ALGEBRAIC EXTENSIONS OF FINITE CORANK OF HILBERTIAN FIELDS

BY

MOSHE JARDEN

ABSTRACT

We consider here a hilbertian field k and its Galois group $\mathscr{G}(k_s/k)$. For a natural number e we prove that almost all $(\sigma) \in \mathscr{G}(k_s/k)^e$ have the following properties. (1) The closedsubgroup $\langle \sigma \rangle$ which is generated by $\sigma_1, \ldots, \sigma_e$ is a free pro-finite group with e generators. (2) Let K be a proper subfield of the fixed fiɩld $k_s(\sigma)$ of $\sigma_1, \ldots, \sigma_e$ in k_s, which contains k. Then the group $\mathscr{G}(k_s/K)$ cannot be topologically generated by less then $e+1$ elements. (3) There does not exist a $\tau \in \mathscr{G}(k/k)$, $\tau \neq 1$, of finite order such that $[k_s(\sigma): k_s(\sigma, \tau)] < \infty$. (4) If $e = 1$, there does not exist a field $k \subseteq K \subset k_s(\sigma)$ such that $1 < [k_s(\sigma): K] < \infty$. Here "almost all" is used in the sense of the Haar measure of the compact group $\mathscr{G}(k_s/k)^e$.

Introduction

We consider a hilbertian field k and denote by k_s its separable closure and by $\mathscr{G}(k_s/k)$ its Galois group. Like every compact group, $\mathscr{G}(k_s/k)$ has a unique normalized Haar measure μ. We pick up an e-tuple $(\sigma) \in \mathscr{G}(k_s/k)^e$ at random and ask what properties does the closed subgroup $\langle \sigma \rangle$ generated by (σ) have in $\mathscr{G}(k_s/k)^e$; or equivalently, what properties does the fixed field $k_s(\sigma)$ of (σ) have in k_s. We give several answers to this question. First we prove that $\langle \sigma \rangle$ is a free pro-finite group with e topological generators. In particular we have that $\langle \sigma_1, \cdots, \sigma_d \rangle \cap \langle \sigma_{d+1}, \cdots, \sigma_e \rangle = 1$ if $1 \leqq d < e$ and that $\sigma_i\sigma_j \neq \sigma_j\sigma_i$ for $1 \leqq i, j \leqq e$, $i \neq j$. Next we prove that the set $S(\sigma)$ of all $(\sigma') \in \mathscr{G}(k_s/k)^e$ such that $k_s(\sigma) \cong_k k_s(\sigma')$ has the measure 0. Moreover we show that there are at least $2^{\aleph_0}$ sets of the form $S(\sigma)$. Then we come to our main problem, namely, what happens outside the group $\langle \sigma \rangle$; or equivalently, what kind of fields can be found between k and $k_s(\sigma)$. Here we adopt the convention of denoting by $\subset$ the proper inclusion and by $\subseteq$ the im-

Received July 1, 1973

proper inclusion of sets. Our first result in this direction is that if $k \subseteq K \subset k_s(\boldsymbol{\sigma})$ then $\mathscr{G}(k_s/K)$ cannot be topologically generated by less than $e+1$ elements. Second, there does not exist any $\tau \in \mathscr{G}(k_s/k)$ of finite order such that $[k_s(\boldsymbol{\sigma}) : k_s(\boldsymbol{\sigma}, \tau)] < \infty$, and third, if $e = 1$, there does not exist any intermediate field $k \subseteq K \subset k_s(\sigma)$ such that $[k_s(\sigma) : K] < \infty$. The conjecture is that the last statement holds for all e. Finally we consider the centralizer and the normalizer of $\langle \boldsymbol{\sigma} \rangle$ in $\mathscr{G}(k_s/k)$ and we find that in the case were k is a global field, $\langle \boldsymbol{\sigma} \rangle$ is its own centralizer if $e = 1$, and that the centralizer is trivial if $e \geqq 2$. For arbitrary hilbertian field k we prove only that the normalizer of $\langle \boldsymbol{\sigma} \rangle$ in $\mathscr{G}(k_s/k)^e$ is a closed subgroup of infinite index.

Note that if $(\boldsymbol{\sigma})$ is not selected at random then it may happen that it does not have the above properties. For example, for a $\tau \in \mathscr{G}(k_s/k)$ such that $\langle \tau \rangle \cong \hat{Z}$, and for $\sigma = \tau^2$, we have that $[k_s(\sigma) : k_s(\tau)] = 2$. Thus σ is not picked up at random. In fact we prove that the set of all proper powers of the elements of $\mathscr{G}(k_s/k)$ has the measure 0.

In the last two sections we obtain some immediate applications of our results to the problem of finite extensions of a hilbertian field and to finitely generated free pro-finite groups.

1. Fields of finite corank

A subset Σ of a topological group G is said to be *a topological system of generators for* G if the closure of the group generated by Σ is equal to G.

We say that G *has the rank* $\aleph$, where $\aleph$ is a cardinal number, if G has a topological system of generators of cardinality $\aleph$, and does not have such a system of cardinality less than $\aleph$.

If K is a field, then by K_s we denote the separable closure of K and by $\mathscr{G}(K_s/K)$ the Galois group of K_s over K. This group is equipped with the usual Krulj topology.

K is said to have *the corank* $\aleph$ if $\mathscr{G}(K_s/K)$ has the rank $\aleph$.

If Σ is a topological system of generators for $\mathscr{G}(K_s/K)$ then K is the fixed field in K_s of Σ and vice versa. In this case we write $K = K_s(\Sigma)$.

We shall be mainly interested in the case where Σ is a finite set $\Sigma = \{\sigma_1, \cdots, \sigma_e\}$. Then $K_s(\Sigma)$ is said to be *a field of finite corank*. In this case we shall use the notation $k_s(\Sigma) = k_s(\sigma_1, \cdots, \sigma_e) = k_s(\boldsymbol{\sigma})$, where $(\boldsymbol{\sigma})$ stands for the e-tuple $(\sigma_1, \cdots, \sigma_e)$. Some of the simplest properties of fields of a finite corank are given below.

LEMMA 1.1. *A field K has corank* $\leqq e$ *if and only if for every finite Galois extension L of K the group* $\mathcal{G}(L/K)$ *is generated by e elements.*

PROOF. Suppose that $\sigma_1, \cdots, \sigma_e$ are topological generators for $\mathcal{G}(K_s/K)$. Then their restrictions to L, $\sigma_1 \mid L, \cdots, \sigma_e \mid L$ generate $\mathcal{G}(L/K)$.

Conversely, suppose that for every such L the finite set $S(L)$ of all e-tuples $(\sigma_1, \cdots, \sigma_e) \in \mathcal{G}(L/K)^e$ which generate $\mathcal{G}(L/K)$, is not empty. Then the inverse limit $S = \varprojlim S(L)$ (with respect to restrictions) is not empty. Any element of S is a system of e topological generators for $\mathcal{G}(K_s/K)$. Q.E.D.

Denote by F_e the free group generated by e elements. F_e has only a finite number $N_e(n)$ of subgroups of a given index n. This number may be calculated from the recursive relations

$$(1) \qquad N_e(1) = 1, \quad N_e(n) = n(n!)^{e-1} - \sum_{i=1}^{n-1} [(n-i)!]^{e-1} N_e(i)$$

(see Hall [6, p. 190]). We further denote by $NL_e(n)$ the number of normal subgroups of F_e of index n. Obviously we have $NL_e(n) \leqq N_e(n)$.

Consider now an arbitrary group G generated by e elements. Then there exists an epimorphism $\theta : F_e \to G$. The map $H \mapsto \theta^{-1}H$ is an injective map of the set of subgroups H of G of index n into the set of subgroups of F_e of index n. Indeed, if $x_1, \cdots, x_n$ are coset representatives of G modulo H and if $z_1, \cdots, z_n$ are elements of F_e which are mapped by θ onto $x_1, \cdots, x_n$ respectively, then $z_1, \cdots, z_n$ are cosets representatives of F_e modulo $\theta^{-1}H$. If H is a normal subgroup of G then $\theta^{-1}H$ is a normal subgroup of F_e.

Hence we have the following lemma.

LEMMA 1.2. *If a group G is generated by e elements then the number of the subgroups (respectively, the normal subgroup) of G of index n is* $\leqq N_e(n)$ *(respectively,* $\leqq NL_e(n)$*).*

LEMMA 1.3. *If a profinite group G is topologically generated by e elements then the number of its closed subgroups (respectively, closed normal subgroups) of index n is* $\leqq N_e(n)$ *(respectively,* $\leqq NL_e(n)$*).*

PROOF. Let $J_1, \cdots, J_m$ be m distinct closed subgroups of G of index n. Then we can find a normal closed subgroup J of G of finite index which is contained in each of the $J_1, \cdots, J_m$. The quotient group G/J will be a finite group generated by e elements and $J_1/J, \cdots, J_m/J$ will be m distinct subgroups of G/J of index n. By Lemma 1.2,

$m \leqq N_e(n)$. Similarly we prove that in G there are no more than $NL_e(n)$ closed normal subgroups of index n. Q.E.D.

COROLLARY 1.4. *Let K be a field of corank $\leqq e$. Then the number of the separable (respectively, Galois) extensions of K of degree n is $\leqq N_e(n)$ (respectively, $\leqq NL_e(n)$).*

2. The free group and the free profinite group with e generators

Consider the free group F_e with e generators. If we take the family of all normal subgroups N_α of F_e of finite index as a basis of the open neighborhoods of 1 then F_e becomes a topological group. Its completion $\hat{F}_e = \varprojlim F_e/N_\alpha$ is called *the free profinite group with e generators*. There is a canonical topological imbedding of F_e in $\hat{F}_e$ in which every element $x \in F_e$ is mapped into the system $\{xN_\alpha\}$. Thus we shall consider F_e as a topological subgroup of $\hat{F}_e$. If $z_1, \cdots, z_e$ are generators of $\hat{F}_e$ and G is any profinite group generated by e elements $a_1, \cdots, a_e$ then the map $z_1 \mapsto a_1, \cdots, z_e \mapsto a_e$ can be extended to a continuous epimorphism of $\hat{F}_e$ onto G. This property of $\hat{F}_e$ also characterizes it (see, for example, Ribes [15, Sect. 7]). A basis for the open neighborhoods of 1 in $\hat{F}_e$ are all the kernels of the epimorphisms of $\hat{F}_e$ onto finite groups which are generated by e elements (see Ribes [15, p. 23]). It follows that every element of $\hat{F}_e$ can be approximated by a sequence of elements of F_e. If A is any subset of $\hat{F}_e$, then we denote its closure by $\hat{A}$.

LEMMA 2.1. *The map $\gamma : H \mapsto \hat{H}$ is a bijective map of the family $\mathscr{H}$ of all subgroups of F_e of finite index onto the family $\hat{\mathscr{H}}$ of all closed subgroups of $\hat{F}_e$ of finite index. For $H \in \mathscr{H}$ we have $(F_e : H) = (\hat{F}_e : \hat{H})$. Moreover, H is a normal subgroup of F_e if and only if $\hat{H}$ is a normal subgroup of $\hat{F}_e$ and in this case we have an isomorphism $\hat{F}_e/\hat{H} \cong F_e/H$.*

PROOF. (i) The map γ is injective. Every $H \in \mathscr{H}$ is a closed subgroup of F_e. Hence $H = \hat{H} \cap F_e$. It follows that γ is injective.

(ii) If $x_1, \cdots, x_n$ is a system of representatives of F_e modulo a subgroup $H \in \mathscr{H}$ then it is also a system of representatives of $\hat{F}_e$ modulo $\hat{H}$. Indeed, since $H = \hat{H} \cap F_e$, the $x_1, \cdots, x_n$ are distinct modulo H. Thus, we have only to show that each of the elements of $\hat{F}_e$ lies in one of the cosets $\hat{H}x_j$, $1 \leqq j \leqq n$. Indeed, let $z \in \hat{F}_e$; then there exists a sequence of elements $z_i \in F_e$ which converges to z. For every i there exists a $1 \leqq j(i) \leqq n$ and an $h_i \in H$ such that $z_i = h_i x_{j(i)}$. Since $\hat{H}$ is compact we can assume that h_i converges to an element $h \in \hat{H}$, and that

$j(i) = j$ is fixed. Hence after taking the limit we have $z = hx_j$. This proves (ii). It follows from (ii) that:

(iii) For $H \in \mathscr{H}$ we have $(F_e : H) = (\hat{F}_e : \hat{H})$. The first part of the lemma follows now from (i), (iii) and Lemma 1.3, since F_e has exactly $N_e(n)$ subgroups of index n. The second part of the theorem is proved in a similar way. Q.E.D.

We note that Lemma 2.1 does not hold for closed subgroups of infinite index. For example, for $e = 1$, we have $F_1 = \mathbb{Z}$ and $\hat{F}_1 = \hat{\mathbb{Z}} = \Pi\ \hat{\mathbb{Z}}_p$ where $\hat{\mathbb{Z}}_p$ is the additive group of the p-adic integers and it is known that $\mathbb{Z}$ does not have subgroups of infinite index (exept 0) while $\hat{\mathbb{Z}}$ has closed non-trivial subgroups of infinite index.

PROBLEM 1. Is every subgroup of $\hat{F}_e$ of finite index, closed in $\hat{F}_e$?

We prove now the following characterization for the $\hat{F}_e$.

LEMMA 2.2. *Let G be a profinite group of rank $\leqq e$. Then G is topologically isomorphic to $\hat{F}_e$ if and only if G has for every n exactly $N_e(n)$ (respectively, $NL_e(n)$) closed (respectively, closed normal) subgroups of index n.*

PROOF. The necessity of the condition follows from Lemma 2.1. We shall prove that it is also sufficient. Indeed, let G be a profinite group of rank $\leqq e$, and suppose that for every $n \geqq 1$ G has exactly $N_e(n)$ closed subgroups of index n. Then there exists a continuous epimorphism $\theta : \hat{F}_e \to G$. Let $J_{n,j}, j = 1, \cdots, N_e(n)$ be the closed subgroups of G of index n. Put $I_{n,j} = \theta^{-1}(J_{n,j}), j = 1, \cdots, N_{e\,n}$. Then the $I_{n\,j}$ are closed subgroups of $\hat{F}_e$ of index n and they are all distinct. Since $\hat{F}_e$ has exactly $N_e(n)$ closed subgroups of index n, the $I_{n\,j}$ are all of them. Let now $x \in \hat{F}_e$ and suppose that $\theta(x) = 1$. Then $\theta(x) \in J_{n\,j}$ for every $n \geqq 1$ and for every $1 \leqq j \leqq N_e(n)$. Hence x belongs to all the $I_{n.j}$. But this means that x belongs to every subgroup of $\hat{F}_e$ of finite index. Hence $x = 1$.

We have therefore proved that θ is a continuous isomorphism. Since both $\hat{F}_e$ and G are compact and Hausdorff, θ is also a homeomorphism.

One proves the statement concerning the normal subgroups in an analogous way. Q.E.D.

As a corollary we obtain the well-known following result (see Binz, Neukirch, Wenzel [3, p. 108]).

LEMMA 2.3. *If $\hat{J}$ is a closed subgroup of $\hat{F}_e$ of index n then $\hat{J}$ is topologically isomorphic to $\hat{F}_f$ where $f = 1 + n(e-1)$.*

PROOF. By Lemma 2.1, $\hat{J}$ is the closure in $\hat{F}_e$ of a subgroup J of F_e of index n.

The subgroup J is isomorphic, by a theorem of Nielsen and Schreier, to F_f (see Kurosh [9, pp. 28, 36]). Lemma 2.1 then implies that J has exactly $N_f(m)$ closed subgroups of index m for every positive integer m. Hence, by Lemma 2.2, $\hat{J} \cong \hat{F}_f$.

A further application is the following.

THEOREM 2.4. *Let G be a profinite group of rank $\leqq e$. Then G is topologically isomorphic to $\hat{F}_e$ if and only if every finite group with e generators is a continuous homomorphic image of G.*

PROOF. The necessity of the condition is clear. In order to prove its sufficiency we put $N = N_e(n)$ for a fixed positive integer n and let $H_1, \cdots, H_N$ be all the subgroups of F_e of index n. Then $J = H_1 \cap \cdots \cap H_N$ is a normal subgroup of F_e of finite index. By our assumptions there exists a closed normal subgroup J' of G such that $G/J' \cong F_e/J$. Hence there exist N distinct subgroups, $H'_1, \cdots, H'_N$, of G which contain J' such that H_i'/J' corresponds to H_i/J, $i = 1, \cdots, n$, under the isomorphism. The H_j are closed subgroups, since J is such, and they all have the index n in G. Thus the number of the closed subgroups of G of index n is $N_e(n)$. Since this is true for every n we have, by Lemma 2.2, that G is topologically isomorphic to $\hat{F}_e$. Q.E.D.

REMARK. Similar characterizations with analogous proofs hold for the discrete free groups F_e.

3. Symmetric extensions of a hilbertian field

Hilbertian fields are the fields k which have the following property: For every irreducible polynomial $f \in k[T_1, \cdots, T_m, X_1, \cdots, X_n]$ and for every Zariski nonempty open set $U \subseteq S^m$ the set of $(a_1, \cdots, a_m) \in k^m \cap U$ for which $f(a_1, \cdots, a_m, X_1, \cdots, X_n)$ is irreducible in $k[X_1, \cdots, X_n]$ is nonempty. Such sets are called k-hilbertian sets. It is known that if l is a finite separable extension of a hilbertian field k then every l-hilbertian set contains a k-hilbertian set (see Lang [13, p. 152]). Furthermore, let $f \in k[T_1, \cdots, T_m, X]$ be an irreducible polynomial whose Galois group over the field $k(T_1, \cdots, T_m)$ is isomorphic to a group G. It is well known that the set of all the m-tuples $(a_1, \cdots, a_m) \in k^m$ for which $f(a_1, \cdots, a_m, X)$ is irreducible and separable over k with a Galois group G, contains a k-hilbertian set (see Kuyk [10, p. 396]). If the Galois group of f over $l(T_1, \cdots, T_m)$ remains unchanged then we can find an m-tuple $(a_1, \cdots, a_m) \in k^m$ such that the Galois groups of $f(a_1, \cdots, a_m, X)$ over k and l are isomorphic to G (since the intersection of two k-hilbertian sets is never empty). In this case the splitting field l' of $f(a_1, \cdots, a_m, X)$ over k is a Galois extension of k, with a Galois group G, and it is linearly disjoint from l over k. In particular we can consider the general polynomial of degree m,

$$f(T_1, \cdots, T_m, X) = X^m + T_1 X^{m-1} + \cdots + T_m.$$

It is well known that for every field l the Galois group of f over $l(T_1, \cdots, T_m)$ is isomorphic to the symmetric group S_m (see Lang [14, p. 201]). Hence we can construct by induction a sequence of Galois extensions $l_1, l_2, l_3, \cdots$ of k with Galois groups S_m such that l_{i+1} is linearly disjoint from $l_1 \cdots l_i$ over k for every $i \geqq 1$. A sequence of extensions with the last property is said to be linearly disjoint [8, p. 70]. We formulate this result as a lemma.

LEMMA 3.1. *Let k be a hilbertian field and m a positive integer. Then we can construct a linearly disjoint sequence $\{l_i/k\}_{i=1}^{\infty}$ of Galois extensions such that $\mathscr{G}(l_i/k) \cong S_m$ for every i.*

4. The Haar measure of a Galois group

Let k be a field. Then it is well known that the Galois group $\mathscr{G}(k_s/k)$ is compact with respect to its Krull topology. There is, therefore, a unique way to define a Haar measure μ on the Borel field of subsets of $\mathscr{G}(k_s/k)$ such that $\mu(\mathscr{G}(k_s/k)) = 1$. If l is a finite separable extension of k then $\mu(\mathscr{G}(k_s/l)) = 1/[l:k]$. We complete μ by adjoining to the Borel field all the subsets of sets having measure 0 and denote the completion also by μ. More generally, for a positive integer e we shall consider the product space $\mathscr{G}(k_s/k)^e$ and denote by μ^e or μ again the appropriate completion of the power measure. It coincides with the completion of the Haar measure of $\mathscr{G}(k_s/k)^e$.

The following lemma is a generalization of [8, Lemmas 1.9 and 1.10]. Its proof is analogous.

LEMMA 4.1. *Let k be a hilbertian field and let $\{k_i/k\}_{i=1}^{\infty}$ be a linearly disjoint sequence of finite Galois extensions. For each i let $\bar{A}_i$ be a nonempty subset of $\mathscr{G}(k_i/k)^e$ and put $A_i = \{(\sigma) \in \mathscr{G}(k_s/k)^e \mid (\sigma \mid k_i) \in \bar{A}_i\}$. Then the sequence of sets $\{A_i\}_{i=1}^{\infty}$ is independent in the probabilistic sense. If*

$$\sum_{i=1}^{\infty} [k_i : k]^{-e} = \infty$$

then

$$\mu\left(\bigcup_{i=1}^{\infty} A_i\right) = 1.$$

If we combine Lemma 3.1 with Lemma 4.1 we obtain the following lemma.

LEMMA 4.2. *Let $\pi_1, \cdots, \pi_e$ be e elements of S_m, and let k be a hilbertian field. Then for almost all $(\sigma) \in \mathcal{G}(k_s/k)^e$ there exists a continuous epimorphism of $\mathcal{G}(k_s/k)$ onto S_m which maps $\sigma_1, \cdots, \sigma_e$ onto $\pi_1, \cdots, \pi_e$ respectively.*

We shall use the notation $A \approx B$ for two measurable subsets A, B of $\mathcal{G}(k_s/k)^e$ to denote that the symmetric difference of A and B has the measure 0. Similarly $A \lessapprox B$ will mean that $\mu(A - B) = 0$.

We shall frequently use the fact that the intersection of a countable set of sets of measure 1 is again a set of measure 1.

5. The free generators theorem

For a field k and e elements $\sigma_1, \cdots, \sigma_e \in \mathcal{G}(k_s/k)$ we denote by $\langle \sigma_1, \cdots, \sigma_e \rangle$ (or also by $\langle \sigma \rangle$) the closed subgroup of $\mathcal{G}(k_s/k)$ generated by $\sigma_1, \cdots, \sigma_e$. Clearly $\langle \sigma \rangle = \mathcal{G}(k_s/k_s(\sigma))$. The e-tuple (σ) is said to be *topologically free* if $\langle \sigma \rangle$ is topologically isomorphic to $\hat{F}_e$.

If $l \subseteq L$ are two Galois extensions of k and if $(\sigma) \in \mathcal{G}(L/k)^e$ then we denote by $l(\sigma) = l(\sigma_1, \cdots, \sigma_e)$ the fixed field of $(\sigma \mid l)$ in l. It is clear that $l \cap L(\sigma) = l(\sigma)$ and hence that l and $L(\sigma)$ are linearly disjoint over $l(\sigma)$.

Our basic result can now be formulated as follows.

THEOREM 5.1. *Let k be a hilbertian field and let e,f be two positive integers. Then almost all $(\sigma) \in \mathcal{G}(k_s/k)^e$ are topologically free. Furthermore, for almost all $(\sigma, \tau) \in \mathcal{G}(k_s/k)^e \times \mathcal{G}(k_s/k)^f$ we have $k_s(\sigma) \cdot k_s(\tau) = k_s$ and $\langle \sigma \rangle \cap \langle \tau \rangle = 1$.*

PROOF. For a positive integer n let $N_1, \cdots, N_h$, $h = NL_e(n)$, be all the normal subgroups of F_e of index n. Put $N = N_1 \cap \cdots \cap N_h$ and $G = F_e/N$. Then G is a finite group generated by e elements and it contains exactly h normal subgroups of index n. We embed G in a symmetric group S_m and construct, by Lemma 3.1, a linearly disjoint sequence $\{k_i/k\}_{i=1}^{\infty}$ of Galois extensions such that $\mathcal{G}(k_i/k) \cong S_m$ for every i. We can find now for every i an intermediate field $k \subseteq k_i' \subseteq k_i$ such that $\mathcal{G}(k_i/k_i') \cong G$. We choose e generators $\sigma_{i1}, \cdots, \sigma_{ie}$ for $\mathcal{G}(k_i/k_i')$, put

$$T_{ni} = \{(\sigma, \tau) \in \mathcal{G}(k_s/k)^{e+f} \mid (\sigma \mid k_i) = (\sigma_i) \text{ and } (\tau \mid k_i) = (1)\}$$

and let

$$T_n = \bigcup_{i=1}^{\infty} T_{ni}.$$

By Lemma 4.1, T_n has the measure 1 in $\mathcal{G}(k_s/k)^{e+f}$ and its projection on the first e coordinates has the measure 1 in $\mathcal{G}(k_s/k)^e$.

Let now $(\sigma, \tau) \in T_n$. Then there exists an i such that $k_i \subseteq k_s(\tau)$ and $k_s(\sigma) \cap k_i = k_i'$. Hence, if we put $K = k_s(\sigma) \cdot k_i$ we have $K \subseteq k_s(\sigma) \cdot k_s(\tau)$ and $\mathcal{G}(K/k_s(\sigma)) \cong G$. This implies that $K/k_s(\sigma)$ has exactly h Galois subextensions of degree n. Since by Corollary 1.4, $k_s(\sigma)$ has no more then h Galois extensions of degree n altogether, we obtain that all of them are contained in $k_s(\sigma) \cdot k_s(\tau)$.

Let now $T = \bigcap_{n=1}^{\infty} T_n$ and put T' for the projection of T on the first e coordinates. Then T and T' have the measure 1 in $\mathcal{G}(k_s/k)^{e+f}$ and $\mathcal{G}(k_s/k)^e$ respectively. If $(\sigma, \tau) \in T$ then $k_s(\sigma)$ has exactly $NL_e(n)$ Galois extensions of degree n for every n and hence, by Lemma 2.2, $\langle \sigma \rangle$ is topologically isomorphic to $\hat{F}_e$. Furthermore, every finite Galois extension of $k_s(\sigma)$ is contained in $k_s(\sigma) \cdot k_s(\tau)$. Hence $k_s(\sigma) \cdot k_s(\tau) = k_s$. Obviously this means that $\langle \sigma \rangle \cap \langle \tau \rangle = 1$. Q.E.D.

REMARK. Theorem 6.1 can be considered as a generalization of a result of J. Ax[1, p. 177] which states that for almost all $\sigma \in \mathcal{G}(\tilde{Q}/Q)$, $\langle \sigma \rangle \cong \tilde{Z}$.

6. Classes of $(\sigma_1, \dots, \sigma_e)$

The Free Generators theorem implies in particular that if k is a hilbertian field then for almost all the $(\sigma) \in \mathcal{G}(k_s/k)^e$ the groups $\langle \sigma \rangle$ are isomorphic to one another. It may be asked whether the reason for this phenomena is that the fields $k_s(\sigma)$ are already isomorphic to one another. In this section we shall show that this is far from being the case and in fact for each $(\sigma') \in \mathcal{G}(k_s/k)^e$ there exists only a zero set of $(\sigma') \in \mathcal{G}(k_s/k)^e$ such that $k_s(\sigma) \cong_k k_s(\sigma')$. We begin by stating the following lemma.

LEMMA 6.1. *Let k be a field and let (σ), $(\sigma') \in \mathcal{G}(k_s/k)^e$. Then $k_s(\sigma) \cong_k k_s(\sigma')$ if and only if there exists a $\tau \in \mathcal{G}(k_s/k)$ such that $k_s(\sigma) = k_s(\tau\sigma'\tau^{-1})$.*

PROOF. Clear.

If k is a field then we denote by k_{ab} the maximal abelian extension of k.

LEMMA 6.2. *Let k be a hilbertian field and let $\sigma_1, \cdots, \sigma_e \in \mathcal{G}(k_s/k)$. Then $k_{ab}(\sigma)$ is an infinite extension of k.*

PROOF. Assume that $k_{ab}(\sigma)$ is a finite extension of k. Put $m = N_e(2) + 1$ and consider the polynomial $X^2 - X - T$. This is an absolutely irreducible polynomial and it is separable with respect to X. Since k is a hilbertian field we can find $a_1, \cdots, a_m \in k$ such that $X^2 - X - a_j$, $j = 1, \cdots, m$, is irreducible and separable over $k_{ab}(\sigma)$ and such that if b_j is a root of $X^2 - X - a_j$ then the m fields $k_s(\sigma)(b_1), \cdots, k_s(\sigma)(b_m)$ are linearly disjoint over $k_s(\sigma)$ [8, p. 74]. The $b_1, \cdots, b_m$ belong to k_{ab}. Hence the Galois group $\mathscr{G}(k_{ab}/k_{ab}(\sigma))$ has at least m closed subgroups of index 2. But its rank is $\leqq e$. Hence it follows from Lemma 1.3 that $m \leqq N_e(2)$, which is a contradiction.

PROBLEM 2. It is known that if k is a hilbertian field then k_{ab} is also hilbertian (see Kuyk [11, p. 113]). Are the fields $k_{ab}(\sigma)$ hilbertian?

THEOREM 6.3. *Let k be a hilbertian field and let $\sigma_1, \cdots, \sigma_e \in \mathscr{G}(k_s/k)$. Put*

$$S(\sigma) = \{(\sigma') \in \mathscr{G}(k_s/k)^e \mid k_s(\sigma') \cong_k k_s(\sigma)\}.$$

Then $S(\sigma)$ is a closed subset of $\mathscr{G}(k_s/k)^e$ of measure zero.

PROOF. Let (ρ) belong to the closure of $S(\sigma)$ in $\mathscr{G}(k_s/k)^e$. Then for every finite Galois extension L of k there exists $(\sigma') \in S(\sigma)$ such that $(\sigma' \mid L) = (\rho \mid L)$. For (σ') there exists a $\tau \in \mathscr{G}(k_s/k)$ such that $k_s(\sigma) = k_s(\tau\sigma'\tau^{-1})$. Hence $L(\sigma) = L(\tau\sigma'\tau^{-1}) = L(\tau\rho\tau^{-1})$. We conclude that the closed set $T(L)$ of all $\tau \in \mathscr{G}(k_s/k)$ such that

$$L(\sigma) = L(\tau\rho\tau^{-1}) \tag{1}$$

is not empty. It is clear that if $L_1, \cdots, L_m$ is a finite family of finite Galois extensions then

$$T(L_1 \cdots L_m) \subseteq \bigcap_{j=1}^{m} T(L_j).$$

Hence by compactness we can find a $\tau \in \mathscr{G}(k_s/k)$ for which (1) holds for every L. For such a τ we shall have $k_s(\sigma) = k_s(\tau\rho\tau^{-1})$. Hence, by Lemma 6.1, $k_s(\rho) \cong_k k_s(\sigma)$ and thus $(\rho) \in S(\sigma)$.

We have therefore proved that $S(\sigma)$ is closed. In order to prove the rest of the theorem we consider a $(\sigma') \in S(\sigma)$. Hence $k_{ab}(\sigma) = k_{ab}(\tau\sigma'\tau^{-1}) = k_{ab}(\sigma')$ and therefore $(\sigma') \in \mathscr{G}(k_s/k_{ab}(\sigma))$. It follows that $S(\sigma) \subseteq \mathscr{G}(k_s/k_{ab}(\sigma))$. But by Lemma 6.2, $k_{ab}(\sigma)/k$ is an infinite extension, hence $\mu(\mathscr{G}(k_s/k_{ab}(\sigma))) = 0$ and thus $S(\sigma)$ is a zero set. Q.E.D.

The condition $k_s(\sigma) \cong_k k_s(\sigma')$ obviously defines an equivalence relation on the group $\mathscr{G}(k_s/k)^e$ and the $S(\sigma)$ are the equivalence classes modulo this relation. In the following section we shall find how many equivalence classes do exist in $\mathscr{G}(k_s/k)^e$.

7. The number of the classes of the $(\sigma_1,\cdots,\sigma_e)$

Let k be a hilbertian field and let S be a subset of $\mathcal{G}(k_s/k)^e$ of positive measure. Theorem 6.3 implies that there are more than $\aleph_0$ non-equivalent e-tuples $(\boldsymbol{\sigma})$ in S. Therefore, if we accept the continuum hypothesis $2^{\aleph_0} = \aleph_1$, then there are at least $2^{\aleph_0}$ non-equivalent e-tuples in S. In what follows we prove this fact without assuming the continuum hypothesis.

THEOREM 7.1. *Let k be a hilbertian field and let S be a subset of $\mathcal{G}(k_s/k)^e$ of positive measure. Then there are at least $2^{\aleph_0}$ non-equivalent e-tuples in S.*

PROOF. By the regularity of the Haar measure we can find a closed subset of S having a positive measure. Hence we can assume, without loss of generality, that S itself is already closed.

We construct, as in the proof of Lemma 6.2, two sequences $a_1, a_2, a_3, \cdots \in k$ and $b_1, b_2, b_3, \cdots \in k_s$, such that $b_i^2 - b_i - a_i = 0$, $[k(b_i):k] = 2$ for $i \geqq 1$, and such that the sequence of fields $\{k(b_i)\}_{i=1}^{\infty}$ is linearly disjoint over k. For every $i \geqq 1$ we put

$$A_i = \mathcal{G}(k_s/k_i)^e \qquad B_i = \mathcal{G}(k_s/k)^e - \mathcal{G}(k_s/k_i)^e.$$

These are closed sets in $\mathcal{G}(k_s/k)^e$ and we have

$$\mu(A_i) = \frac{1}{2^e} \qquad \mu(B_i) = 1 - \frac{1}{2^e}.$$

Further we denote by C_i a variable which assumes either the value A_i or the value B_i. It follows from our construction and by Lemma 4.1 that every sequence of the form $(C_1, C_2, C_3, \cdots)$ is independent in the probabilistic sense.

ASSERTION. There exists an i_1 such that for every $i \geqq i_1$,

$$\mu(S \cap A_i) > 0 \quad \text{and} \quad \mu(S \cap B_i) > 0.$$

Indeed, if such an i_1 did not exist we could have found for every positive integer n a set I of n positive integers such that for every $i \in I$

$$\mu(S \cap A_i) = 0 \quad \text{or} \quad \mu(S \cap B_i) = 0$$

and hence that

$$S \precsim B_i \qquad \text{or} \qquad S \precsim A_i.$$

Hence $S \precsim \bigcap_{i \in I} C_i$ for a certain n-tuple $\{C_i \mid i \in I\}$. Therefore we would have

$$\mu(S) \leqq \mu\Big(\bigcap_{i \in I} C_i\Big) = \prod_{i \in I} \mu(C_i) \leqq \Big(1 - \frac{1}{2^e}\Big)^n.$$

This inequality would have to hold for every n, hence we would obtain that $\mu(S) = 0$, which is a contradiction.

By applying the same assertion to $S \cap A_{i_1}$ and to $S \cap B_{i_1}$ we can deduce that there exists an $i_2 > i_1$ such that for every $i \geqq i_2$,

$$\mu(S \cap A_{i_1} \cap A_i) > 0 \quad \text{and} \quad \mu(S \cap A_{i_1} \cap B_i) > 0$$

$$\mu(S \cap B_{i_1} \cap A_i) > 0 \quad \text{and} \quad \mu(S \cap B_{i_1} \cap B_i) > 0.$$

Proceeding this way we find a sequence $i_1 < i_2 < i_3 < \cdots$ of positive integers such that $\mu(S \cap C_{i_1} \cap \cdots \cap C_{i_n}) > 0$ and hence $S \cap C_{i_1} \cap \cdots \cap C_{i_n} \neq \emptyset$ for every $n \geqq 1$ and for every n-tuple $(C_{i_1}, \cdots, C_{i_n})$. All the sets involved are closed, hence it follows by the compactness of $\mathcal{G}(k_s/k)^e$, that $S \cap \bigcap_{n=1}^{\infty} C_{i_n} \neq \emptyset$ for every sequence $(C_{i_1}, C_{i_2}, C_{i_3}, \cdots)$.

Let now $(C_{i_1}, C_{i_2}, C_{i_3}, \cdots)$ and $(C'_{i_1}, C'_{i_2}, C'_{i_3}, \cdots)$ be two distinct sequences and let

$$(\sigma) \in S \cap \bigcap_{n=1}^{\infty} C_{i_n}, \qquad (\sigma') \in S \cap \bigcap_{n=1}^{\infty} C'_{i_n}.$$

Then there exists an n such that $C_{i_n} \neq C'_{i_n}$. Suppose, for example, that $C_{i_n} = A_{i_n}$ and that $C'_{i_n} = B_{i_n}$. Then the equation $X^2 - X - a_i = 0$ has a solution in $k_s(\sigma)$ but none in $k_s(\sigma')$. It follows that these fields are not isomorphic over k.

There are $2^{\aleph_0}$ distinct sequences of C. Hence there are at least $2^{\aleph_0}$ non-equivalent (σ) in S. Q.E.D.

COROLLARY 7.2. *If k is a hilbertian field then there are at least $2^{\aleph_0}$ non-equivalent e-tuples (σ) in $\mathcal{G}(k_s/k)^e$ which are topologically free.*

We apply now Theorem 7.1 to a problem in model theory. Denote by T the theory of all the elementary statements which hold in almost all finite fields. Then it follows from [8, 3.5] and Ax[2, Th. 9] that $\tilde{Q}(\sigma)$ is a model of T for almost all $\sigma \in \mathcal{G}(\tilde{Q}/Q)$. Hence, by Theorem 7.1, there are at least $2^{\aleph_0}$ non-isomorphic models for T among the $\tilde{Q}(\sigma)$. Since their number can not exceed $2^{\aleph_0}$ it is exactly $2^{\aleph_0}$. Thus we have proved the following theorem.

THEOREM 7.3. *The theory of all elementary statements which hold in almost all finite fields has exactly $2^{\aleph_0}$ non-isomorphic models which are algebraic over Q.*

8. Elementary properties of the group $\mathcal{G}(k_s/k)$

The Free Generators theorem implies in particular that if $w(X_1, \cdots, X_e)$ is a nonempty reduced word (in the sense of group theory) and k is a hilbertian field then for almost all $(\sigma_1, \cdots, \sigma_e) \in \mathcal{G}(k_s/k)^e$, $w(\sigma_1, \cdots, \sigma_e) \neq 1$. We wish now to generalize this result. In order to do it we consider the first order calculus language of the theory of groups. A *normal perinex formula* is a formula of the form $Q_1X_1 \cdots Q_mX_m \, \Psi(X_1, \cdots, X_e)$ $(e \leqq n)$, where each Q_i is either the existential quantifier $\exists$ or the universal quantifier $\forall$. A *negative formula* is a formula which is logically equivalent to a normal perinex formula of the above form, in which $\Psi(X_1, \cdots, X_n)$ is a disjunction of inequalities. For example

$$\exists X_1 \forall X_2 \exists X_3 [X_1 X_2^{-1} \neq X_4 \vee [X_3 X_2 \neq X_5 \wedge X_6^{-1} X_5 X_8 \neq X_8 X_5]]$$

is a negative formula. It is easy to prove by induction on the number of the quantifiers that if $\phi(X_1, \cdots, X_e)$ is a negative formula in the free variables $X_1, \cdots, X_e$, if G' is a homomorphic image of a group G, if $a_1, \cdots, a_e$ are elements of G and $a_1', \cdots, a_e'$ are their images in G', then

$$G \models \phi\,(a_1, \cdots, a_e) \Rightarrow G' \models \phi(a_1', \cdots, a_e').$$

("$G = \phi$" means "ϕ holds in G".)

THEOREM 8.1. *Let k be a hilbertian field and let $\phi(X_1, \cdots, X_e)$ be a negative formula in the free variables $X_1, \cdots, X_e$. Suppose that there exists a positive integer m such that*

$$S_m \models \exists X_1 \cdots \exists X_e : \phi(X_1, \cdots, X_e);$$

then

$$\mathcal{G}(k_s/k) \models \phi(\sigma_1, \cdots, \sigma_e)$$

for almost all $(\sigma_1, \cdots, \sigma_e) \in \mathcal{G}(k_s/k)^e$.

PROOF. Let $\pi_1, \cdots, \pi_m$ be elements of S_m such that $S_m \models \phi(\pi_1, \cdots, \pi_e)$. Then, by Lemma 4.2, there is for almost every $(\sigma_1, \cdots, \sigma_e) \in \mathcal{G}(k_s/k)^e$ an epimorphism of $\mathcal{G}(k_s/k)$ onto S_m which maps $\sigma_1, \cdots, \sigma_e$ onto $\pi_1, \cdots, \pi_e$ respectively. Hence by the above remark we have that $\mathcal{G}(k_s/k) \models \phi(\sigma_1, \cdots, \sigma_e)$. Q.E.D.

By applying Theorem 8.1 to specific negative formulas we obtain the following corollary.

COROLLARY 8.2. *Let k be a hilbertian field.*

(i) *If $w(X_1, \cdots, X_e)$ is a nonempty reduced word then $w(\sigma_1, \cdots, \sigma_e) \neq 1$ for almost all $(\sigma) \in \mathcal{G}(k_s/k)^e$.*

(ii) *For almost all* $(\sigma,\tau) \in \mathcal{G}(k_s/k)^2$ *we have that* $\sigma\tau \neq \tau\sigma$.

(iii) *The set of all nontrivial powers of the elements of* $\mathcal{G}(k_s/k)$ *is of measure zero.*

(iv) *Almost no two elements of* $\mathcal{G}(k_s/k)$ *are conjugate to each other.*

PROOF. (i) It is known that there exists an m such that $w(X_1,\cdots,X_e) = 1$ is not an identity in S_m (refer to Kurosh [9, p. 42]). The corresponding negative formula is $w(X_1,\cdots,X_e) \neq 1$.

(ii) This is a consequence of (i) for the special case in which $w(X_1, X_2) = X_1X_2X_1^{-1}X_2^{-1}$.

(iii) Let $n > 1$ be an integer and consider the cycle $(1 \cdots n)$ in S_n. For this cycle we have $(1 \cdots n)^n = 1$. This implies that the map $x \mapsto x^n$ of S_n into itself is not injective, hence it is also not surjective. It follows that S_n contains an element x such that $S_n \models \forall Y : Y^n \neq x$. Theorem 8.1 therefore implies that the set of all n-powers in $\mathcal{G}(k_s/k)$ is a zero set. If we take the union over all $n \geqq 2$ we obtain that almost no element of $\mathcal{G}(k_s/k)$ is a nontrivial power.

(iv) This follows from the fact that, for example, in S_2, $x_1 = (1)$ and $x_2 = (1\ 2)$ are not conjugate, that is, $S_2 \models \forall Y : Yx_1Y^{-1} \neq x_2$. We note that this result can also be derived from Theorem 6.3.

PROBLEM 3. Let $\phi(X_1,\cdots,X_e)$ be an arbitrary formula of the first order language of the theory of groups with the free variables $X_1,\cdots,X_n$. Let k be a hilbertian field. Is it true that the subset

$$\{(\boldsymbol{\sigma}) \in \mathcal{G}(k_s/k)^e \,|\, \mathcal{G}(k_s/k) \models \phi(\sigma_1,\cdots,\sigma_e)\}$$

of $\mathcal{G}(k_s/k)^e$ is measurable?

9. The Bottom theorem

Corollary 8.2 (iii) states that if k is a hilbertian field, then for almost no $\sigma \in \mathcal{G}(k_s/k)$ there exists a $\tau \in \mathcal{G}(k_s/k)$ and an integer $n > 1$ such that $\tau^n = \sigma$. In this section we intend to generalize this result, first by considering e-tuples of elements of $\mathcal{G}(k_s/k)$ rather then the elements themselves and second by letting the σ_i be in the closed subgroup generated by the τ_i rather then in the discrete group generated by them. More precisely, we prove the following theorem.

THEOREM 9.1. *Let k be a hilbertian field. Then for almost all* $(\boldsymbol{\sigma}) \in \mathcal{G}(k_s/k)^e$ *there does not exist a* $(\boldsymbol{\tau}) \in \mathcal{G}(k_s/k)^e$ *such that* $k_s(\boldsymbol{\tau})$ *is properly contained in* $k_s(\boldsymbol{\sigma})$.

PROOF. We begin our proof by introducing certain maps attached to elements of $\hat{F}_e$ and profinite groups. Let $z_1, \cdots, z_e$ be free topological generators of $\hat{F}_e$. For every e-tuple $(v) \in \hat{F}_e{}^e$and every profinite group G we define a map $v_G : G^e \to G^e$ in the following way: Let $(a) \in G^e$; then there exists a unique continuous homomorphism $\theta_a : \hat{F}_e \to G$ which maps $z_1, \cdots, z_e$ onto $a_1, \cdots, a_e$ respectively. We set

$$v_G(a) = (\theta_a(v_1), \cdots, \theta_a(v_e)).$$

ASSERTION 1. If H is a closed subgroup of G and if $a_1, \cdots, a_e \in H$, then θ_a maps $\hat{F}_e$ into H. Hence $v_G \,|\, H^e = v_H$.

PROOF. Clear.

ASSERTION 2. If π is a continuous homomorphism of G into a profinite group $\bar{G}$ then the following diagram is commutative.

$$\begin{array}{ccc} G^e & \xrightarrow{\;v_G\;} & G^e \\ {\scriptstyle \pi^e}\downarrow & & \downarrow{\scriptstyle \pi^e} \\ \bar{G}^e & \xrightarrow{\;v_{\bar{G}}\;} & \bar{G}^e \end{array}$$

PROOF. Let $(a) \in G^e$ and let $(\bar{a}) = \pi^e(a)$. The continuous homomorphism $\pi \cdot \theta_a : \hat{F}_e \to \bar{G}$ satisfies the relation $(\pi \cdot \theta_a)^e(z) = (\bar{a})$. Hence $\pi \cdot \theta_a = \theta_{\bar{a}}$ and we have

$$v_{\bar{G}}(\pi^e(a) = v_{\bar{G}}(\bar{a}) = \theta^e_{\bar{a}}(v) = \pi^e(\theta^e_a(v)) = \pi^e(v_G(a)),$$

that is,

$$v_{\bar{G}} \cdot \pi^e = \pi^e \cdot v_G.$$

ASSERTION 3. The map v_G is continuous.

PROOF. Let $(a) \in G^e$ and put $(b) = v_G(a)$. Consider an open neighborhood V of (b). V must contain a set of the form $V' = \{(b') \in G^e \,|\, \pi^e(b') = \pi^e(b)\}$, where π is a continuous epimorphism of G onto a finite group $\bar{G}$. The set $U = \{(a') \in G^e | \pi^e(a') = \pi^e(a)\}$ is an open neighborhood of (a), and Assertion 2 implies that it is mapped by v_G into V'. Hence v_G is indeed continuous.

For every positive integer m we set $v_m = v_{S_m}$.

ASSERTION 4. If the maps v_m are surjective for every positive integer m then the maps v_G are bijective for every profinite group G.

PROOF. Let G be a finite group. Then G may be considered as a subgroup of S_m for some m. Since S_m^e is a finite set, our assumption implies that v_m is injective. Therefore, by Assertion 1, $v_G = v_m \,|\, G$ is injective and hence also surjective.

Consider now an arbitrary profinite group G. Let (a), $(a') \in G^e$ be two distinct elements. Then there exists a continuous epimorphism π of G onto a finite group $\bar{G}$ such that $\pi^e(a) \neq \pi^e(a')$. It follows, by what we have proved, that $v_{\bar{G}}(\pi^e(a)) \neq v_{\bar{G}}(\pi^e(a'))$. Hence, by Assertion 2, $v_G(a) \neq v_G(a')$. This means that v_G is injective. We now prove that it is also surjective. Let $(b) \in G^e$ and let π be a continuous epimorphism of G onto a finite group $\bar{G}$. Then there exists an $(\bar{a}) \in \bar{G}^e$ such that $v_{\bar{G}}(\bar{a}) = \pi^e(b)$. Choose now an element $(a) \in G^e$ such that $\pi^e(a) = (\bar{a})$. Then, by Assertion 2, we have that $\pi^e(v_G(a)) = \pi^e(b)$. This argument implies that (b) is contained in the closure of the set $v_G(G^e)$. But this set is closed since G^e is compact and Haussdorf and v_G is continuous. Hence $(b) \in v_G(G^e)$. Thus v_G is surjective.

ASSERTION 5. If the maps v_m are surjective for every positive integer m, G is a profinite group, $(a) \in G^e$ and $(b) = v_G(a)$ then $\langle a \rangle = \langle b \rangle$.

PROOF. Assertion 1 implies that $\langle b \rangle \subseteq \langle a \rangle$. Conversely, Assertion 4 implies that the map $v_{\langle b \rangle}$ is surjective. Hence there exists an $(a') \in \langle b \rangle^e$ such that $v_{\langle b \rangle}(a') = (b)$. Thus, by Assertion 1, $v_G(a') = v_G(a)$. But v_G is injective, by Assertion 4, hence $(a') = (a)$. Hence $(a) \in \langle b \rangle^e$, which completes the proof of our assertion.

We come now to the proof of our theorem itself.

We put $\mathscr{G} = \mathscr{G}(k_s/k)$ and we denote by S the set of all $(\sigma) \in \mathscr{G}^e$ for which there exists a $(\tau) \in \mathscr{G}^e$ such that $k_s(\tau) \subset k_s(\sigma)$. For every positive integer m and every $(b) \in S_m^e$ we denote by $S(b)$ the set of all $(\sigma) \in \mathscr{G}^e$ for which there does not exist a continuous epimorphism of $\mathscr{G}$ onto S_m which maps (σ) onto (b). By Lemma 4.2, $S(b)$ has the measure 0. Since there are only a countable number of $S(b)$ it suffices to show that S is contained in the union of the $S(b)$.

Let $(\sigma) \in S$. Then there exists a $(\tau) \in \mathscr{G}^e$ such that $k_s(\tau) \subset k_s(\sigma)$. Let θ_τ be the continuous homomorphism of $\hat{F}_e$ into $\mathscr{G}$ which maps $z_1, \cdots, z_e$ onto $\tau_1, \cdots, \tau_e$ respectively. The homomorphism θ_τ maps $\hat{F}_e$ onto $\langle \tau \rangle$. Hence there exists a $(v) \in \hat{F}_e^e$ such that $\theta_\tau^e(v) = (\sigma)$, that is, that $v_{\mathscr{G}}(\tau) = (\sigma)$. The groups $\langle \sigma \rangle$ and $\langle \tau \rangle$ are not equal, hence there exists by Assertion 5, a positive integer m such that the map v_m is not surjective. For this m there exists a $(b) \in S_m^e - v_m(S_m^e)$. For this (b) there does not exist a continuous epimorphism π of $\mathscr{G}$ onto S_m which maps (σ) onto (b), because otherwise we would have had

$$(b) = \pi^e(\sigma) = \pi^e(v_{\mathscr{G}}(\tau)) = v_m(\pi^e(\tau)) \in v_m(S_m^e)$$

which is a contradiction. Therefore $(\sigma) \in S(b)$. Q.E.D.

10. Substitutions in irreducible polynomials

Consider again a $(\sigma) \in \mathscr{G}(k_s/k)^e$ selected at random. We already know that $k_s(\sigma)$ contains no proper subfields K containing k of corank $\leqq e$. It certainly contains fields having higher corank. However we want to show that if their index is finite then their Galois groups are torsion free. Since elements of finite order of $\mathscr{G}(k_s/k)$ are strongly connected with formal real fields we must develop some technique to handle irreducible polynomials over hilbertian formal real fields. In particular we prove that if k is a hilbertian ordered field then its hilbertian sets are dense in k^r with respect to the order topology.

We begin by proving a rather general lemma.

LEMMA 10.1 (W.D.Geyer). *Let $F(T, X)$ be an irreducible polynomial in the variables $(T, X) = (T, X_1, \cdots, X_n)$ over a field k, and let $g(Y)$ be a nonconstant polynomial with coefficients in k in the variables $(Y) = (Y_1, \cdots, Y_m)$. Assume that $g(Y) - c$ is absolutely irreducible for every $c \in \tilde{k}$. Then the polynomial $F(g(Y), X)$ is irreducible in $k[X, Y]$.*

PROOF. If T does not appear in $F(T, X)$ then the statement is obvious. We therefore suppose that the degree of $F(T, X)$ in T is positive.

Let V be the k-algebraic set defined in the affine space S^{1+n+m} by the equations $F(T, X) = 0$ and $g(Y) = T$. This set is not empty. Moreover the polynomial $g(Y) - T$ does not vanish on the variety $V(F)$. Hence by the Dimension theorem (see Lang [12, p. 36]) we have that all k-components of V have dimension $n + m - 1$. Let now (t, x, y) and (t', x', y') be two points of V having dimension $n + m - 1$ over k. Then $\dim_k(x) = \dim_k(x') = n$. Hence, since $F(T, X)$ is irreducible there exists a k-isomorphism $\theta_0 : k(t, x) \to k(t', x')$ for which $\theta_0(t) = t'$ and $\theta_0(x_i) = x_i'$, $i = 1, \cdots, n$. Again, since $\dim_{k(t,x)}(y) = \dim_{k(t',x')}(y') = m - 1$, and $g(Y) - t$ is irreducible over $k(t, x)$ we can extend θ_0 to an isomorphism $\theta : k(t, x, y) \to k(t', x', y')$ such that $\theta(y_j) = y_j'$, $j = 1, \cdots, m$. This means that V has only one k-component, that is, V is irreducible over k.

Consider now a generic point (t, x, y) of V over k. Then (x, y) is a generic point of the projection V' of V on the space S^{n+m} in the variables (X, Y). Since $t = g(y)$ we have that $\dim V' = \dim V = n + m - 1$. V' is therefore a k irreducible hypersurface in S^{n+m}. Hence there exists an irreducible polynomial $H \in k[X, Y]$ which generates the ideal of all polynomials in $k[X, Y]$ which vanish on V' (see Weil [18, p. 74]). It is clear that H vanishes on the algebraic set defined by the equation $F(g(y), X) = 0$; hence, by Hilbert Nullstellensatz, we have an equation of the form

$$H(X, Y)^r = F(g(Y), Y)G(X, Y)$$

where $r \geqq 1$ and $G \in k[X, Y]$. Since $H(X, Y)$ is irreducible there exists an $1 \leqq s \leqq r$ such that

$$F(g(Y), X) = H(X, Y)^s. \tag{1}$$

If $s = 1$ we are done. Suppose therefore that $s > 1$. Then (1) implies

$$\frac{\partial F}{\partial X_i}(t, x) = sH(x, y)^{s-1}\frac{\partial H}{\partial X_i}(x, y) = 0 \qquad i = 1, \cdots, n \tag{2}$$

$$\frac{\partial F}{\partial T}(t, x)\frac{\partial g}{\partial Y_j}(y) = sH(x, y)^{s-1}\frac{\partial H}{\partial Y_j}(x, y) = 0 \qquad j = 1, \cdots, m. \tag{3}$$

But (t, x) is a generic point of the k-variety defined by the irreducible polynomial $F(T, X)$ in S^{1+n}. Hence it follows from (2) that $\partial F/\partial T(t, x) \neq 0$. On the other hand since $y_1, \cdots, y_m$ are algebraically independent over k and $g(Y)$ is irreducible, there exists a $1 \leqq j \leqq m$ such that $\partial g/\partial Y_j(y) \neq 0$. This contradicts (3).

Q.E.D

We generalize Lemma 10.1 as follows.

LEMMA 10.2. *Let k be a field and let $F \in k(T_1, \cdots, T_r)[X_1, \cdots, X_n]$ be an irreducible polynomial. Let $g_i \in k[Y_{i1}, \cdots, Y_{im}]$, $i = 1, \cdots, r$, be nonconstant polynomials for which $g_i(Y_i) + c$ is absolutely irreducible for every $c \in \tilde{k}$. Then the polynomial $F(g(Y), X) = F(g_1(Y_1), \cdots, g_r(Y_r), X_1, \cdots, X_n)$ is defined and irreducible in $k(Y)[X]$.*

PROOF. (i) Assume first that $F \in k[T_1, \cdots, T_r, X_1, \cdots, X_n]$ is an irreducible polynomial. In this case we can substitute successively $T_r = g_r(Y_r)$, $T_{r-1} = g_{r-1}(Y_{r-1}), \cdots, T_1 = g_1(Y_1)$ and obtain from Lemma 10.1 in r steps that $F(g(Y), X)$ is irreducible in $k[Y, X]$.

(ii) In the general case we can write F in the form

$$F(T, X) = \frac{G(T)}{H(T)}F_1(T, X)$$

where $G, H \in k[T]$ are nonzero polynomials and $F_1 \in k[T, X]$ is irreducible. It is clear that $G(g(Y)), H(g(Y)) \neq 0$. Hence, by (i), $F(g(Y), X)$ is defined and irreducible in $k(Y)[X]$.

In particular we can choose $g_i(Y_i) = Y_{i1}^2 + Y_{i2}^2 + Y_{i3}^2$. If $\mathrm{char}(k) \neq 2$, then $g_i(Y_i) + c$ is absolutely irreducible for every $c \in \tilde{k}$. Hence, as a corollary of Lemma 10.2, we have the following lemma.

LEMMA 10.3. *Let k be a field with* $\mathrm{char}(k) \neq 2$ *and let* $F \in k(T_1, \cdots, T_r)[X_1, \cdots, X_n]$ *be an irreducible polynomial. Then the polynomial*

$$F\left(\sum_{j=1}^{3} Y_{1j}^2, \cdots, \sum_{j=1}^{3} Y_{rj}^2, X_1, \cdots, X_n\right)$$

is defined and irreducible in $k(Y)[X]$.

11. Formal real fields

LEMMA 11.1. *Let k be a hilbertian formal real field, and let H be a hilbertian set in k^r. Then for every $2r$ rational numbers $a_1 < b_1, \cdots, a_r < b_r$ there exists a point $(z_1, \cdots, z_r) \in H$ such that in every ordering of k we have $a_i < z_i < b_i$ for $i = 1, \cdots, r$.*

PROOF. For convenience we prove the lemma only for the case $r = 1$, the proof of the general case is analogous.

We are given irreducible polynomials $F_\lambda \in k(T)[X_1, \cdots, X_n]$, $\lambda = 1, \cdots, l$, and two rational numbers $a < b$. Put $c = 1/(b - a)$. Then the polynomials $F_\lambda(a+(1/(c + T), X)$ are also irreducible in $k(T)[X]$. By Lemma 10.3 the polynomials $F_\lambda(a+(1/(c + Y_1^2 + Y_2^2 + Y_3^2)), X)$ are defined and irreducible in $k(Y)[X]$. Therefore there exist $y_1, y_2, y_3 \in k$, $y_1 \neq 0$, such that the polynomials $F_\lambda(a + (1/(c + y_1^2 + y_2^2 + y_3^2)), X)$ are defined and irreducible in $k[X]$. Put $z = a + (1/(c + y_1^2 + y_2^2 + y_3^2))$. Then $a < z < b$ in every ordering of k and the $F_\lambda(z, X)$ are defined and irreducible in $k[X]$. Q.E.D.

We use Lemma 11.1 to construct a special linearly disjoint sequence of extensions of k.

LEMMA 11.2. *Let k be a hilbertian formal real field and let $m \geqq 2$ be an integer. Then there exists a linearly disjoint sequence $\{k_i/k\}_{i=1}^{\infty}$ of Galois extensions such that for every i, $\mathscr{G}(k_i/k) = S_m$ and k_i/k has an absolutely imaginary quadratic subextension k_i'/k.*

PROOF. It is sufficient to prove that for every finite extension L of k there exists a Galois extension K/k which is linearly disjoint from L/k and which contains a quadratic absolutely imaginary subextension K'/k.

Let $\Delta(T)$ be the discriminant of the general polynomial of degree m, $f(T, X) = X^m + T_1 X^{m-1} + \cdots + T_m$. Let

$$f(c, X) = (X^2 + 2) \prod_{i=1}^{m-2} (X - i) = X^m + c_1 X^{m-1} + \cdots + c_m.$$

Then the c_i are integers and $\Delta(c) < 0$. Since $\Delta(T)$ is a polynomial with integral coefficients there exist rational numbers $a_i < b_i$, $i = 1, \cdots, m$, such that for every ordering of k and for every $z_1, \cdots, z_m \in k$ which satisfy $a_i < z_i < b_i$ in this ordering we have $\Delta(z) < 0$. (In fact it is sufficient to choose the a_i and the b_i in such a way that the statement will hold for z_i real, since every real closed field is elementarily equivalent to the field of real numbers.)

By section 3 and Lemma 11.1, we can choose $z_1, \cdots, z_m \in k$ such that the Galois group of the polynomial $f(z, X)$ is isomorphic to S_m both over k and over L, and that $a_i < z_i < b_i$, $i = 1, \cdots, m$, for every ordering of k. Let K be the splitting field of $f(z, X)$ over k. Then $\mathcal{G}(K/k) \cong S_m$, K is linearly disjoint from L over k and it contains the absolutely imaginary quadratic extension $k(\sqrt{\Delta(z)})$ of k.

Q.E.D.

12. Excluding the case of elements of finite order

We need the following group theoretic lemma.

LEMMA 12.1 (J. Ritter, S. Böge). *Let p be an odd prime, let c be the cycle $(1\ 2 \cdots p)$ in S_p, and let N be the normalizer of $\langle c \rangle$ in S_p. If π is an element of N of order 2 then $\pi \in A_p$ if and only if $p \equiv 1 \pmod 4$.*

PROOF. By assumption there exists a $1 \leqq i \leqq p - 1$ such that $\pi^{-1} c \pi = c^i$. Since $c^i(x) \equiv x + i \pmod p$ for every x we have that $\pi^{-1}(1 + \pi(x)) \equiv x + i \pmod p$ for every x. Hence $\pi(x + zi) \equiv z + \pi(x) \pmod p$ for every x and z. Therefore, if a satisfies $ai \equiv 1 \pmod p$ we have that $\pi(x + l) = la + \pi(x) \pmod p$ for every x and l. In particular if we put $b = \pi(1) - \pi(a)$ we have that

$$\pi(y) \equiv ay + b \pmod p \qquad \forall y. \tag{1}$$

Conversely, it is easy to verify that if $1 \leqq a \leqq p - 1$ and b is arbitrary then π, which is defined by (1), belongs to N.

Let therefore π be of the form (1) and let s be the order of a modulo p. Then the permutation $x \mapsto ax \pmod p$ is the product of $(p - 1)/s$ cycles of length s (and one cycle of length 1, namely (p)). Its sign must be

$$(-1)^{(s-1)(p-1)/s}.$$

Furthermore, the permutation $y \mapsto y + b \pmod p$ is a cycle of either length p or 1, hence it is an even permutation (since $p \neq 2$). It follows that

$$\text{sign}(\pi) = (-1)^{(s-1)(p-1)/s}.$$

If π is of order 2 then $s = 2$ and our lemma follows immediately from the formula

$$\mathrm{sign}(\pi) = (-1)^{(p-1)/2}. \qquad \text{Q.E.D.}$$

REMARK. It follows from the proof that the order of N is $p(p-1)$, hence its index in S_p is $(p-2)!$

THEOREM 12.2. *Let k be a hilbertian field. Then for almost every $(\sigma) \in \mathcal{G}(k_s/k)_e$ there does not exist a $\tau \in \mathcal{G}(k_s/k)$, $\tau \neq 1$, of finite order such that $[k_s(\sigma) : k_s(\sigma, \tau)] < \infty$.*

PROOF. By the Artin-Schreier theorem, we have to prove the theorem only for the case where k is a formal real field, $\tau^2 = 1$ and $\tau \neq 1$ (see Lang [14, p. 223]). Moreover, it suffices to prove that the following statement holds for every positive integer n.

For almost every $(\sigma) \in \mathcal{G}(\tilde{k}/k)^e$ there does not exist a $\tau \in \mathcal{G}(\tilde{k}/k)$ such that $\tau^2 = 1$, $\tau \neq 1$ and $[\tilde{k}(\sigma) : \tilde{k}(\sigma, \tau)] = n$.

We choose a prime $p \equiv 1 \pmod 4$, $p \geqq n$, and consider for this p the sequence $\{k_i/k\}_{i=1}^{\infty}$ which was constructed in Lemma 11.2. For every i we denote by ρ_i the element of $\mathcal{G}(k_i/k)$ which corresponds to the cycle $(1\ 2 \cdots p)$ under the isomorphism $\mathcal{G}(k_i/k) = S_p$. Let S be the set of all the $(\sigma) \in \mathcal{G}(\tilde{k}/k)^e$ for which there exists an i such that $\sigma_1 \mid k_i = \cdots = \sigma_e \mid k_i = \rho_i$. By Lemma 4.1, this set has the measure 1. We prove that every element in S has the desired property.

Let $(\sigma) \in S$ and assume that there exists a $\tau \in \mathcal{G}(\tilde{k}/k)$ such that $\tau^2 = 1$, $\tau \neq 1$ and $[\tilde{k}(\sigma) : \tilde{k}(\sigma, \tau)] = n$. Then $\tilde{k}(\tau)$ is a real closed field (see Lang [14, p. 274]). Let L be smallest normal extension of $\tilde{k}(\sigma, \tau)$ which contains $\tilde{k}(\sigma)$. Then $[L : \tilde{k}(\sigma, \tau)]$ divides $n!$ and hence $[L : \tilde{k}(\sigma)]$ divides $(n-1)!$ Hence p does not divide $[L : \tilde{k}(\sigma)]$. We know that there exists an i such that $\sigma_1 \mid k_i = \cdots = \sigma_e \mid k_i = \rho_i$. For this i we certainly have $\tilde{k}(\sigma) \cap k_i(\rho_i) = k_i$. For if $L \cap k_i$ were a proper extension of $k_i(\rho_i)$, we would have that $L \cap k_i = k_i$ and hence that p divides $[L : \tilde{k}(\sigma)]$, which is a contradiction.

Put now $\bar{\tau} = \tau \mid k_i$. Then $\bar{\tau}^2 = 1$ and $k_i(\rho_i)$ is a normal extension of $k_i(\rho_i, \bar{\tau})$, that is, $\bar{\tau}$ belongs to the normalizer of $\langle \rho_i \rangle$. By Lemma 12.1, it follows that in the isomorphism $\mathcal{G}(k_i/k) \cong S_p$, $\bar{\tau}$ corresponds to an element of A_p. The subgroup of $\mathcal{G}(k_i/k)$ which corresponds to A_p fixes the field k_i', since this field is the only quadratic subextension of k_i/k. Hence $\bar{\tau} \in \mathcal{G}(k_i/k_i')$. This means that $k_i' \subset \tilde{k}(\tau)$, which contradicts the fact that k_i' is an absolutely imaginary quadratic extension of k and $\tilde{k}(\tau)$ is a real closed field. It follows that such a τ does not exist. Q.E.D.

13. The Bottom conjecture

THEOREM 9.1 and 12.2 make the following conjecture plausible.

CONJECTURE. Let k be a hilbertian field and let e be a positive integer. Then for almost all $(\sigma) \in \mathscr{G}(k_s/k)^e$ there does not exist a field $k \subseteq K \subset k_s(\sigma)$ such that $[k_s(\sigma):K] < \infty$.

Stalling proved in [17] that if a finitely generated torsion-free (discrete) group G has a free subgroup of finite index then G is free. If Stalling's theorem is true also for finitely generated free profinite groups then we can prove our conjecture as follows: We denote by S the set of all $(\sigma) \in \mathscr{G}(k_s/k)^e$ which are topologically free and for which there does not exist a $(\rho) \in \mathscr{G}(k_s/k)^e$ such that $k_s(\sigma) \supset k_s(\rho)$, and for which there does not exist a $\tau \in \mathscr{G}(k_s/k)$ of finite order such that $[k_s(\sigma):k_s(\sigma,\tau)] < \infty$. By Theorems 5.1, 9.1, and 12.2, S has the measure 1. Let $(\sigma) \in S$ and suppose that there exists a field $k \subseteq K \subset k_s(\sigma)$ such that $[k_s(\sigma):K] < \infty$. Then there exists a $\tau \in \mathscr{G}(k_s/k) - \langle\sigma\rangle$. For this τ we have that $\langle\sigma\rangle$ is a proper closed subgroup of $\langle\sigma,\tau\rangle$ of finite index. By the choice of (σ), $\langle\sigma,\tau\rangle$ is a finitely generated torsion-free profinite group. Hence by our assumption $\langle\sigma,\tau\rangle$ is also a free profinite group. Again, by the choice of (σ), the rank of $\langle\sigma,\tau\rangle$ must be greater that e, hence it is $e+1$. On the other hand, putting $n = [k_s(\sigma):k_s(\sigma,\tau)]$ we have by Lemma 2.3 that $e = \operatorname{rank}\langle\sigma\rangle = 1 + ne$ which is a contradiction.

However, since we do not have the desired generalization of Stalling's theorem at hand, we are able to prove the conjecture only for the case $e = 1$. This needs some more preliminaries.

We refer to the notation in the beginning of the proof of Theorem 9.1. For $v \in \hat{F}_1 = \hat{\mathbb{Z}}$ and an element a of a profinite group G we put $v_G(a) = a^v$. Then the function $(v,a) \mapsto a^v$ of $\hat{\mathbb{Z}} \times G$ into G has all the properties of the power function in the real numbers. In particular it is continuous. For $v \in \mathbb{Z}$, a^v is the usual power function. If v is not divisible by a certian prime p and G is a finite group then there exists an integer i which is not divisible by p such that $a^v = a^i$ for every $a \in G$. Indeed the intersection H of all the kernels of the continuous homomorphisms of $\hat{\mathbb{Z}}$ into G is an open subgroup of G, since there are only a finite number of such maps. Hence the intersection $p\hat{\mathbb{Z}} \cap H$ is also open in $\hat{\mathbb{Z}}$. We can therefore find an integer i such that $v = i \pmod{p\hat{\mathbb{Z}} \cap H}$. This i is certainly relatively prime to p and it satisfies $a^v = a^i$ for every $a \in G$.

THEOREM 13.1. *Let k be a hilbertian field. Then for almost all $\sigma \in \mathscr{G}(k_s/k)$ there does not exist a field $k \subseteq K \subset k_s(\sigma)$ such that $[k_s(\sigma):K] < \infty$.*

PROOF. Denote by S the set of all $\sigma \in \mathscr{G}(k_s/k)$ with the following properties:

(i) $\langle\sigma\rangle \cong \hat{\mathbb{Z}}$.

(ii) For every prime p there exists a continuous homomorphism of $\mathscr{G}(k_s/k)$ onto S_p which maps σ onto the cycle $c = (1\ 2 \cdots p)$.

(iii) There does not exist an element $\zeta \in \mathscr{G}(k_s/k)$ of finite order such that $[k_s(\sigma) : k_s(\sigma, \zeta)] < \infty$.

By Theorems 5.1, 4.2, and 12.2, S has the measure 1. We show that every element of S has the desired property.

Indeed let $\sigma \in S$ and suppose that there exists a field $k \subseteq K \subset k_s(\sigma)$ such that $[k_s(\sigma) : K] < \infty$. Choose a prime p which divides $[k_s(\sigma) : K]$, put $G = \mathscr{G}(k_s/K)$, and let G_p be a p-Sylow group of G (see Ribes [15, p. 47]). Then G_p is not contained in $\langle\sigma\rangle$. Let L be the fixed field of G_p and put $M = k_s(\sigma)L$. $\mathscr{G}(k_s/M) = \mathscr{G}(k_s/k_s(\sigma)) \cap \mathscr{G}(k_s/L)$. Hence $\mathscr{G}(k_s/M)$ is a p-Sylow group of $\langle\sigma\rangle$. Since $\langle\sigma\rangle \cong \hat{\mathbb{Z}}$ we have that $\mathscr{G}(k_s/M) = \hat{\mathbb{Z}}_p$. Obviously $1 < p^m = (G_p : \mathscr{G}(k_s/M)) = [M : L] < \infty$. Moreover G_p is torsion free by (iii). It follows by a theorem of Serre [16, Cor. 12] that G_p is a free p-profinite group. Its rank r is clearly finite (it is certainly $\leqq 1 + p^m$). Since the usual formula for the ranks holds also for pro-p-finite groups (see Binz, Neukirch, Wenzel [3, p. 108]), we have that $r = 1$. This means that G_p is procyclic. Let ρ be a topological generator for G_p. Then ρ^{p^m} is a topological generator for $\mathscr{G}(k_s/M)$. Since $\mathscr{G}(k_s/M)$ is the Sylow p-group of $\langle\sigma\rangle$ there exists a $v \in \hat{\mathbb{Z}}$ which is not divisible by p such that

$$\rho^p = \sigma^v. \tag{1}$$

For this v there exists an integer i which is not divisible by p such that $a^v = a^i$ for every $a \in S_p$. If we apply the homomorphism of $\mathscr{G}(k_s/k)$ onto S_p (which exists by (iii)) to (1) and denote by b the image of ρ, we obtain that $b^{p^m} = c^i$ Hence

$$1 = b^{(p-1)!p^m} = c^{(p-1)!i}.$$

It follows that p divides $(p-1)!\ i$, which is a contradiction. Therefore such a K does not exist. Q.E.D.

14. The centralizer and the normalizer

The following statement is a possible property of a field k.

(*) Every closed abelian subgroup of $\mathscr{G}(k_s/k)$ is procyclic.

It is clear that if a field k has the property (*) then every algebraic extension of k

has this property. W. D. Geyer proved in [5, Satz 2.3 and Sect. 6] that the following hilbertian fields have the property (*): number fields, and function fields of one variable over finite, real, or algebraically closed fields. For these fields we prove the following theorem.

THEOREM 14.1. *Let k be hilbertian field with the property (*). Then for almost all $\sigma \in \mathcal{G}(k_s/k)$ the subgroup $\langle\sigma\rangle$ is its own centralizer, and if $e \geqq 2$ then for almost all $(\boldsymbol{\sigma}) \in \mathcal{G}(k_s/k)^e$ the centralizer of $\langle\boldsymbol{\sigma}\rangle$ is trivial.*

PROOF. Let S be the set of all $\sigma \in \mathcal{G}(k_s/k)$ for which there does not exist a $\tau \in \mathcal{G}(k_s/k)$ such that $k_s(\tau) \subset k_s(\sigma)$. By Theorem 9.1, S has the measure 1. Let now $\sigma \in S$ and suppose that an element $\rho \in \mathcal{G}(k_s/k)$ commutes with σ. Then $\langle\sigma, \rho\rangle$ is an abelian group and hence, by our assumption, there exists a $\tau \in \mathcal{G}(k_s/k)$ such that $\langle\sigma, \rho\rangle = \langle\tau\rangle$. But then, by the choice of σ, we have that $\langle\sigma\rangle = \langle\tau\rangle$. Hence $\rho \in \langle\sigma\rangle$. It follows that $\langle\sigma\rangle$ is its own centralizer in $\mathcal{G}(k_s/k)$.

Next, for $e \geqq 2$, let T be the set of all $(\boldsymbol{\sigma}) \in \mathcal{G}(k_s/k)^e$ with the following properties:

(i) There does not exist a $\tau \in \mathcal{G}(k_s/k)$ such that $k_s(\tau) \subset k_s(\sigma_1)$ or $k_s(\tau) \subset k_s(\sigma_2)$.

(ii) $\langle\sigma_1\rangle \cap \langle\sigma_2\rangle = 1$.

By Theorems 9.1 and 5.1, T has the measure 1.

Let now $(\boldsymbol{\sigma}) \in T$ and suppose that an element $\rho \in \mathcal{G}(k_s/k)$ is in the centralizer of $\langle\boldsymbol{\sigma}\rangle$. Then, as before, $\rho \in \langle\sigma_1\rangle$ and $\rho \in \langle\sigma_2\rangle$. Hence $\rho = 1$. This means that the centralizer of $\langle\boldsymbol{\sigma}\rangle$ in $\mathcal{G}(k_s/k)$ is trivial. Q.E.D.

We do not know if Theorem 14.1 holds also for arbitrary hilbertian fields. However, the following theorem can be proved.

THEOREM 14.2. *Let k be a hilbertian field. Then for almost all $(\boldsymbol{\sigma}) \in \mathcal{G}(k_s/k)^e$ the normalizer of $\langle\boldsymbol{\sigma}\rangle$ in $\mathcal{G}(k_s/k)$ is a torsion-free closed subgroup of an infinite index and hence of measure 0.*

PROOF. It is clear that the normalizer of $\langle\boldsymbol{\sigma}\rangle$ is a closed subgroup of $\mathcal{G}(k_s/k)$ for every $(\boldsymbol{\sigma}) \in \mathcal{G}(k_s/k)^e$. In order to prove that it is almost always torsion-free and of infinite index, we denote by S the set of all $(\boldsymbol{\sigma}) \in \mathcal{G}(k_s/k)^e$ with the following properties:

(i) There does not exist any $\tau \in \mathcal{G}(k_s/k)$ of finite order such that $[k_s(\boldsymbol{\sigma}) : k_s(\boldsymbol{\sigma}, \tau)] < \infty$.

(ii) For every odd prime p there exists a continuous epimorphism of $\mathcal{G}(k_s/k)$ onto S_p which maps $\sigma_1, \cdots, \sigma_e$ onto the cycle $(1\ 2 \cdots p)$.

By Theorem 12.2 and Lemma 4.2, S has the measure 1.

Let $(\boldsymbol{\sigma}) \in S$. Then no element τ of finite order belongs to the normalizer of $\langle \boldsymbol{\sigma} \rangle$, since for such an element we would have $[k_s(\boldsymbol{\sigma}) : k_s(\boldsymbol{\sigma}, \tau)] < \infty$. Next, the index of the normalizer of $\langle \boldsymbol{\sigma} \rangle$ in $\mathcal{G}(k_s/k)$ must be greater of equal to the index of the normalizer of $(1\ 2 \cdots p)$ in S_p. But the later is equal to $(p-2)!$ (refer to the remark after Lemma 12.1). Hence the index of the normalizer of $\langle \boldsymbol{\sigma} \rangle$ is $\geqq (p-2)!$. Since this inequality holds for every odd prime p we conclude that the index is infinite.

Q.E.D.

Corollary 14.3. *Let k be a hilbertian field. Then for almost all $(\boldsymbol{\sigma}) \in \mathcal{G}(k_s/k)^e$ the extension $k_s(\boldsymbol{\sigma})/k$ is not normal. Furthermore, for every $\sigma \in \mathcal{G}(k_s/k)$ the smallest normal extension of k which contains $k_s(\sigma)$ is k_s.*

Proof. The first statement follows from Theorem 14.2. The second follows from a theorem of Kuyk which asserts that no closed solvable subgroup of $\mathcal{G}(k_s/k)$ can be normal (see [11, p. 114]). Q.E.D.

Are the following statements about a hilbertian field k true?

Problem 4. For almost all $(\boldsymbol{\sigma}) \in \mathcal{G}(k_s/k)^e$ the centralizer of $\langle \boldsymbol{\sigma} \rangle$ in $\mathcal{G}(k_s/k)$ is $\langle \boldsymbol{\sigma} \rangle$ if $e = 1$, and is trivial if $e > 1$.

Problem 5. For almost all $(\boldsymbol{\sigma}) \in \mathcal{G}(k_s/k)^e$ the normalizer of $\langle \boldsymbol{\sigma} \rangle$ in $\mathcal{G}(k_s/k)$ is $\langle \boldsymbol{\sigma} \rangle$.

Problem 6. For all $(\boldsymbol{\sigma}) \in \mathcal{G}(k_s/k)^e$ the smallest normal extension of k which contains $k_s(\boldsymbol{\sigma})$ is k_s.

15. Applications to extension problems over hilbertian fields

In this section we translate our results to results about field extensions. We fix a finite Galois extension l of a hilbertian field k and prove the existence of certain extensions of l with prescribed properties.

Theorem 15.1. *Let $1 \to H \to G \xrightarrow{\theta} \mathcal{G}(l/k) \to 1$ be a short exact sequence of finite groups. Then there exists a finite separable extension k'/k which is linearly disjoint from l/k, and there exist finite extensions l'/k' and m'/l' such that m'/k' is Galois and the following diagram in which the vertical arrows are isomorphisms is commutative.*

$$\begin{array}{ccccccccc} 1 & \rightarrow & \mathscr{G}(m'/l') & \rightarrow & \mathscr{G}(m'/k') & \rightarrow & \mathscr{G}(l'/k') & \rightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & H & \longrightarrow & G & \xrightarrow{\theta} & \mathscr{G}(l/k) & \longrightarrow & 1 \end{array}$$

REMARK. Kuyk [10, Th. 3] proved this theorem by using a certain transcendental construction. We deduce it from the Free Generators theorem.

PROOF. Let $g_1,\cdots,g_e$ be generators of G and put $\sigma'_1,\cdots,\sigma'_e$ for the corresponding elements of $\mathscr{G}(l/k)$ by θ. Then $\sigma'_1,\cdots,\sigma'_e$ generate $\mathscr{G}(l/k)$. The set of all e-tuples $(\boldsymbol{\sigma}) \in \mathscr{G}(k_s/k)^e$ whose restriction to l is $(\boldsymbol{\sigma}')$ is of positive measure. Hence, by Theorem 5.1, we can choose among them an e-tuple $(\boldsymbol{\sigma})$ such that $\langle \boldsymbol{\sigma} \rangle \cong F_e$. For this $(\boldsymbol{\sigma})$ we have that $k_s(\boldsymbol{\sigma}) \cap l = k$. Hence, if we put $L = k_s(\boldsymbol{\sigma}) \cdot l$, we obtain that $\mathscr{G}(L/k_s(\boldsymbol{\sigma})) \cong \mathscr{G}(l/k)$. Further, we can extend the map $\sigma_i \mapsto g_i$, $i=1,\cdots,e$, to a continuous epimorphism of $\langle \boldsymbol{\sigma} \rangle$ onto G. The fixed field M of the kernel of this epimorphism contains L and we have $\mathscr{G}(M/k_s(\boldsymbol{\sigma})) \cong G$.

Let now a be an element which generates the field M over $k_s(\boldsymbol{\sigma})$. Then we can find a finite extension k' of k contained in $k_s(\boldsymbol{\sigma})$ such that $m' = k'(a)$ is a Galois extension of k' which is linearly disjoint from $k_s(\boldsymbol{\sigma})$. If we put $l' = L \cap m'$ then k', l' and m' will satisfy all the requirements of the theorem. Q.E.D.

For the rest of this section we denote by $\mathscr{L}$ the set of all finite Galois extensions of k which contain l.

THEOREM 15.2. *Let $(\boldsymbol{\sigma}') \in \mathscr{G}(l/k)^e$ and $(\boldsymbol{\tau}') \in \mathscr{G}(l/k)^f$. Then there exists an $L \in \mathscr{L}$ and an extension $(\boldsymbol{\sigma}'', \boldsymbol{\tau}'')$ of $(\boldsymbol{\sigma}', \boldsymbol{\tau}')$ to L such that the restriction of every element of $\langle \boldsymbol{\sigma}'' \rangle \cap \langle \boldsymbol{\tau}'' \rangle$ to l is the identity.*

PROOF. Assume that for every $L \in \mathscr{L}$ and for every extension $(\boldsymbol{\sigma}'', \boldsymbol{\tau}'')$ of $(\boldsymbol{\sigma}', \boldsymbol{\tau}')$ to L there exists a $\rho'' \in \langle \boldsymbol{\sigma}'' \rangle \cap \langle \boldsymbol{\tau}'' \rangle$ such that $\rho'' \mid l \neq 1$. We shall show that this assumption leads to the conclusion that for every $(\boldsymbol{\sigma}, \boldsymbol{\tau}) \in \mathscr{G}(k_s/k)^{e+f}$ which extends $(\boldsymbol{\sigma}', \boldsymbol{\tau}')$ we have $\langle \boldsymbol{\sigma} \rangle \cap \langle \boldsymbol{\tau} \rangle \neq 1$. Since the set of these $(\boldsymbol{\sigma}, \boldsymbol{\tau})$ has a positive measure we shall obtain a contradiction to Theorem 5.1.

Indeed, let $(\boldsymbol{\sigma}, \boldsymbol{\tau})$ be an $e+f-$ tuple which extends $(\boldsymbol{\sigma}', \boldsymbol{\tau}')$. For every $L \in \mathscr{L}$ denote by $S(L)$ the set of all $\rho'' \in \langle \boldsymbol{\sigma} \mid L \rangle \cap \langle \boldsymbol{\tau} \mid L \rangle$ such that $\rho'' \mid l \neq 1$. Then $S(L)$ is a nonempty finite set. If M is another field in $\mathscr{L}$ which contains L then the restriction map of $\mathscr{G}(M/k)$ onto $\mathscr{G}(L/k)$ induces a canonical map θ_L^M of $S(M)$ into $S(L)$.

Thus $\{S(L), \theta_L^M\}$ is a projective system of nonempty finite sets. The projective limit of such a system is not empty [4, Th. 3.6]. An element of this limit induces a

$\rho \in \mathscr{G}(k_s/k)$ such that $\rho \mid L \in \langle \boldsymbol{\sigma} \mid L \rangle \cap \langle \boldsymbol{\tau} \mid L \rangle$ for every $L \in \mathscr{L}$ and $\rho \mid l \neq 1$. Hence $\rho \in \langle \boldsymbol{\sigma} \rangle \cap \langle \boldsymbol{\tau} \rangle$ and $\rho \neq 1$.

PROBLEM 7. Let $(\boldsymbol{\sigma}') \in \mathscr{G}(l/k)^e$ and $(\boldsymbol{\tau}') \in \mathscr{G}(l/k)^f$. Does there exist a field $L \in \mathscr{L}$ and an extension $(\boldsymbol{\sigma}'', \boldsymbol{\tau}'')$ of $(\boldsymbol{\sigma}', \boldsymbol{\tau}')$ to L such that $\langle \boldsymbol{\sigma}'' \rangle \cap \langle \boldsymbol{\tau}'' \rangle = 1$?

We note that the analogous group theoretical problem has a positive solution, that is, one can find a finite group G, an epimorphism $\pi : G \to \mathscr{G}(l/k)$, and elements $(\boldsymbol{s}, \boldsymbol{t}) \in G^{e+f}$ such that $\pi(\boldsymbol{s}, \boldsymbol{t}) = (\boldsymbol{\sigma}', \boldsymbol{\tau}')$ and $\langle \boldsymbol{s} \rangle \cap \langle \boldsymbol{t} \rangle = 1$.

THEOREM 15.3. *Let $\phi(X_1, \cdots, X_e)$ be a negative formula in the free variables $X_1, \cdots, X_e$ and suppose that there exists a positive integer m such that $S_m \models \exists X_1 \cdots \exists X_m \phi(X_1, \cdots, X_m)$. Let $(\boldsymbol{\sigma}') \in \mathscr{G}(l/k)^e$. Then there exists an $L \in \mathscr{L}$ and there exists $(\boldsymbol{\sigma}'') \in \mathscr{G}(L/k)^e$ which extends $(\boldsymbol{\sigma}')$ such that $\mathscr{G}(L/k) \models \phi(\sigma_1'', \cdots, \sigma_e'')$.*

PROOF. Assuming that the theorem is false we argue as in the proof of Theorem 15.2. The main point of the argument is the following: Let $\sigma_1, \cdots, \sigma_e \in \mathscr{G}(k_s/k)$ such that $\mathscr{G}(L/k) \models \sim \phi(\sigma_1 \mid L, \cdots, \sigma_e \mid L)$ for every $L \in \mathscr{L}$. Since $\sim \phi(X_1, \cdots, X_e)$ is a positive formula one can prove by induction on the number of the quantifiers of ϕ that $\mathscr{G}(k_s/k) \models \sim \phi(\sigma_1, \cdots, \sigma_e)$. This leads to a contradiction to Theorem 8.1.

Q.E.D.

In the same way one can now deduce Theorems 15.4, 15.5 and 15.6 from the Theorems 9.1, 12.2 and 13.1 respectively.

THEOREM 15.4. *Let $(\boldsymbol{\sigma}')$, $(\boldsymbol{\tau}') \in \mathscr{G}(l/k)^e$ such that $l(\boldsymbol{\tau}') \subset l(\boldsymbol{\sigma}')$. Then there exists a field $L \in \mathscr{L}$ and a $(\boldsymbol{\sigma}'') \in \mathscr{G}(L/k)^e$ which extends $(\boldsymbol{\sigma}')$ such that for every $(\boldsymbol{\tau}'') \in \mathscr{G}(L/k)^e$ which extends $(\boldsymbol{\tau}')$ we have $L(\boldsymbol{\tau}'') \nsubseteq L(\boldsymbol{\sigma}'')$.*

THEOREM 15.5. *Let $(\boldsymbol{\sigma}') \in \mathscr{G}(l/k)^e$, $\tau' \in \mathscr{G}(l/k)$, $\tau' \neq 1$, and let n be a positive integer. Then there exists a field $L \in \mathscr{L}$ and an extension $(\boldsymbol{\sigma}'')$ of $(\boldsymbol{\sigma}')$ to L such that for every $\tau'' \in \mathscr{G}(L/k)$ which extends τ', either* $\mathrm{ord}\, \tau'' > n$ *or* $[L(\boldsymbol{\sigma}'') : L(\boldsymbol{\sigma}'', \tau'')] > n$.

THEOREM 15.6. *Let $\boldsymbol{\sigma}' \in \mathscr{G}(l/k)$ and let k_0 be a field such that $k \subseteq k_0 \subset l(\sigma')$. Then there exists a field $L \in \mathscr{L}$ and an extension σ'' of σ' to L for which there does not exist a field $k \subseteq K'' \subseteq L(\sigma'')$ such that $l \cap K'' = k_0$ and $[L(\sigma'') : K''] \leqq n$.*

We note that for the proof of this theorem it is important to remember that a finite separable extension contains only a finite number of subextensions (see Lang [14, p. 185]).

16. Applications to finitely generated free profinite groups

As an application we deduce the following result.

THEOREM 16.1. *Let* $z_1, \cdots, z_e$ *be free topological generators for* $\hat{F}_e$ *and let* $1 \leqq d \leqq e$. *Then*

(i) $\hat{F}_e$ *is a torsion-free group.*

(ii) *Every abelian closed subgroup of* $\hat{F}_e$ *is procyclic.*

(iii) *If* $1 \leqq d < e$ *then* $\langle z_1, \cdots, z_d \rangle \cap \langle z_{d+1}, \cdots, z_e \rangle = 1$.

(iv) *There do not exist* $x_1, \cdots, x_d \in \hat{F}_e$ *such that* $\langle z_1, \cdots, z_d \rangle \subset \langle x_1, \cdots, x_d \rangle$.

(v) *There does not exist a closed subgroup J of* $\hat{F}_e$ *which contains* z_1 *such that* $1 < (J : \langle z_1 \rangle) < \infty$.

(vi) *The closed subgroup* $\langle z_1 \rangle$ *is its own centralizer in* $\hat{F}_e$.

(vii) *If* $d \geqq 2$ *then the centralizer of* $\langle z_1, \cdots, z_d \rangle$ *in* $\hat{F}_e$ *is trivial. In particular* $\hat{F}_e$ *has a trivial center.*

PROOF. (ii) Take any hilbertian field k having characteristic different from 0. By Theorem 5.1 we can find a topologically free e-tuple $(\sigma_1, \cdots, \sigma_e) \in \mathscr{G}(k_s/k)^e$. Then $\hat{F}_e \cong \langle \sigma \rangle$. Since there are no elements of finite order in $\mathscr{G}(k_s/k)$ (see Lang [14, p. 223]), $\hat{F}_e$ is a torsion free group.

(ii)-(vii) Consider the set S of all $(\sigma) \in \mathscr{G}(\tilde{Q}/Q)^e$ with the following properties:

(a) $\langle \sigma \rangle \cong \hat{F}_e$.

(b) If $1 \leqq d < e$ then $\langle \sigma_1, \cdots, \sigma_d \rangle \cap \langle \sigma_{d+1}, \cdots, \sigma_e \rangle = 1$.

(c) There does not exist a $(\tau) \in \mathscr{G}(\tilde{Q}/Q)^e$ such that $\tilde{Q}(\tau) \subset \tilde{Q}(\sigma)$.

(d) There does not exist a field $k \subseteq K \subset \tilde{Q}(\sigma_1)$ such that $[\tilde{Q}(\sigma_1) : K] < \infty$.

(e) The closed subgroup $\langle \sigma_1 \rangle$ is its own centralizer in $\mathscr{G}(\tilde{Q}/Q)$.

(f) If $d \geqq 2$ then the centralizer of $\langle \sigma_1, \cdots, \sigma_d \rangle$ in $\mathscr{G}(\tilde{Q}/Q)$ is trivial.

By Theorems 5.1, 9.1, 13.1, and 14.1, S has the measure 1. It follows that it is not empty. The existence of an e-tuple $(\sigma) \in S$ implies automatically the statements (iii)-(vii). The statement (ii) follows from the fact that Q has the property (*) of Section 14. Q.E.D.

ACKNOWLEDGEMENTS

It is a pleasure to express here my appreciation to my thesis adviser H. Furstenberg who gave me the first inspiration for this work, and to W. D. Geyer for many discussions through which I was able to bring the work to its present level.

REFERENCES

1. J. Ax, *Solving diophantic problems modulo every prime*, Ann. of Math. **85** (1967), 161–183.

2. J. Ax, *The elementary theory of finite fields*, Ann. of Math. **88** (1968), 239–271.

3. E. Binz, J. Neukirch, G. H. Wenzel, *A subgroup theorem for free products of pro-finite groups*, J. Algebra **19** (1971), 104–109.

4. S. Eilenberg and N. Steenrod, *Foundations of Algebraic Topology*, Princeton University Press, Princeton, New Jersey.

5. W. D. Geyer, *Unendliche algebraische Zahlkörper, über denen jede Gleichung auflösbar von beschränkter Stufe ist*, J. Number Theory **1** (1969), 346–374.

6. M. Hall, Jr., *Subgroups of finite index in free groups*, Canad. J. Math. **I**, (1949), 187–190.

7. M. Hall, Jr., *A topology for free groups and related groups*, Ann. of Math. (2) **52** (1950), 127–139.

8. M. Jarden, *Elementary statements over large algebraic fields*, Trans. Amer. Math. Soc. **164** (1972), 67–91.

9. A. G. Kurosh, *The Theory of Groups*, Vol. II, second English edition, Chelsea Publishing Company, New York.

10. W. Kuyk, *Generic approach to the Galois embedding and extension problem*, J. Algebra **9** (1968), 393–407.

11. W. Kuyk, *Extensions de corps hilbertiens*, J. Algebra **14** (1970), 112–124.

12. S. Lang, *Introduction to algebraic geometry*, Intersience tracts in pure and applied Mathematics, No. 5, Intersience Publishers, Inc., New York.

13. S. Lang, *Diophantine geometry*, Intersience tracts in pure and applied Mathematics, No. 11, Intersience Publishers, New York, London.

14. S. Lang, *Algebra*, Addison-Wesley Publishing Company, Reading, Massachusetts.

15. L. Ribes, *Introduction to pro-finite groups and Galois cohomology*, Queens papers in pure and applied Mathematics, No. 24, 1970.

16. J. P. Serre, *Sur la dimension cohomologique des groupes profinis*, Topology, **3** (1964–65), 413–420.

17. J. R. Stalling, *On torsion-free groups with infinitely many ends*, Ann. of Math. **88** (1968), 312–334.

18. A. Weil, *Foundations of Algebraic Geometry*, Revised and enlarged edition (1962), A. M. S. Colloquium publications Vol. XXIX Providence, Rhode Island.

DEPARTMENT OF MATHEMATICS
THE HEBREW UNIVERSITY OF JERUSALEM
JERUSALEM, ISRAEL

AND

MATHEMATISCHES INSTITUT
HEIDELBERG UNIVERSITÄT
HEIDELBERG, WEST GERMANY

Present address:
DEPARTMENT OF MATHEMATICAL SCIENCES
TEL-AVIV UNIVERSITY
RAMAT-AVIV, ISRAEL