An analogue of Čebotarev density theorem for fields of finite corank

By

Moshe JARDEN*

(Communicated by Prof. M. Nagata, Nov. 10, 1978)

Introduction.

Michel Fried and G. Sacerdate established in [5] a primitive recursive decision procedure for the elementary theory of finite fields. The crucial theorem used in the proof was the "Non-regular analogue of the Čebotarev density theorem" (see [5, Proposition 4.1] and also Fried [3, Proposition 2]). This analogue is a certain combination of Čebotarev density theorem and Riemann Hypothesis for curves over finite fields. Fried-Sacerdate procedure gives automatically a primitive recursive procedure for the theory of all elementary statements that are true in $\tilde{Q}(\sigma)$, for almost all $\sigma\in G(Q)$, since this theory is equal to the theory of all elementary statements true in F_p, for almost all primes p (see [7, Thm. 3.17]). Moreover, as was already hinted in [5, p. 207], it is very probable that Fried-Sacerdate procedure might be generalized to give a primitive recursive procedure for the theory of all elementary statements that are true in $\tilde{Q}(\sigma_1, \cdots, \sigma_e)$ for almost all $(\underline{\sigma})=(\sigma_1, \cdots, \sigma_e)\in G(Q)^e$. In this work we take the first step toward this goal and prove an appropriate analogue of the Čebotarev density theorem for the fields $\tilde{Q}(\sigma)$:

Almost all $(\underline{\sigma})\in G(Q)^e$ *have the followig property*: *Let* E *be a finitely generated regular extension of* $M=\tilde{Q}(\underline{\sigma})$, *let* F *be a finite Galois extension of* E, *let* $\varepsilon_1, \cdots, \varepsilon_e$ *be elements of* $\mathcal{G}(F/E)$, *let* $u_1, \cdots, u_m$ *be elements of* E *and let* N_0 *be the algebraic closure of* M *in* F. *Suppose that* $\varepsilon_i|N_0=\sigma_i|N_0$ *for* $i=1, \cdots, e$. *Then there exists an* M*-place* $\varphi: F\to\tilde{Q}$ *such that* a) $\varphi(E)=M$, b) φ *is finite at* $u_1, \cdots, u_m$, c) $H=<\varepsilon_1, \cdots, \varepsilon_e>$ *is the decomposition group of* φ, d) $N=\varphi(F)$ *is a Galois extension of* M *and the map of* H *onto* $\mathcal{G}(N/M)$ *induced by* φ *is an isomorphism that maps* ε_i *onto* $\sigma_i|N$, *for* $i=1, \cdots, e$.

The Čebotarev Property of the $(\underline{\sigma})$'s implies that their fixed fields $\tilde{Q}(\underline{\sigma})$ are e-free and PAC. Here a field M is said to be e-free, if its absolute Galois group $G(M)$ is isomorphic to the free profinite group $\hat{F}_e$ on e generators. A field M is said to be PAC if every non-void absolutely irreducible variety

* Partially supported by the United States-Israel Binational Science Foundation.

defined over M has an M-rational point.

It is probable that the converse implication is also true, namely that e-free and PAC implies the Čebotarev Property, but I do not have as yet a proof to this statement.

As an application it is proved that every ω-free zero characteristic PAC field is Hilbertian. Here an ω-free field is one over which every finite embedding problem is solvable.

In [10] we have discussed the elementary theory of perfect ω-free PAC fields. In particular we proved that in any specific characteristic the theory is decidable. This investigation was carried out in analogy to the investigation of the elementary theory of perfect e-free PAC fields. However, although we have been able to supply an abundance of algebraic models of the last theory, no algebraic model was suggested for the first one. At the end of this work we fill up this gap and construct an algebraic extension N of $\boldsymbol{Q}$ which is ω-free and PAC, hence also Hilbertian.

Acknowledgement: The author is indebted to Michael Fried for inspiring the writing of this paper.

1. The Čebotarev Property.

Let M/K be a Galois extension of fields, let N be an extension of M and let $\varepsilon_1, \cdots, \varepsilon_e$ be automorphisms of N over K. We denote by $M(\underline{\varepsilon})$ and $N(\underline{\varepsilon})$ the fixed field in M and N respectively of $\varepsilon_1, \cdots, \varepsilon_e$. Obviously $M(\underline{\varepsilon})=M\cap N(\underline{\varepsilon})$.

Definitions: Let K be a field, let $\sigma_1, \cdots, \sigma_e$ be elements of $G(K)$. Let $M=K_s(\underline{\sigma})$ and let N_0, E, F be fields such that:

I. E is a finitely generated regular extension of M

II. F is a finite Galois extension of E.

III. N_0 is the algebraic closure of M in F.

The system $(\underline{\sigma}, E, F)$ is said to have the Čebotarev Property if for every m elements $u_1, \cdots, u_m$ of E and e elements $\varepsilon_1, \cdots, \varepsilon_e$ of $\mathcal{G}(F/E)$ that satisfy $\varepsilon_i|N_0=\sigma_i|N_0$ for $i=1, \cdots, e$, there exists an M-place $\varphi: F\to M_s$ such that

a) $\varphi(E)=M$,

b) φ is finite at $u_1, \cdots, u_m$

c) $H=\langle\varepsilon_1, \cdots, \varepsilon_e\rangle$ is the decomposition group of φ.

d) $N=\varphi(F)$ is a Galois extension of M and the map of H onto $\mathcal{G}(N/M)$ induced by φ is an isomorphism that maps ε_i onto $\sigma_i|N$ for $i=1, \cdots, e$.

In this definition M_s is the separable closure of M. If $\delta\in H$ and δ' is its image in $\mathcal{G}(N/M)$, then $\delta'(\varphi(x))=\varphi(\delta(x))$ for every $x\in F$ such that $\varphi(x)\neq\infty$. Also, $\varphi(E)$ is the residue field of E under φ.

We say that $(\underline{\sigma})$ has the Čebotarev Property if $(\underline{\sigma}, E, F)$ has the Čebotarev Property for every E, F that satisfy I, II, III.

A field M is said to be of *corank*$\leqq e$ if its absolute Galois group $G(M)$ is

generated by e elements.

An algebro-geometric consequence of the Čebotarev Property is

Lemma 1.1. *Let K be a field and let $(\sigma_1, \cdots, \sigma_e)$ be an e-tuple of elements of $G(K)$ that has the Cebotarev Property. Let $M=K_s(\underline{\sigma})$, let V be an absolutely irreducible variety defined over M and let $\eta_1, \cdots, \eta_e$ be birational transformations of V into itself, defined over M. If the group $H=\langle \eta_1, \cdots, \eta_e \rangle$ is finite, then there exists a point $Q \in V(M_s)$ such that $\eta_i^k Q=\sigma_i^k Q$ for every integer k and $i=1, \cdots, e$.*

Proof. Without loss of generality we can assume that V is affine and let $(\underline{x})$ be a generic point of V over M. Every element $\eta \in H$ defines an automorphism ε of $F=M(\underline{x})$ over M such that $\varepsilon(f(\underline{x}))=f(\eta(\underline{x}))$ for every $f \in M(\underline{x})$. The map $\eta \to \varepsilon$ is an anti-isomorphism of H on a finite subgroup G of $\mathrm{Aut}(F/M)$. Thus F is a finite Galois extension of the fixed field of G and it is a regular extension of M. It follows that there exists an M-place $\varphi: F \to M_s$ which is defined at $\eta(\underline{x})$ for every $\eta \in H$ and such that $\varepsilon_i'=\sigma_i|N$, where $N=\varphi(F)$. Let $(\underline{a})=\varphi(\underline{x})$. Then $(\underline{a}) \in V(N)$ and $\eta_i^k(a)=\sigma_i^k(a)$ for all k and i.

Another consequence of the Čebotarev Property is:

Lemma 1.2. *If $(\underline{\sigma})$ is as in Lemma 1.1 then $K_s(\underline{\sigma})$ and hence also $\tilde{K}(\underline{\sigma})$ are e-free* PAC *fields. Here $\tilde{K}(\underline{\sigma})$ is the maximal purely inseparable extension of $K_s(\underline{\sigma})$.*

Proof. In order to prove that M is e-free it suffices to prove that every finite group H of rank $\leqq e$ can be realized over $M=K_s(\underline{\sigma})$ (see [8, Thm. 2.4]).

Indeed, embed H in a symmetric group S_n. Choose n algebraically independent elements $t_1, \cdots t_n$ over M, let $F=M(\underline{t})$, let S_n operate on $t_1, \cdots, t_n$ in the obvious way and let E be the fixed field of H in F. Then H appears as a decomposition group of some M-rational place $\varphi: F \to M_s$ with trivial intertia group. It follows that H can be realized over M.

In order to prove that M is PAC take $\eta_1, \cdots, \eta_e$ in Lemma 1.1 as the identity maps.

2. The main theorem

Consider the following situation: K is a field, $t_1, \cdots, t_r$ are algebraically independent elements over K, F is a finite Galois extension of $K(\underline{t})$ and L is the algebraic closure of K in F. Suppose that $\varepsilon_1, \cdots, \varepsilon_e$ are elements of $\mathcal{G}(F/K(\underline{t}))$ and $\sigma_1, \cdots, \sigma_e$ are elements of $G(K)$ such that $\varepsilon_i|L=\sigma_i|L$ for $i=1, \cdots, e$. Then $\varepsilon_1, \cdots, \varepsilon_e$ can be extended to automorphisms of K_sF which will be again denoted by $\varepsilon_1, \cdots, \varepsilon_e$ and such that $\varepsilon_i|K_s=\sigma_i$ for $i=1, \cdots, e$. Then $\varepsilon_1, \cdots, \varepsilon$ fix every element of $M(\underline{t})$, where $M=K_s(\underline{\sigma})$. Denote therefore by $H_{(\underline{\sigma})}$ the subgroup of $\mathcal{G}(MF/M(\underline{t}))$ generated by $\varepsilon_1|MF, \cdots, \varepsilon_e|MF$. Then $H_{(\underline{\sigma})}$ is canonically isomorphic to $H=\langle \varepsilon_1|F, \cdots, \varepsilon_e|F \rangle$. Also ML is the algebraic closure of M in MF. In this situation we have the following.

Lemma 2.1. *If K is Hilbertian and if $u_1, \cdots, u_m$ are elements of $K(\underline{t})$, then for almost all $(\underline{\sigma}) \in G(K)^e$ that satisfy $\sigma_j | L = \varepsilon_j | L$ for $j=1, \cdots, e$, and denoting $M = K_s(\underline{\sigma})$, there exists an M-place $\varphi: MF \to K_s$ such that*

a) *$\varphi(M(\underline{t}))=M$ and φ is finite at $u_1, \cdots, u_m$*

b) *$H_{(\underline{\sigma})}$ is the decomposition group of φ*

c) *$N=\varphi(MF)$ is a Galois extension of M, the map $\delta \to \delta'$ of $H_{(\underline{\sigma})}$ onto $\mathcal{G}(N/M)$ induced by φ is an isomorphism, and $\varepsilon'_j = \sigma_j | N$ for $j=1, \cdots, e$.*

Proof. Let x be an element of P which is integral over $K[\underline{t}]$ and such that $F=K(\underline{t}, x)$. Let $f \in K[\underline{T}, X]$ be an irreducible polynomial which is monic and separable with respect to X such that $f(\underline{t}, x)=0$. Let g be an irreducible factor of f over L such that $g(\underline{t}, x)=0$. Then $g(T, X)$ is absolutely irreducible. We can therefore construct by induction a sequence of points $(\underline{a}_i, b_i)$, $i=1, 2, 3, \cdots$ such that

1) $a_{i1}, \cdots, a_{ir} \in K$.

2) $u_1, \cdots, u_m$ belong to the local ring of $K[\underline{t}]$ in the point $(\underline{a}_i)$,

3) $g(\underline{a}_i, b_i)=0$, hence also $f(\underline{a}_i, b_i)=0$.

4) $\dfrac{\partial f}{\partial x}(\underline{a}_i, b_i) \neq 0$.

5) $[K(b_i): K]=[F: K(\underline{t})]$ and $[L(b_i): L]=[F: L(\underline{t})]$, hence

$$K(b_i)=L(b_i)=L_i .$$

6) The sequence of fields $L_1, L_2, L_3, \cdots$ are linearly disjoint over L.

(Compare similar construction in [7, Lemma 2.2] or in [6, Lemma 1]). The specialization $(\underline{t}, x) \to (\underline{a}_i, b_i)$ can be extended to an L-place $\varphi: F \to L_i$ such that $\varphi(F)=L_i$, $\varphi(K(\underline{t})=K$ and φ is finite at $u_1, \cdots, u_m$. Further the map $\delta \to \delta'$ of $\mathcal{G}(F/K(\underline{t}))$ onto $\mathcal{G}(L_i/K)$ induced by φ is an isomorphism (c. f. Lang [13, p. 248]). In particular, $\varepsilon'_j | L = \varepsilon_j | L$ for $j=1, \cdots, e$ and $\varphi(F(\underline{\varepsilon}))=L_i(\underline{\varepsilon}')$.

Using (6) and Lemma 4.1 of [8] we get that almost all $(\underline{\sigma}) \in G(K)^e$ for which $\sigma_j | L = \varepsilon_j | L$, $j=1, \cdots, e$, belong to one of the sets

$$\{(\underline{\tau}) \in G(K)^e \mid \tau_j | L_i = \varepsilon'_j \quad \text{for} \quad j=1, \cdots, e\} \tag{7}$$

Let therefore $(\underline{\sigma})$ be in the set (7). Let $M=K_s(\underline{\sigma})$, extend $\varepsilon_1, \cdots, \varepsilon_e$ to automorphisms of K_sF, as in the discussion above, and extend φ to an M-place, also called φ, of MF into K_s. Then condition (a) is satisfied. Also $N=\varphi(MF) = ML_i$ is a Galois extension of M (c. f. Deuring [2], p. 178). Denote by E the decomposition field of φ. It is the maximal subfield of MF that contains $M(\underline{t})$ and $\varphi(E) \equiv M$. Obviously the map $\delta \to \delta'$ of $\mathcal{G}(MF/E)$ onto $\mathcal{G}(N/M)$ induced by φ is an isomorphism. In particular

$$[MF: E]=[N: M] \tag{8}$$

Claim:
$$M \cdot F(\underline{\varepsilon})=(MF)(\underline{\varepsilon}) .$$

Indeed the ε_i fix the elements of M. Hence the left hand side is included in the right hand side. In order to prove the inverse inclusion note that F is

linearly disjoint from M over $L(\underline{\varepsilon})=L\cap M$. Let $\{m_\alpha\}$ be a linear base for M over $L(\underline{\varepsilon})$. Then $\{m_\alpha\}$ is a base of MF over F, since $M/L(\underline{\varepsilon})$ is an algebraic extension. Any element z of $(MF)(\underline{\varepsilon})$ can therefore be written as

$$z=\sum m_\alpha x_\alpha\,, \tag{9}$$

where $x_\alpha\in F$ and almost all of them are zero. Applying ε_j on (9) we obtain $z=\sum m_\alpha(\varepsilon_j x_\alpha)$ and $\varepsilon_j x_\alpha\in F$. Hence $\varepsilon_j x_\alpha=x_\alpha$ for $j=1,\cdots,e$, i.e. $x_\alpha\in F(\underline{\varepsilon})$, as desired.

The claim implies that $\varphi((MF)(\underline{\varepsilon}))=M$. Hence $(MF)(\underline{\varepsilon})\subseteq E$. It follows by (8) that

$$[F\colon F(\underline{\varepsilon})]=[L_i\colon L_i(\underline{\varepsilon})]=[N\colon M]=[MF\colon E]\leqq[MF\colon (MF)(\underline{\varepsilon})]=[F\colon F(\underline{\varepsilon})].$$

Hence $(MF)(\underline{\varepsilon})=E$ is the decomposition field of φ and $\langle\varepsilon_1|MF,\cdots,\varepsilon_e|MF\rangle$ is the decomposition group of φ in MF. Conditions (b) and (c) are thus also satisfied.

Theorem 2.2. *If K is a contable Hilbertian field, then almost all $(\underline{\sigma})\in G(K)^e$ have the Čebotarev Property.*

Proof. It is easy to see that in the notation of section 1, it suffices to consider only fields E that are purely transcendental over M. Our Theorem follows therefore from Lemma 2.2, using arguments as in the proofs of Theorem 2.5 of [7] or Theorem 6.2 of [6].

3. An application to ω-free PAC fields.

Theorem 3.1*. *Every ω-free field L of characteristic zero is Hilbertian.*

Proof. First note tha L contains some countable Hilbertian field K. In order to prove that L is Hilbertian it surffices to prove that the following statements are true in L: (+) For all absolutely irreducible polynomials $f(T_1,\cdots,T_r,X)$ of degree d which are separable normal in X and have a Galois group G of rank $\leqq e_0$ and for all non-zero polynomials $g(T_1,\cdots,T_r)$ of degree $\leqq d$ there exist $a_1,\cdots,a_r$ such that $f(a_1,\cdots,a_r,X)$ is separable and normal with Galois group isomorphic to G and $g(a_1,\cdots,a_r)\neq 0$.

If $e\geqq e_0$ and $(\underline{\sigma})\in G(K)^e$ has the Čebotarev Property, then (+) is true in the field $\tilde{K}(\underline{\sigma})$, since $T_1,\cdots,T_r$ can be specialized such that G is the decomposition group. It follows by Theorem 2.2 that (+) is true for $\tilde{K}(\underline{\sigma})$, for almost all $(\underline{\sigma})\in\mathcal{G}(K)^e$. Also it is not difficult to see that (+) is equivalent to a sentence in the language of the theory of fields. Theorem 7.1 of [10] implies therefore that (+) is true in L.

Note that the above proof shows that statement (+) remains true for every ω-free perfect PAC field, without any restriction on the characteristic.

* The author has learned about the validity of this Theorem from Peter Roquette.

We recall that if M is a countable field, then M is ω-free if and only if $G(M)$ is isomorphic to the free profinite group, $\hat{F}_\omega$, on $\aleph_0$ generators that converge to 1.

Lemma 3.2*. *Let G be a profinite separable froup. If $\hat{F}_\omega$ is a homomorphic image of G, then $\hat{F}_\omega$ is isomorphic to a closed subgroup of G.*

Proof. By assumption there exists an epimorphism $\theta: G \to \hat{F}_\omega$. Let $z_1, z_2, z_3, \cdots$ be a sequence of free generators of $\hat{F}_\omega$ that converges to 1. We have to find a sequence $y_1, y_2, y_3, \cdots$ in G that converges to 1 such that $\theta(y_i)=z_i$ for $i=1, 2, \cdots$. Having found such a sequence we can extend the map $z_i \to y_i$ to a homomorphism θ' of $\hat{F}_\omega$ into G such that $\theta' \circ \theta = Id$. Thus θ' is a monomorphism.

In order to construct the desired sequence consider a countable basis of open normal subgroups of G

$$G=G_0 \geqq G_1 \geqq G_2 \geqq G_3 \geqq \cdots .$$

Further choose a sequence $(\underline{x})=(x_1, x_2, x_3, \cdots)$ in G such that $\theta(x_i)=z_i$ for $i \geqq 1$. If H is an open subgroup of G that contains $N=\operatorname{Ker}\theta$, then almost all the x_i belong to H. Further, $N_i=N \cap G_i$ is closed in G and $N_0 \geqq N_1 \geqq N_2 \geqq \cdots$ is a basis of open normal subgroups of N. Let $(\underline{x}^{(0)})=(\underline{x})$. Assume inductively that we have already found a sequence $(\underline{x}^{(n)})=(x_1^{(n)}, x_2^{(n)}, x_3^{(n)}, \cdots)$ such that

a) $x_i^{(n)} \equiv x_i^{(n-1)} \bmod N_{n-1}$, for every $i \geqq 1$

b) Every open subgroup H of G that contains N_n contains almost all the elements of $(\underline{x}^{(n)})$.

Construct a sequence $(\underline{x}^{(n+1)})$ in the following way. The subgroup $N_n G_{n+1}$ is open in G. Hence there exists a positive integer k such that $x_i^{(n)} \in N_n G_{n+1}$ for every $i \geqq k$. The map $aN_{n+1} \to aN_n$ is an isomorphism of G_{n+1}/N_{n+1} onto $N_n G_{n+1}/N_n$. Hence for every $i \geqq k$ there exists an $x_i^{(n+1)} \in G_{n+1}$ such that $x_1^{(n+1)} \equiv x_i^{(n)} \bmod N_n$. For $i<k$ define $x_i^{(n+1)}=x_i^{(n)}$. The sequence $(\underline{x}^{(n+1)})$ thus defined satisfies condition (a). One can check that it also satisfies condition (b).

Condition (a) implies that for every $i \geqq 1$ there exists a $y_i \in G$ such that $y_i = \lim_{n \to \infty} x_i^{(n)}$. Certainly $y_i \equiv x_i \bmod N$. If H is an open subgroup of G, then there exists an m such that $G_m \subseteq H$. By (b) there exists a k such that $x_i^{(m)} \in G_m$ for every $i \geqq k$. By (a), $x_i^{(n)} \in G_m$ for every $n \geqq m$. Hence $y_i \in H$ for every $i \geqq k$. The sequence $y_1, y_2, y_3, \cdots$ is the desired one.

Thorem 3.3. *Let K be a countable Hilbertian field of characteristic zero. Then there exists an algebraic extension M of K which is ω-free and* PAC, *hence also Hilbertian. In particular $\boldsymbol{Q}$ has such an extension.*

Proof. By Theorem 4.4 of [4], K has an algebraic extension K' which is PAC and Hilbertian. By Theorem 4 of Kuyk [12], K' has algebraic extensions $L \subset L'$ such that L'/L is Galois and $\mathcal{G}(L'/L) \cong \hat{F}_\omega$. The restriction map gives therefore an epimorphism of $G(L)$ onto $\hat{F}_\omega$. By Lemma 3.2, $G(L)$ contains a

* The author is indebted to Jürgen Neukirch for calling his attention to this Lemma.

closed subgroup H which is isomorphic to $\hat{F}_\omega$. Let M be the fixed field of H. Then M is ω-free. Being a separable algebraic extension of a PAC field, M is also PAC (see Ax [1, p. 261] or [6, Lemma 4.1]). By Theorem 3.1, M is also Hilbertian.

The field $\boldsymbol{Q}$ is also Hilbertian. Hence $\boldsymbol{Q}$ has also an algebraic extension M with the above properties.

MATHEMATICAL DEPARTMENT
TEL-AVIV UNIVERSITY

References

[1] J. Ax, The elementary theory of finite fields, Annals of Math. 88 (1968), 239-271.
[2] M. Deuring, Lectures on the theory of algebraic functions of one variable, Lecture Notes in Math. 714, Springer, Heidelberg, 1973.
[3] M. Fried, On Hilbert Irreducibility Theorem, Jour. of Number Theory 6 (1974), 211-231.
[4] M. Fried and M. Jarden, Diophantine properties of subfields of $\tilde{Q}$, to appear in American Jour. of Math.
[5] M. Fried and G. Sacerdate, Solving diophantine problems over all residue class fields of a number field and all finite fields, Annals of Math. **104** (1976), 203-233.
[6] W.-D. Geyer and M. Jarden, Fields with the density property, Jour. of Algebra **35** (1975), 178-189.
[7] M. Jarden, Elementary statements over large algebraic fields, Trans. of AMS **164** (1972), 67-91.
[8] M. Jarden, Algebraic extensions of finite corank of Hilbertian fields, Israel Jour. of Math. **18** (1974), 279-307.
[9] M. Jarden, Roots of unity over large algebraic fields, Math. Annalen **213** (1975), 109-127.
[10] M. Jarden, The elementary theory of ω-free Ax fields, Ihventiones math. **38** (1976), 187-206.
[11] M. Jarden and U. Kiehne, The elementary theory of algebraic fields of finite corank, Inventiones math. **30** (1975), 275-294.
[12] W. Kuyk, Generic approach to the Galois embedding and extension problem, Jour. of Algebra **9** (1968), 393-407.
[13] S. Lang, Algebra, Addison-Wesley, Reading, Mass. 1967.