Arch. Math., Vol. 45, 229–231 (1985)

0003-889X/85/4503-0229 $ 2.10/0

The Bottom Theorem

By

Dan Haran*)

In this note we prove the following result:

(The Bottom) Theorem. *Let K be a Hilbertian field, K_s its separable closure and $G(K) = G(K_s/K)$ its absolute Galois group. Let e be a positive integer. Then for almost all e-tuples $\sigma \in G(K)^e$ the fixed field $K_s(\sigma)$ of σ is a finite extension of no proper subfield containing K.*
(Here "almost all" is used in the sense of the Haar measure on $G(K)^e$.)

This has been conjectured by Jarden in [2, p. 300], where the case $e = 1$ has been settled. Later Jarden [3] proved the Bottom Conjecture over global fields for $e \leqq 5$, developing some properties of maximal p-extensions of fields.

The theorem gains particularly in interest as the profinite analogue of Stalling's theorem – which by [2, p. 300] would imply the Bottom Conjecture – is now known to be false (cf. [1]).

Our proof is based on results of [2] and some elementary properties of permutation groups. Fix K and e as above and write the free profinite group $\hat{F}_e$ on e generators as the inverse limit of a sequence $\ldots \xrightarrow{\pi_3} H_3 \xrightarrow{\pi_2} H_2 \xrightarrow{\pi_1} H_1$ of epimorphisms of finite groups.

Lemma 1. *There exists a sequence $\ldots \xrightarrow{\pi_3} A_3 \xrightarrow{\pi_2} A_2 \xrightarrow{\pi_1} A_1$ of finite groups such that for every $k \geqq 1$:*

(i) *H_k is a subgroup of A_k, and $\pi_k \colon A_{k+1} \to A_k$ extends the map $\pi_k \colon H_{k+1} \to H_k$;*
(ii) *there exists a subgroup B_k of A_k such that $A_k = B_k H_k$ and $B_k \cap H_k = 1$;*
(iii) *for almost all $\sigma \in G(K)^e$ there exists a continuous homomorphism $\varrho \colon G(K) \to A_k$ such that $\varrho\langle\sigma\rangle = H_k$.*

Proof. (i) For every $k \geqq 1$ let $n_k = |H_k|$ and let S_{n_k} be the symmetric group on the set $\{1, \ldots, n_k\}$. Apply Cayley theorem to construct an embedding $\mu_k \colon H_k \to S_{n_k}$ with the property

(1) for all $1 \leqq i, j \leqq n_k$ there is a unique $h \in H_k$ s.t. $i^{\mu_k(h)} = j$.

Denote $A_k = S_{n_1} \times \ldots \times S_{n_k}$ and define $\lambda_k \colon H_k \to A_k$ by

$$\lambda_k(h) = (\mu_1 \circ \pi_1 \circ \cdots \circ \pi_{k-1}(h),\ \mu_2 \circ \pi_2 \circ \cdots \circ \pi_{k-1}(h), \ldots, \mu_k(h)).$$

*) Supported by Rothschild Fellowship.

This is an embedding, so we may identify H_k with its image in A_k. Now let $\pi_k\colon A_{k+1} \to A_k$ be the projection on the first k components of A_{k+1}. Then (i) is obviously satisfied.

(ii) Fix a $1 \leqq j_k \leqq n_k$ and let

$$B_k = \{(\tau_1, \ldots, \tau_k) \in A_k = S_{n_1} \times \ldots \times S_{n_k} \mid j_k^{\tau_k} = j_k\}$$

Then (ii) follows easily from (1).

(iii) Choose $\bar\sigma_1, \ldots, \bar\sigma_e \in A_k$ such that $H_k = \langle \bar\sigma_1, \ldots, \bar\sigma_e \rangle$. Let $p_i\colon A_k \to S_{n_i}$, $i = 1, \ldots, k$ be the coordinate projections. By [2, Lemma 4.2] for almost all $\sigma \in G(K)^e$ there exist epimorphisms $\varrho_i\colon G(K) \to S_{n_i}$ such that $\varrho_i(\sigma_j) = p_i(\bar\sigma_j)$ for $i = 1, \ldots, k$, $j = 1, \ldots, e$. (We use the fact that an intersection of finitely many sets of measure 1 is again a set of measure 1.) These maps define a unique homomorphism $\varrho\colon G(K) \to A_k$ such that $\varrho(\sigma_j) = \bar\sigma_j$, for $j = 1, \ldots, e$, whence $\varrho\langle\sigma\rangle = \langle\bar\sigma\rangle = H_k$. $\square$

Proof of the Theorem. Let $\sigma_1, \ldots, \sigma_e \in G(K)$ and let G be a closed subgroup of $G(K)$ such that $H = \langle \sigma_1, \ldots, \sigma_e \rangle \leqq G$ and $n = (G\colon H) < \infty$. Then G is clearly finitely generated and we may assume without loss of generality that

(i) G is torsion-free (by [2, Theorem 12.2]),
(ii) $H \cong \hat F_e$ (by [2, Theorem 5.1]),
(iii) the sets

$$X_k = \{\varrho\colon G \to A_k \mid \varrho(H) = H_k\}, \qquad k = 1, 2, \ldots$$

are not empty (by Lemma 1 (iii)).

The sets X_k's form an inverse system $\ldots \xrightarrow{\pi_3 \circ -} X_3 \xrightarrow{\pi_2 \circ -} X_2 \xrightarrow{\pi_1 \circ -} X_1$, and they are finite since every homomorphism from G into A_k is determined by its action on a finite set of generators of G. Thus $\varprojlim_k X_k \neq \emptyset$, i.e., there exist $\varrho_k \in X_k$ such that $\pi_{k+1} \circ \varrho_{k+1} = \pi_k$ for every k.

Denote $G_k = \varrho_k(G)$. Then $\ldots \xrightarrow{\pi_3} G_3 \xrightarrow{\pi_2} G_2 \xrightarrow{\pi_1} G_1$ is an inverse system and ϱ_k's define an epimorphism $\varrho\colon G \to \varprojlim_k G_k$ such that $\varrho(H) = \varprojlim_k H_k$. Now by the choice of H_k's and by (ii), $\varrho(H) \cong \hat F_e \cong H$. Thus $H \cap \operatorname{Ker}\varrho = 1$, by [4, Corollary 7.7]. But then $(\operatorname{Ker}\varrho\colon 1) = (H \operatorname{Ker}\varrho\colon H) \leqq (G\colon H) < \infty$, hence $\operatorname{Ker}\varrho = 1$, by (i). Thus $G = \varprojlim_k G_k$, $H = \varprojlim_k H_k$.

It follows that there is a k_0 such that

(iv) $\qquad (G_k\colon H_k) = (G\colon H) = n$ for all $k \geqq k_0$. Without loss $k_0 = 1$.

For every $k \geqq 1$ let Y_k be the set of all subgroups B'_k of G_k that satisfy

(v) $\qquad B'_k \cap H_k = G_k$

and one of the following three equivalent conditions

(vi) $\qquad B'_k \cap H_k = 1, \quad |B'_k| = n, \quad |B'_k| \leqq n$

(the equivalence is an immediate consequence of (iv) and (v)). The finite sets Y_k form an inverse system $\ldots \xrightarrow{\pi_3} Y_3 \xrightarrow{\pi_2} Y_2 \xrightarrow{\pi_1} Y_1$, and they are not empty, since $B_k \cap G_k \in Y_k$, by

Lemma 1 (ii). Thus $\varprojlim_k Y_k \neq \emptyset$, i.e., for every k there is a $B'_k \leqq G_k$ of order n such that $\pi_{k+1} B'_{k+1} = B'_k$ for all k.

It follows that there exists a subgroup B' of G such that $B' = \varprojlim_k B'_k$, in particular, $|B'| = n$. But this implies $n = 1$, by (i). Hence $G = H$. $\square$

References

[1] D. Haran, Non-free torsion free profinite groups with open free subgroups. To appear in Israel. J. Math.

[2] M. Jarden, Algebraic extensions of finite corank of Hilbertian fields. Israel. J. Math. **18**, 279–307 (1974).

[3] M. Jarden, An analogue of Artin-Schreier theorem. Math. Ann. **242**, 193–200 (1979).

[4] L. Ribes, Introduction to profinite groups and Galois cohomolgy. Queen's Papers in Pure and Appl. Math. **24**, Kingston 1970.

Eingegangen am 26.9.1984

Anschrift des Autors:

Dan Haran
Mathematisches Institut
Universität Erlangen-Nürnberg
Bismarckstraße 1 1/2
D-8520 Erlangen