INTERSECTIONS OF CONJUGATE FIELDS OF FINITE CORANK OVER HILBERTIAN FIELDS

MOSHE JARDEN

Introduction

It was proved in [4] that if K is a Hilbertian field and e is a positive integer, then for almost all $(\sigma) = (\sigma_1, \ldots, \sigma_e) \in G(K)^e$, the closed subgroup $\langle\sigma\rangle = \langle\sigma_1, \ldots, \sigma_e\rangle$ generated by $\sigma_1, \ldots, \sigma_e$ is isomorphic to $\hat{F}_e$, the free pro-finite group on e generators. This is the Free Generators Theorem. Here $G(K)$ is the absolute Galois group, $\mathfrak{G}(K_s/K)$, of K and " almost all " is meant in the sense of the Haar measure of $G(K)$. It was also proved in [4] that given an e-tuple $(\sigma) \in G(K)^e$, the set

$$S(\sigma) = \{(\sigma') \in G(K)^e \mid \exists\, \tau \in G(K) : \tau^{-1}\sigma_i\tau = \sigma_i' \text{ for } i = 1, \ldots, e\}$$

has measure zero. Therefore the Free Generators Theorem implies nothing on the groups $\langle\sigma^{\tau_1}, \ldots, \sigma^{\tau_e}\rangle$. In this work we fill up this gap and prove

THEOREM A. *Let K be a Hilbertian field. Then $\langle\sigma^{\tau_1}, \ldots, \sigma^{\tau_e}\rangle \cong \hat{F}_e$ for almost all $\sigma \in G(K)$ and almost all $(\tau) \in G(K)^e$.*

The proof of Theorem A uses methods developed by Geyer in [2] in order to prove that, for almost all $(\tau) \in G(\mathbb{Q})^e$, the group $\langle G(\mathbb{Q}_v)^{\tau_1}, \ldots, G(\mathbb{Q}_v)^{\tau_e}\rangle$ is isomorphic to the free product of e copies of $G(\mathbb{Q}_v)$. Here v is an absolute value of $\mathbb{Q}$, and $\mathbb{Q}_v$ is the Henselization of $\mathbb{Q}$ with respect to v.

The fixed field of $\sigma_1, \ldots, \sigma_e$ in K_s is denoted by $K_s(\sigma)$. It was proved in [3] that if K is a countable Hilbertian field, then the fields $K_s(\sigma)$ are PAC for almost all $(\sigma) \in G(K)^e$. This is the Nullstellensatz. Here a field F is said to be PAC if every absolutely irreducible variety defined over F has an F-rational point. Again, using the stability property of fields of characteristic zero, proved in [1], we strengthen the Nullstellensatz and prove

THEOREM B. *Let K be a countable Hilbertian field of characteristic zero. Then for almost all $(\sigma) \in G(K)^e$, the maximal Galois extension of K contained in $\tilde{K}(\sigma)$ is a* PAC *field. Here $\tilde{K}$ is the algebraic closure of K.*

A perfect PAC field F such that $G(F) \cong \hat{F}_e$ is said to be an e-free Ax field. It was proved in [6] that the elementary theory of e-free Ax fields is decidable. Recalling that a separable algebraic extension of a PAC field is again a PAC field, one can combine Theorems A and B to obtain new models for e-free Ax fields.

THEOREM C. *Let K be a countable Hilbertian field of characteristic zero. Then $K(\sigma^{\tau_1}, \ldots, \sigma^{\tau_e})$ is an e-free* Ax *field for almost all $\sigma \in G(K)$ and almost all $(\tau) \in G(K)^e$.*

Received 5 August, 1977.

1. *Proof of Theorem A*

Consider two sets A and B of n elements, let s be a permutation of A and let σ be a permutation of B. We say that σ is *similar* to s, if there exists a bijective map $\tau : A \to B$ such that $s = \tau^{-1}\sigma\tau$. If $A = B$, then σ and s are conjugate in $S(A)$, the group of all permutations of A.

Let $s \in S_n$ and let $\sigma \in G(K)$. We say that σ satisfies the condition $P(n, s)$ if there exists a sequence $f_1, f_2, f_3, \ldots$ of polynomials in $K[X]$ of degree n such that the following conditions hold:

(a) The splitting field K_i of f_i over K is Galois and $\mathfrak{G}(K_i/K) \cong S_n$.

(b) The representation of σ as a permutation of the roots of f_i is similar to s, for every $i \geqslant 1$.

(c) The sequence $K_1, K_2, K_3, \ldots$ is linearly disjoint over K.

LEMMA 1.1. *Almost all $\sigma \in G(K)$ satisfy $P(n, s)$ for every n and s.*

Proof. It suffices to prove that, for a given n and s, almost all $\sigma \in G(K)$ satisfy the condition $P(n, s)$. Indeed, we can find polynomials $f_1, f_2, f_3, \ldots$ in $K[X]$ of degree n, satisfying (a) and (c) (by [**4**; Section 3]). For every $i \geqslant 1$ we choose an element $s_i \in \mathfrak{G}(K_i/K)$ which is similar to s. By the Borel-Cantelli Lemma, for almost all $\sigma \in G(K)$ there exist infinitely many numbers i such that $\sigma | K_i = s_i$ (see [**5**; Lemma 1.4]). Every such σ satisfies the condition $P(n, s)$.

LEMMA 1.2. *For every finite group H, generated by e elements, there exists a finite group G generated by e elements $g_1, \ldots, g_e$ and an epimorphism $\theta : G \to H$ such that every permutation s of $g_1, \ldots, g_e$ can be extended to an automorphism of G.*

Proof. Consider the free group F_e generated by the letters $z_1, \ldots, z_e$. This group has only finitely many normal subgroups, say, $N_1, \ldots, N_r$, such that $F_e/N_i \cong H$. The intersection $N = N_1 \cap \ldots \cap N_r$ is a characteristic subgroup of F_e of a finite index. Indeed, every $\alpha \in \mathrm{Aut}(F_e)$ induces a permutation of $\{N_1, \ldots, N_r\}$, hence $N^\alpha = N$. Let $G = F_e/N$ and let $g_i = z_i N$ for $i = 1, \ldots, n$. Then G is an extension of H and it is generated by $g_1, \ldots, g_e$. Let s be a permutation of $g_1, \ldots, g_e$. Then s induces an automorphism α of F_e by

$$\alpha(z_i) = z_j \Leftrightarrow s(g_i) = g_j.$$

Hence α induces an automorphism $\tilde{\alpha}$ of G that extends s.

Theorem A will follow now from Lemma 1.1 and from

LEMMA 1.3. *Let $\sigma \in G(K)$ be an element that satisfies the conditions $P(n, s)$ for every n and s. Then*

$$\langle \sigma^{\tau_1}, \ldots, \sigma^{\tau_e} \rangle \cong \hat{F}_e$$

for almost all $(\tau) \in G(K)^e$.

Proof. It was proved in [**4**; p. 284] that if a profinite group G of rank $\leqslant e$ has every finite group H of rank $\leqslant e$ as a homomorphic image, then $G \cong \hat{F}_e$. It follows therefore, by Lemma 1.2, that in order to prove our Lemma it suffices to prove:

If $H = h_1, \ldots, h_e$ is a finite group such that every permutation of $\{h_1, \ldots, h_e\}$ can be extended to an automorphism of H, then for almost all $(\tau) \in G(K)^e$ there exists a continuous epimorphism of $\langle \sigma^{\tau_1}, \ldots, \sigma^{\tau_e} \rangle$ onto H.

Indeed, the symmetric group S_e operates on such an H in an obvious way. Let $H \cdot S_e$ be the semi-direct product of H and S_e. This is a finite group and therefore it can be considered as a subgroup of a symmetric group S_n. All the elements $h_1, \ldots, h_e$ are conjugate in $H \cdot S_e$, hence also in S_n. Hence they are all similar to $s = h_1$. By assumption, σ satisfies the condition $P(n, s)$. Let $i \geqslant 1$ and let $s_{i1}, \ldots, s_{ie}$ be the elements of $\mathfrak{G}(K_i/K)$ that correspond to $h_1, \ldots, h_e$ under the isomorphism $\mathfrak{G}(K_i/K) \cong S_n$. All these elements are similar to S. By assumption, $\sigma|K_i$ is similar to s as well. Hence there exist $t_{i1}, \ldots, t_{ie}$ in $\mathfrak{G}(K_i/K)$ such that $t_{ij}^{-1} (\sigma|K_i)\, t_{ij} = s_{ij}$ for $j = 1, \ldots, e$.

By [5; Lemma 4.1] and by (c) we have that for almost all (τ) in $G(K)^e$ there exists an i such that $\tau_j|K_i = t_{ij}$ for $j = 1, \ldots, e$. In this case we have $(\tau_j^{-1} \sigma \tau_j)|K_i = s_{ij}$ for $j = 1, \ldots, e$. Hence there exists a continuous epimorphism of $\langle \sigma^{\tau_1}, \ldots, \sigma^{\tau_e} \rangle$ onto H, since $H \cong \langle s_{i1}, \ldots, s_{ie} \rangle$.

Theorem A and the Theorem of Geyer cited in the introduction give rise to

PROBLEM 1. *Let K be a Hilbertian field and let $\sigma \in G(K)$. Is it true that for almost all $(\tau) \in G(K)^e$, the group $\langle \sigma^{\tau_1}, \ldots, \sigma^{\tau_e} \rangle$ is isomorphic to the free product of e copies of $\langle \sigma \rangle$?*

We note that the method of proof of Theroem A actually gives also

THEOREM A*. *If K is a Hilbertian field, then $\langle \sigma^{\tau_1}, \ldots, \sigma^{\tau_1} \rangle \cong \hat{F}_{ef}$ for almost all $(\sigma) \in G(K)^e$ and almost all $(\tau) \in G(K)^f$.*

2. *Proof of Theorem B*

Let K be a countable Hilbertian field of characteristic zero. For a $(\sigma) \in G(K)^e$ we denote by N_σ the maximal Galois extension of K which is contained in $\tilde{K}(\sigma)$. It is the intersection of all the fields $\tilde{K}(\sigma_1^{\tau_1}, \ldots, \sigma_e^{\tau_e})$ for $\tau \in G(K)$.

Recall that an absolutely irreducible polynomial $f \in K[T_1, \ldots, T_r, X]$ is said to be *stable with respect to* $T_1, \ldots, T_r$, if $\deg_X f > 0$ and if the Galois group of f over $L(T)$ is isomorphic to the Galois group G of f over $K(T)$ for every algebraic extension L of K.

Let f be such a polynomial and let A be a non-void K-open set in the affine space S^r. As in the proof of Theorem 4.4 of [1], one can inductively construct a linearly disjoint sequence $K_1, K_2, K_3, \ldots$, of Galois groups of K, with Galois groups isomorphic to G, such that for every $i \geqslant 1$ there exists a point $(a_1, \ldots, a_r, b) \in K_i^{r+1}$ such that (a) $\in A$ and $f(a, b) = 0$. If $(\sigma) \in G(K_i)^e$, then $K_i \subseteq N_\sigma$. Further, the set

$$S(f, A) = \bigcup_{i=1}^{\infty} G(K_i)^e$$

has measure one in $G(K)^e$, by Lemma 4.1 of [4]. Since there are only countably many possible pairs (f, A) the intersection $S = \cap\, S(f, A)$ is also a set of measure one. If $(\sigma) \in S$ then for every pair (f, A) as above there exists

$(a, b) \in N_\sigma^{r+1}$ such that $(a) \in A$ and $f(a, b) = 0$. It follows that N_σ is a PAC field, by Lemma 4.1 of [**1**].

PROBLEM 2. *Is it true that for almost all* $\sigma \in G(\mathbb{Q})$ *there exists a sequence* $\tau_1, \tau_2, \tau_3, \ldots$ *in* $G(\mathbb{Q})$ *such that* $\langle \sigma^{\tau_1}, \sigma^{\tau_2}, \sigma^{\tau_3}, \ldots \rangle$ *is isomorphic to* $\hat{F}_\omega$, *the free pro-finite group on* $\aleph_0$ *generators*?

References

1. M. Fried and M. Jarden, " Diophantine properties of subfields of $\tilde{\mathbb{Q}}$ ", *Amer. J. Math. to appear*
2. W.-D. Geyer, " Galois groups of intersections of local fields ", *Israel J. Math.*, to appear.
3. M. Jarden, " Elementary statements over large algebraic fields ", *Trans. Amer. Math. Soc.*, 164 (1972), 67–91.
4. M. Jarden, "Algebraic extensions of finite corank of Hilbertian fields ", *Israel J. Math.*, 18 (1974), 279–307.
5. M. Jarden, " Roots of unity over large algebraic fields ", *Math. Ann.*, 213 (1975), 109–127.
6. M. Jarden and U. Kiehne, " The elementary theory of algebraic fields of finite corank ", *Invent. Math.* 30 (1975), 275–294.

Department of Mathematical Sciences,
Tel-Aviv University,
Ramat-Aviv, Tel-Aviv,
Israel.