroups of finite index. (See [Lu-vd D, p. 28].) This gives:

Lemma 64: $\Gamma(G) \cong \Gamma(\hat{G})$.

Now we face the construction problem. Given a graph Γ, we must construct a group G with $\Gamma(G) \cong \Gamma$.

Stage 1: Fix distinct odd primes p and q. Let V be a vector space over $\mathbb{F}_2$, the field of 2 elements. Let $\mathcal{H}$ and $\mathcal{I}$ be families of (linear) subspaces of V of codimension 1. We define a vector space A over $\mathbb{F}_p$ by taking $(a_H)_{H \in \mathcal{H}}$ as a basis, and a vector space B over $\mathbb{F}_q$ by taking $(b_I)_{I \in \mathcal{I}}$ as basis. We define an action of the additive group V on the additive group $A \oplus B$ by:

$$a_H^v = a_H \text{ if } v \in H \quad , \quad b_I^v = b_I \text{ if } v \in I$$

$$- a_H \text{ if } v \notin H \qquad - b_I \text{ if } v \notin I.$$

It is easy to check that these formulas uniquely determine for each $v \in V$ an automorphism $x \mapsto x^v$ of $A \oplus B$.

Let G be the semidirect product $(A \oplus B) \ltimes V$ corresponding to this action.

Let us note here that G is residually finite. As we do not need this fact, we leave the (easy) proof to the reader. (The main point is to use that A, B and V are locally finite groups.)

Now we try to identify those $N \lhd G$ with $G/N \cong \mathbb{F}_2$, Dp, Dq.

Let $\varphi: G \to \mathbb{F}_2$ be an epi. $A \oplus B \subset \ker(\varphi)$, since A is of exponent p and B of exponent q. Considering the exact sequence $0 \to A \oplus B \to G \to V \to 0$ we see that φ corresponds with an epi $V \to \mathbb{F}_2$, and so with a subspace of V of codimension 1.

Next, suppose $\varphi: G \to Dp$ is an epi. Then $B \subset \ker(\varphi)$. Let r, s with $r^p = s^2 = 1$, $s^{-1}rs = r^{-1}$ generate Dp. Then necessarily $\varphi(A) = \langle r \rangle$ and $\varphi(V) = \langle s \rangle$. So $\ker(\varphi) \cap A$ is a subspace of codimension 1, and $\ker(\varphi) \cap V$ is a subspace of V of codimension 1. Take $H \in \mathcal{H}$ such that $\varphi(a_H) \neq 1$. Then $\varphi(n.a_H) = r$ for some $n \in N$. We'll show that $\ker(\varphi) = (\langle a_I : I \neq H \rangle \oplus B).\ H$. First of all, for $v \in H$ we have $a_H^v = a_H$, whence $\varphi(v) = 1$. (Here we use that $\delta = \varphi(v)$ satisfies $\delta^2 = 1$, $\delta^{-1}r\delta = r$, implying $\delta = 1$.) Next, for $I \in \mathcal{H}$, $I \neq H$ we take $v \in H \setminus I$ and get $a_I^v = -a$, so $\varphi(a_I)^{-1} = \varphi(a_I)$, and $\varphi(a_I)P = 1$, which implies $\varphi(a_I) = 1$. The assertion on $\ker(\varphi)$ follows.

Conversely, if $H \in \mathcal{H}$, then $N = (\langle a_I : I \in \mathcal{H} \setminus \{H\} \rangle \oplus B)$. N is a normal subgroup of G and $G/N \cong Dp$.

It follows that the map $H \to N$, N as above, is a bijection of $\mathcal{H}$ onto the underlying set of $\Gamma(G)$. Via this map we identify $\mathcal{H}$ with the underlying set of $\Gamma(G)$. Now we replace p by q in the penultimate

paragraph and get a corresponding identification of $\mathcal{I}$ with the set of $N \lhd G$ with $G/N \cong Dq$. This allows us to identify the graph relation on $|\Gamma(G)| = H$. If $H_1, H_2 \in H$, then $R(H_1,H_2)$ holds iff $H_1 \neq H_2$ and there exists $I \in \mathcal{I}$ with $H_1 \cap H_2 \subset I$.

Stage 2: Let (Γ,R) be a graph. We let V be a vectorspace over $\mathbb{F}_2$ with basis $(v_\gamma)_{\gamma\in\Gamma}$. Let $H_\gamma = \langle v_\delta : \delta \neq \gamma\rangle$. H_γ is a subspace of codimension 1. Put $H = \{H_\gamma : \gamma \in \Gamma\}$. For $\gamma \neq \delta$ let $I(\gamma,\delta) = \langle v_\gamma + v_\delta\rangle \oplus \langle v_\lambda : \lambda \neq \gamma,\delta\rangle$. $I(\gamma,\delta)$ is of codimension 1, and we put $\mathcal{I} = \{I(\gamma,\delta) : R(\gamma,\delta)\}$. Now construct G as in Stage 1. As observed there, the set $|\Gamma(G)|$ can be identified with Γ, and so with H. The relation R on $\Gamma(G)$ holds between H_γ and H_δ iff $\gamma \neq \delta$ and for some γ',δ' with $\gamma' \neq \delta'$ and $R(\gamma',\delta')$ we have $I(\gamma',\delta') \supset H_\gamma \cap H_\delta$. But note that there are exactly three subspaces of codimension 1 containing $H_\gamma \cap H_\delta$, namely H_γ, H_δ and $I(\gamma,\delta)$. Clearly $H \cap \mathcal{I} = \emptyset$, so $R(H_\gamma,H_\delta)$ holds iff $I(\gamma,\delta) = I(\gamma',\delta')$ for some γ',δ' with $R(\gamma',\delta')$. But then $\{\gamma,\delta\} = \{\gamma',\delta'\}$ and $R(\gamma,\delta)$. So $R(H_\gamma,H_\delta)$ iff $R(\gamma,\delta)$.

We have proved that $\Gamma(G) \cong \langle\Gamma,R\rangle$. This proves:

Theorem 65: For every graph Γ there is a projective profinite G with $\Gamma(G) \cong \Gamma$. If Γ is finite, we can take G finitely generated.

Proof: The first statement follows from the lemmas in this section and the constructions given in Stages 1 and 2 above. For the second part we note that the discrete group G which we associate to Γ is finite, if Γ is finite. Then $P(G)$ is finitely generated of rank $rk(G)$. □

Corollary: The cotheory of projective profinite groups is undecidable. In fact, it is recursively inseparable from the set of cosentences refutable in some finitely generated projective profinite group.

Proof: Directly from interpretability and the corresponding result for graphs.

Remarks:

1. The cotheory of (projective) profinite groups is recursively enumerable, as is the set of cosentences refutable in some finitely generated (projective) profinite group.

2. The projective covers $P(G)$ of the profinite completions of the discrete groups considered at Stage 1 are prosolvable of class 2.

Translated to RC-fields we have:

Corollary: The theory of RC-fields is undecidable. The theory of RC-fields of finite corank is undecidable.

Remarks: Both statements remain true if we prescribe characteristic and any degree of imperfectness compatible with the characteristic.

Proof: By Proposition 38 and the previous corollary.

§8. Concluding Remarks

8.1. We are confident that all main problems in the model theory of RC-fields have now been solved. We regret the long delay between our discovery of the results (by end of April 1980) and the production of a finished manuscript (January 1982). During that period other groups have published their independent findings (as we detailed in the text), and we thank especially Ersov, and Fried-Haran-Jarden-Lubotzky for a free exchange of ideas. To our knowledge, the only important new result since April 1980 is the decidability of Iwasawa RC-fields, by Haran-Lubotzky [Ha-L]. We point out here a consequence of their method:

Theorem 66: The theory of Iwasawa RC-fields is equal to the theory of Iwasawa RC-fields of finite corank.

This should be contrasted with the inseparability result of Theorem 60.

8.2. We expect that our "comodel theory" will be a useful tool in the model theory of arbitrary fields. Here are three challenging problems:

(1) Is the class of all $G(K)$ coelementary?

(2) Is $G(Q)$ decidable?

(3) Prove that K infinite stable implies $G(K) = 1$, via "costability" for profinite groups.

A negative answer to (2) would give a radically new proof of undecidability of Q. A positive answer will need very detailed information relating to the inverse problem of Galois theory.

8.3. We hope to see a systematic treatment of profinite model theory, not just for groups. A promising start has been made by Zoé Chatzidakis [Cha] at Yale. She has proved the dual of the Keisler-Shelah Theorem, as well as a Completeness Theorem.

We remark that we have an unpublished treatment of co-model completeness, comprising duals of Robinson's Test, existentially closed models, model companions and forcing. The details may appear later, if they prove useful in applications.

We are aware of formal connections between our work and that of Henson ([He], but mostly unpublished) on nonstandard hulls of Banach spaces. We believe that it will be fruitful to analyze the precise connection, and to seek a common topological model theory subsuming both.

REFERENCES

[Ax] J. Ax, The elementary theory of finite fields, Annals of Mathematics 88 (1968), 239-271.

[Ba] B. Banaschewski, Projective covers in categories of topological spaces and topological algebras. General Topology and its relations to Modern Analysis and Algebra (Proc. Kanpur Top. Conf., 1968), Academic, Prague, 1971, 63-91.

[Bo] N. Bourbaki, Algèbre, Chapitres 4 et 5. Hermann, Paris, 1950.

[C-K] C. Chang and J. Keisler, Model Theory, North-Holland, Amsterdam, 1973.

[Ch-vdD-M] G. Cherlin, L. van den Dries, A. Macintyre, Decidability and undecidability theorems for PAC-fields, Bull, AMS (1981), 101-104.

[Do] A. Douady, Cohomologie des groupes compacts totalement discontinus, Seminaire Bourbaki 189, Décembre 1959.

[Du] J. Duret, Les corps pseudofinis ont la propriete d'independance, C. R. Acad. Sc. Paris 290 (1980), 981-983.

[v.dD] L. van den Dries, New decidable fields of algebraic numbers. Proc. AMS 77 (1978), 251-256.

[vdD-M] L. van den Dries and A. Macintyre, More on PAC-fields, in preparation.

[vdD-S] L. van den Dries and R. Smith, Decidability PAC-subfields of Q., in preparation.

[E1] Ju. Eršov, Fields with a solvable theory, Soviet Math. Dokl. 8.

[E2] Ju. Eršov, On elementary theories of regularly closed fields,

[E3] Ju. Eršov, Unpublished manuscript, 1981.

[E-F] Ju. Eršov and M. Fried, Frattini covers and projective groups without the extension property, Math Annalen 253 (1980), 233-239.

[ELTT] Ju. L. Eršov, I.A. Lavrov, AD Taĭmanov, M.A. Taiclin, Elementary theories, Soviet, Math 20 (1965), 34-105.

[F-H-J] M. Fried, D. Haran, M. Jordan, Galois stratification over Frobenius fields, preprint, 64 pages.

[G] K. Gruenberg, Projective profinite groups, Journal of the London Math. Society 42 (1967), 155-165.

[He] C. W. Henson, When do two Banach spaces have isometrically isomorphic nonstandard hulls? Israel Journal 22 (1975), 57-67.

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

[J1] M. Jordan, Elementary statements over large algebraic fields, Trans. AMS 164 (1972), 67-91.

[J2] M. Jarden, Algebraic extensions of hilbertian fields of finite corank, Israel J. of Math. 18 (1974), 279-307.

[J3] M. Jarden, The elementary theory of -free Ax fields, Inventiones Math. 38, (1976), 181-206.

[J-K] M. Jarden and U. Kiehne, The elementary theory of algebriac fields of finite corank, Inventiones Math. 30 (1975), 275-294.

[L] S. Lang, Introduction to Algebraic Geometry, Interscience, New New York, 1958.

[Lu-vdD] A. Lubotzky and L. van den Dries, Subgroupes of free profinite groups and large subfields of Q, Israel J. of Math. 39 (1981), 25-45.

[M] O. Mel'nikov, Normal subgroups of free profinite groups, Math. USSR Izvestija 12 (1978), no. 1, 1-20.

[R] L. Ribes, Introduction of profinite groups and Galois cohomology, Queen's papers in pure and applied Math. 24, Queen's University. Kingston, Ontario, 1970.

[Ra] M. Rabin, Computable algebra: general theory and theory of computable fields, Trans. AMS 95 (1960), 341-360.

[S] B. Schuppar, Elementare Aussagen zur Arithmetik und Galoistheorie von Funktionenkörpern, Grelles Journal 313 (1980), 59-71.

[Sh] J. R. Shoenfield, Quantifier elimination in fields. Proc. 3rd Latin-Amer. Sympos. Math. Logic, Campenias 1976, 243-252. North-Holland 1977.

[T] T. Tamagawa, To appear in Proceedings of Jacobson Conference (Yale 1981), edited by G. Seligman.

[vdW] B. L. van den Waerden, Moderne Algebra I, Springer Verlag, Berlin and New York, 1930.

[Wh] W. Wheeler, Model-complete theories of pseudo-algebraically closed fields, Annals of Math. Logic 17 (1979), 205-226.

[Wo] C. Wood, Notes on the stability of separably closed fields, Journal of Symb. Logic 44 (1979), 412-416.