GEOMETRIC REPRESENTATION IN THE THEORY OF PSEUDO-FINITE FIELDS

ÖZLEM BEYARSLAN AND ZOÉ CHATZIDAKIS

Abstract. We study the automorphism group of the algebraic closure of a substructure A of a pseudofinite field F, or more generally, of a bounded PAC field F. This paper answers some of the questions of [1], and in particular that any finite group which is geometrically represented in a pseudo-finite field must be abelian.

Introduction. This paper investigates the relationship between model-theoretic definable closure and model-theoretic algebraic closure in certain fields. In other words: if F is a field, and $A \subseteq F$ satisfies $A = \mathrm{dcl}(A)$, what can one say of the group $\mathrm{Aut}(\mathrm{acl}(A)/A)$ of restrictions to $\mathrm{acl}(A)$ of elements of $\mathrm{Aut}(F/A)$? When is it non-trivial? A natural assumption to add is to look at a slightly smaller group, and to impose on A that it contains an elementary substructure of F. Indeed, we certainly want to impose that our automorphisms fix $\mathrm{acl}^{eq}(\emptyset)$.

This paper extends some of the results of [1], with completely new proofs, and answers some of the questions there. We investigate here the particular case of a pseudo-finite field F, or more generally, of a bounded pseudo-algebraically closed (PAC) field, i.e., a PAC field which for each integer n, has only finitely many separable algebraic extensions of degree n. Here are the main results we obtain:

THEOREM 1.7. *Let F be a bounded field, $A = \mathrm{dcl}(A)$ a subfield of F containing an elementary substructure of F, and let p be a prime dividing the order of some finite quotients of $\mathrm{Aut}(\mathrm{acl}(A)/A)$ and of $G(F)$. Then $p \neq \mathrm{char}(F)$, and the group of all primitive p^n-th roots of unity μ_{p^∞} is contained in the field F adjoined a primitive p-th root of unity ζ_p.*

THEOREM 1.8. *Let F be a pseudo-finite field, or more generally a bounded PAC field. Assume that for some subfield $A = \mathrm{dcl}(A)$ of F containing an elementary substructure of F, the group $H := \mathrm{Aut}(\mathrm{acl}(A)/A)$ is non-trivial. Assume in addition that all primes dividing the order of some finite quotient of H divide the order of some finite quotient of $\#G(F)$.*
Then H is abelian, the characteristic of F does not divide the order of any finite quotient of H, and $\mu_{p^\infty} \subset F$.

Received February 23, 2016.
2010 *Mathematics Subject Classification.* 03C60, 03C65, 12F10, 12L12.
Key words and phrases. pseudo-finite fields.

DOI:10.1017/jsl.2017.7

We give an example (2.4) which shows that the hypotheses on F cannot be weakened to assume that A contains a substucture F_0 with $\mathrm{acl}^{eq}(\emptyset) \subset \mathrm{dcl}^{eq}(F_0)$. We also give a partial answer to a question of [1] on centralisers.

§1. The results.

NOTATION 1.1. *Let F be a field. Throughout the paper,* dcl *and* acl *will denote the model-theoretic definable and algebraic closures, taken within the structure F or possibly some elementary extension of F.*
We let F^{alg} denote an algebraic closure of F (i.e., an algebraically closed field containing F and minimal such), F^s its separable closure and $G(F)$ its absolute Galois group $\mathrm{Gal}(F^s/F)$.
If $A \subset B$ are subfields of F, we denote by $\mathrm{Aut}(B/A)$ *the set of automorphisms of B which preserve all $\mathcal{L}(A)$-formulas true in F, and by* $\mathrm{Aut}_{\mathrm{field}}(B/A)$ *the set of (field) automorphisms of B which fix the elements of A. Equivalently, if F is sufficiently saturated, then* $\mathrm{Aut}(B/A)$ *is the group of restrictions to B of elements of* $\mathrm{Aut}(F/A)$.
If $p \neq$ $\mathrm{char}(F)$ *we let μ_{p^∞} denote the group of all p^n-th roots of unity, and ζ_p a primitive p-th root of unity.*
Let G_1, G_2 be profinite groups, p a prime. We say that p divides $\#G_1$ if G_1 has a finite (continuous) quotient with order divisible by p. We write $(\#G_1, \#G_2) = 1$ if there is no prime number which divides both $\#G_1$ and $\#G_2$.

DEFINITION 1.2. Let $\mathcal{L}$ be a language, T a complete theory.

(1) We say that the group G is *geometrically represented in the theory T* if there exist $M_0 \prec M \models T$ and $M_0 \subseteq A \subseteq B \subseteq M$, such that $\mathrm{Aut}(B/A) \simeq G$. We say that a *prime number p is geometrically represented in T* if p divides the order of some finite group G geometrically represented in T.
(2) A field F is *bounded* if for every integer n, F has only finitely many separable extensions of degree n. In this case we also say that $G(F)$ is *bounded*.
(3) A field F is *pseudo-algebraically closed*, henceforth abbreviated by *PAC*, if every absolutely irreducible variety defined over F has an F-rational point.
(4) A field is *pseudo-finite* if it is PAC, perfect, and has exactly one extension of degree n for each integer $n > 1$.

REMARK 1.3 (Folklore). Let F be any field, A a subfield of F, and assume that $A = \mathrm{dcl}(A)$. Then $A^s \cap F$ is a Galois extension of A, equals $\mathrm{acl}(A)$, and $\mathrm{Aut}(\mathrm{acl}(A)/A) = \mathrm{Gal}(A^s \cap F/A)$. Hence the finite groups $\mathrm{Aut}(B/A)$ as above correspond to the finite quotients of $\mathrm{Gal}(A^s \cap F/A)$.
Furthermore, F is a separable extension of A.

Indeed, if $\alpha \in \mathrm{acl}(A)$, let $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ be the conjugates of α over A. Then the symmetric polynomials in n variables evaluated at $(\alpha_1, \dots, \alpha_n)$ are in $\mathrm{dcl}(A) = A$, i.e.: α satisfies a monic separable polynomial with its coefficients in A and F contains all the roots of this polynomial. This shows the first assertion and the second assertion is immediate.
For the last assertion, assume that F is not separable over A. Then there are elements $a, a_1, \dots, a_n \in A$ which are linearly independent in the A^p-vector space A, but for some $c_1, \dots, c_n \in F$ we have $a = \sum c_i^p a_i$. This equation defines uniquely the c_i's, which must therefore belong to A.

1.4. Properties of pseudo-finite fields and bounded PAC fields. We list some of the properties of these fields that we will use all the time, often without reference. The language is the ordinary language of rings $\mathcal{L} = \{+, -, \cdot, 0, 1\}$, often expanded with parameters. Pseudo-finite fields are the infinite models of the theory of finite fields. They were studied by Ax in the 60's.

An algebraic extension of a PAC field is PAC (Corollary 11.2.5 of [4]). Theorem 20.3.3 of [4] (applied to $K = A$, $L = M = A^s \cap F$, $E = F = F$) gives the following:

Fact 1. *Let F be a PAC field, A a subfield of F over which F is separable, and assume that A has a Galois extension C such that the restriction map $G(F) \to \mathrm{Gal}(C/A)$ is an isomorphism, and $C \cap F = A$. Let $B = A^s \cap F$; then $\mathrm{Aut}_{\mathrm{field}}(B/A) = \mathrm{Aut}(B/A)$.*

It suffices to notice that $CF = F^s$, and therefore also $CB = B^s$. So, if $\varphi_0 \in \mathrm{Aut}_{\mathrm{field}}(B/A)$, extend φ_0 to $\Phi_0 \in \mathrm{Aut}_{\mathrm{field}}(B^s/CA)$ by imposing Φ_0 to be the identity on C. Then Φ_0 induces the identity on $\mathrm{Gal}(C/A) \simeq G(B)$. The result now follows immediately from 20.3.3 in [4]. It also has the following consequence:

Fact 2. *If $F_0 \subset F$ are PAC fields of the same degree of imperfection, F is separable over F_0, and the restriction map $G(F) \to G(F_0)$ is an isomorphism, then $F_0 \prec F$.*

The following remark is folklore, but for want of a good reference we will discuss it.

Fact 3. *Let $F_0 \prec F$ and assume that $G(F)$ is bounded. Then the restriction map $G(F) \to G(F_0)$ is an isomorphism.*

From $F_0 \prec F$, it follows immediately that F is a regular extension of F_0, so that the restriction map $G(F) \to G(F_0)$ is onto. Hence $G(F_0)$ is bounded. Fix an integer $n > 1$, and let $m(n)$ be the number of distinct separably algebraic extensions of F_0 of degree n. Then there is an $\mathcal{L}(F_0)$-sentence which expresses this fact: that there are $m(n)$ distinct separably algebraic extensions of F_0 of degree n, and that each separably algebraic extension of degree n is contained in one of these. As $F_0 \prec F$, F satisfies the same sentence, and this implies that $F^s = F_0^s F$, and that the restriction map $G(F) \to G(F_0)$ is an isomorphism.

Putting all these facts together, and summarising, we obtain:

Fact 4. *Let F be a PAC field, and assume that A is a subfield of F over which F is separable, and such that $(*)$: whenever L is a finite Galois extension of F, then L has a generator with minimal polynomial over F in $A[X]$. Then*

$$\mathrm{Aut}(\mathrm{acl}(A)/A) = \mathrm{Aut}_{\mathrm{fields}}(A^s \cap F/A).$$

The hypothesis $(*)$ is satisfied when F is bounded and A contains an elementary substructure of F.

Lemma 1.5. *Let F be a bounded field, and $A = \mathrm{dcl}(A)$ a subfield of F containing an elementary substructure F_0 of F, and let $B = A^s \cap F$. Then $G(A) \simeq G(F_0) \times \mathrm{Gal}(B/A)$.*

Proof. Because $G(F_0)$ is bounded and $F_0 \prec F$, we know that $F^s = F_0^s F$ and the fields F_0^s and F are linearly disjoint over F_0. Hence $B^s = F_0^s B$, the fields B and AF_0^s are linearly disjoint over A, both are Galois extensions of A, and therefore $G(A) = \mathrm{Gal}(B^s/A) \simeq G(F_0) \times \mathrm{Gal}(B/A)$. ⊣

Theorem 1.6 (Koenigsmann, Theorem 3.3 in [6]). *Let K be a field with $G(K) \simeq G_1 \times G_2$. If a prime p divides $(\#G_1, \#G_2)$, then there is a non-trivial Henselian valuation*

v on K, $\mathrm{char}(K) \neq p$, and $\mu_{p^\infty} \subset K(\zeta_p)$. Furthermore, if Kv denotes the residue field of v and $\pi : G(K) \to G(Kv)$ the canonical epimorphism, then $G(K)$ is torsion-free and $(\#\pi(G_1), \#\pi(G_2)) = 1$.

THEOREM 1.7. *Let F be a field with bounded Galois group. Assume that p is a prime number geometrically represented in $\mathrm{Th}(F)$ and that p divides $\#G(F)$. Then $\mathrm{char}(F) \neq p$, and $F(\zeta_p)$ contains μ_{p^∞}.*

PROOF. Let $F_0 \prec F$, and A a subfield of F containing F_0, with $A = \mathrm{dcl}(A)$. Let $B = A^s \cap F$, and assume that p divides $\#\mathrm{Gal}(B/A)$, as well as $\#G(F_0)$. By Lemma 1.5, we know that $G(A) \simeq G(F_0) \times \mathrm{Gal}(B/A)$. The result follows immediately from Theorem 1.6. ⊣

THEOREM 1.8. *Let F be a pseudo-finite field, or more generally a bounded PAC field. Assume that for some subfield $A = \mathrm{dcl}(A)$ of F containing an elementary substructure of F, the group $H := \mathrm{Aut}(\mathrm{acl}(A)/A)$ is non-trivial. Assume in addition that all primes dividing $\#H$ divide $\#G(F)$ (This hypothesis is alsways satisfied when F is pseudo-finite).*
Then H is abelian, and for any prime p dividing $\#H$ we have $p \neq \mathrm{char}(F)$ and $\mu_{p^\infty} \subset F$.

PROOF. Let $F_0 \prec F$, and $A = \mathrm{dcl}(A)$ a subfield of F containing F_0, let $B = A^s \cap F$, and assume that p divides $\#\mathrm{Gal}(B/A)$. By assumption, p divides $\#G(F_0)$, and by Lemma 1.5, $G(A) \simeq \mathrm{Gal}(B/A) \times G(F_0)$, with p dividing the order of both factors. Let v be the Henselian valuation on A given by Theorem 1.6, and $\pi : G(A) \to G(Av)$ the corresponding epimorphism of Galois groups. As F_0 is relatively algebraically closed in A, the valuation v restricts to a Henselian valuation on F_0; but because F_0 is PAC, the only Henselian valuation on F_0 is the trivial valuation ([4], Corollary 11.5.6). Hence $F_0 \subseteq Av$, and by Henselianity of v, $F_0^s \cap Av = F_0$. Hence the map π is an isomorphism between $G(A)$ and $G(F_0)$. It follows that $\mathrm{Gal}(BF_0^s/AF_0^s)$ is contained in $\mathrm{Ker}(\pi)$, the inertia subgroup of v, and its order is prime to the characteristic. Hence A^s is the composite of the purely residual extension AF_0^s of A, and the totally ramified extension B of A. The characteristic of F does not divide $\#\mathrm{Gal}(B/A)$, and this implies that $\mathrm{Gal}(B/A)$ is abelian: indeed, by Theorem 5.3.3 and Section 5.3 in [3], we have

$$\mathrm{Gal}(B/A) \simeq \mathrm{Gal}(BF_0^s/AF_0^s) \simeq \mathrm{Hom}(\Gamma(A^s)/\Gamma(AF_0^s)), (Aw)^{s\times}),$$

where w denotes the unique extension of v to A^s, and $\Gamma(A^s)$, $\Gamma(AF_0^s)$ the value groups $w(A^s)$ and $w(AF_0^s) = v(A)$.
We also know that $\mu_{p^\infty} \subset F(\zeta_p)$. Assume first that $G(F)$ is abelian. Then so is $G(A)$, and therefore any field between A and A^s is a Galois extension of A. In particular, because p divide $\#H$, some element $\gamma \in v(A)$ is not divisible by p in $v(A)$. Thus, if $v(a) = \gamma$, then $a^{1/p} \in A^s$, and generates a Galois extension of A: this implies that $\zeta_p \in A$, and by the above that $\mu_{p^\infty} \subset F_0$.
Assume now that $G(F)$ is arbitrary, and that $\zeta_p \notin F_0$. Then there is some $\sigma \in G(F)$ such that $\sigma(\zeta_p) \neq \zeta_p$, and the closed subgroup generated by σ has order divisible by p (here we use that p divides $\#G(F)$). Then the restriction of σ to A^s commutes with all elements of $\mathrm{Gal}(A^s/F_0^sA)$, and so we may apply the previous result to the PAC field K, subfield of F^s fixed by σ, and its elementary substructure K_0, subfield of F_0^s fixed by σ, to deduce that $\zeta_p \in K_0$, which contradicts our choice of σ. ⊣

Corollary 1.9. *Let F be a pseudo-finite field, or a bounded PAC field with $\#G(F)$ divisible by every prime number. Then every group geometrically represented in* $\mathrm{Th}(F)$ *is abelian. Furthermore, if p is a prime geometrically represented in* $\mathrm{Th}(F)$, *then $\mu_{p^\infty} \subset F$ and $p \neq \mathrm{char}(F)$.*

Corollary 1.10. *Let F be a pseudo-finite field such that if p is a prime number $\neq \mathrm{char}(F)$, then $\mu_{p^\infty} \not\subset F$. Then definable closure and algebraic closure agree on subsets of F containing an elementary substructure of F.*

§2. Other comments and remarks. As was shown in Theorem 7 of [1], if F is a pseudo-finite field not of characteristic p and containing μ_{p^∞}, then every abelian p-group is geometrically represented in $\mathrm{Th}(F)$. I.e., a certain statement about the relative algebraic closure of the prime field in F implies that p is geometrically represented in $\mathrm{Th}(F)$. Our Theorem 1.8 shows that this is an if and only if condition: which primes are geometrically represented in $\mathrm{Th}(F)$ depends uniquely on the characteristic of F and which μ_{p^∞} it contains. Moreover, by Remark 12 in [1], the class of groups geometrically represented in $\mathrm{Th}(F)$ is stable under direct products, and it follows that which groups are geometrically represented in $\mathrm{Th}(F)$ only depends on the relative algebraic closure of the prime field in F.
Remark 12 of [1] applies to any perfect PAC field F, as they do have a notion of amalgamation over models. The construction given in Theorem 7 of [1] does not use the pseudo-finiteness of F, only the fact that F is PAC. We give here again this construction, as it will be used in example 2.4.

2.1. The construction. Let F be a perfect field containing all primitive roots of unity, and consider the field K of generalized power series $F^s((t^{\mathbb{Q}}))$ over F^s. Its members are formal sums $\sum_\gamma a_\gamma t^\gamma$, with $\gamma \in \mathbb{Q}$, $a_\gamma \in F^s$, satisfying that $\{\gamma \mid a_\gamma \neq 0\}$ is well-ordered. Then K is algebraically closed. We define an action of $G(F)$ on K by setting

$$\tau(\sum_\gamma a_\gamma t^\gamma) = \sum_\gamma \tau(a_\gamma) t^\gamma$$

for all $\tau \in G(F)$. So, the subfield of K fixed by $G(F)$ coincides with $F((t^{\mathbb{Q}}))$. For each $n \in \mathbb{N}$ not divisible by the characteristic of F, choose a primitive n-th root of unity ζ_n, and choose them in a compatible way, i.e., such that $\zeta_{nm}^m = \zeta_n$. Let $\sigma \in \mathrm{Aut}(K)$ be defined by defining $\sigma(t^{1/n}) = \zeta_n t^{1/n}$ for n prime to the characteristic, and if q is a power of the characteristic, then $\sigma(t^{1/q}) = t^{1/q}$; extend σ to the multiplicative group $t^{1/n}$, $n \in \mathbb{Z}$, and then to K by setting

$$\sigma(\sum_\gamma a_\gamma t^\gamma) = \sum_\gamma a_\gamma \sigma(t^\gamma).$$

Let A be the subfield of K fixed by $G(F)$ and by σ. Then $G(A) \simeq G(F) \times \langle\sigma\rangle$, with $\langle\sigma\rangle \simeq \hat{\mathbb{Z}}$ if $\mathrm{char}(F) = 0$, $\langle\sigma\rangle \simeq \prod_{\ell \neq p} \mathbb{Z}_\ell$ if $\mathrm{char}(F) = p > 1$.

2.2. Remark. Let F be a perfect PAC field, and let A be the field constructed above in 2.1. So A contains a copy of F and is contained in $F((t^{\mathbb{Q}}))$; as $F((t^{\mathbb{Q}}))$ is a regular extension of F, it follows that F has an elementary extension F^* which contains $B = A^s \cap F((t^{\mathbb{Q}}))$. Then $\mathrm{Aut}(B/A) = \mathrm{Gal}(B/A) \simeq \langle\sigma\rangle$. This proof already appears in [1] (Theorem 7).

2.3. Comment 1. The proof of Lemma 1.5 works exactly in the same fashion as soon as the field A contains enough information about $G(F)$, more precisely:

Assume A contains $\mathrm{acl}(\emptyset)$*, and that for each finite extension L of F, there is α such that $L = F(\alpha)$ and the minimal polynomial of α over F has its coefficients in $A =$* $\mathrm{dcl}(A)$.

This hypothesis implies that A has a Galois extension C which is linearly disjoint from F over A, and is such that $CF = F^s$. Then again one has $G(A) \simeq G(F) \times \mathrm{Gal}(A^s \cap F/A)$. The proof of Theorem 1.7 goes through verbatim and gives:

If p is a prime number dividing $\mathrm{Aut}(A^s \cap F/A)$ *and dividing* $\#G(F)$*, then* $\mathrm{char}(F) \neq p$ *and* $\mu_{p^\infty} \subset F(\zeta_p)$.

We were trying to weaken the hypotheses on A in Theorem 1.8, and a natural weaker assumption is to assume that A contains a subfield F_0 such that $\mathrm{acl}^{eq}(\emptyset) \subseteq \mathrm{dcl}^{eq}(F_0)$ and $\mathrm{acl}(F_0) = F_0$. However the proof of Theorem 1.8 used in an essential way the fact that F_0 was PAC. The example below shows that this condition is not sufficient.

2.4. An example showing that the hypothesis of containing an elementary substructure is necessary. Let A_0 be a field containing $\mathbb{Q}^{alg}$, and consider $A_0^{alg}((t^{\mathbb{Q}}))$; define actions of $G(A_0)$ and of σ on $A_0^{alg}((t^{\mathbb{Q}}))$ as in 2.1 above. Then $G(A_0((t))) \simeq G(A_0) \times \langle\sigma\rangle$. Let $F_0 = \mathbb{Q}^{alg}((t))$, the subfield of $\mathbb{Q}^{alg}((t^{\mathbb{Q}}))$ fixed by σ, and $A = A_0((t))$. Then $G(F_0) \simeq \hat{\mathbb{Z}}$, and A contains F_0. Furthermore, because $G(F_0)$ is isomorphic to $\hat{\mathbb{Z}}$, there is a pseudo-finite field F which is a regular extension of F_0 (this follows easily from Theorem 23.1.1 in [4]), so that the restriction map $G(F) \to G(F_0)$ is an isomorphism. By Corollary 3.1 in [5], the theory of F eliminates imaginaries in the language augmented by constants for elements of F_0. As F_0 also contains $\mathrm{acl}(\emptyset) = \mathbb{Q}^{alg}$, it follows that $\mathrm{acl}^{eq}(\emptyset) \subset \mathrm{dcl}^{eq}(F_0)$. Furthermore, by standard results on pseudo-finite fields, F has an elementary extension F^* which contains A and is a regular extension of $B = A^{alg} \cap A_0^{alg}((t))$. Then $\mathrm{Gal}(B/A) = \mathrm{Aut}(B/A) \simeq G(A_0)$, even though $G(A_0)$ may be nonabelian.
This shows that the hypothesis of A containing an elementary substructure of F^* cannot be weakened to A containing a substructure F_0 with $\mathrm{acl}^{eq}(\emptyset) \subset \mathrm{dcl}^{eq}(\emptyset)$ and $F_0 = \mathrm{acl}(F_0)$.

2.5. Comment 2. One can wonder what happens for a bounded PAC field F with $G(F)$ not divisible by all primes. If S is the set of prime numbers $\neq \mathrm{char}(F)$ and which do not divide $\#G(F)$, and if H is a projective S-group (i.e., the order of the finite quotients of S are products of members of S), then $G(F) \times H$ is a projective profinite group. Hence F has a regular extension K which is PAC and with $G(K) \simeq G(F) \times H$ (Theorem 23.1.1 in [4]). We may also impose, if the characteristic is positive, that K and F have the same degree of imperfection. As K is a regular extension of F, the restriction map $G(K) \to G(F)$ restricts to an isomorphism on $G(F)\times(1)$, and sends $(1)\times H$ to 1. Let K_1 be the subfield of K^s fixed by $G(F) \times (1)$. Then K_1 is PAC, and because the restriction map $G(K_1) \to G(F)$ is an isomorphism, we have $F \prec K_1$. If A is the subfield of K^s fixed by $G(F) \times H$, then $A \subset F_1$, and $\mathrm{Gal}(F_1/A) = \mathrm{Aut}(F_1/A) \simeq H$.

2.6. Comment 3. Let K be a field, $H := \mathrm{Aut}(K(t)^{alg}/K(t))$, and $\sigma \in H$. Consider $H(\sigma)$, the centralizer of σ in H. Let B be the subfield of $K(t)^{alg}$ fixed by σ, $F_0 = K^{alg} \cap B$, and assume that F_0 is pseudo-finite, and that the centraliser of

$G(F_0)$ in $G(K)$ is $G(F_0)$. Because $G(B) = \langle\sigma\rangle$ projects onto $G(F_0) \simeq \hat{\mathbb{Z}}$, we have $G(B) \simeq \hat{\mathbb{Z}}$, and F_0 has an elementary extension F which is a regular extension of B. We work inside F, and are interested in $\mathrm{Aut}(B/F_0(t))$ and in $\mathrm{Aut}_{\text{field}}(B/F_0(t))$; as $B \cap F_0^{alg} = F_0$, B is linearly disjoint from $F_0^{alg}(t)$ over $F_0(t)$, and therefore $\mathrm{Aut}_{\text{field}}(B/F_0(t)) = \mathrm{Aut}(B/F_0(t))$, and its elements commute with σ.
Let U be a closed subgroup of $H(\sigma)$ such that $U \cap \langle\sigma\rangle = 1$. Then Theorem 1.8 tells us that U is abelian, and that the subfield A of B fixed by U has a nontrivial Henselian valuation v, which is trivial on F_0. Furthermore, if p divides $\#U$, then $p \neq \mathrm{char}(F_0)$ and $\mu_{p^\infty} \subset F_0$. We take the unique extension of v to A^s (and also call it v); then the residue fields Av and Bv equal F_0, and $(Av)^s = F_0^s$. Furthermore U is procyclic, because $\Gamma(A) \simeq \mathbb{Z}$, and $U \simeq \mathrm{Hom}(\mathbb{Q}/\mathbb{Z}, F_0^{s\times})$. The restriction of v to $F_0(t)$ corresponds to a point of $\mathbb{P}^1(F_0)$ (because $Av = F_0$), i.e., either $v(t-a) = 1$ for some $a \in F_0$, or $v(t) = -1$. On the other hand, the field B can carry at most one Henselian valuation (see Theorem 4.4.1 of [3]). It follows that $\mathrm{Aut}_{\text{field}}(B/F_0(t))$ is abelian, procyclic. Hence $H(\sigma)$ splits as $\langle\sigma\rangle \times \langle\tau\rangle$ for some $\tau \in \mathrm{Aut}_{\text{field}}(B/F_0(t))$.
The result generalises to any bounded PAC subfield F_0 of K with $G(F_0)$ containing its centraliser in $G(K)$, with exactly the same reasoning.

This gives a partial answer to Questions 15 and 16 of [1].

Consider $K = \mathbb{Q}$, and endow $G(\mathbb{Q}(t))$ with the Haar measure. Then the set

$$\{\tau \in G(\mathbb{Q}) \mid \mathbb{Q}^{alg}(\tau) \text{ is pseudo-finite and } C_{G(\mathbb{Q})}(\tau) = \langle\tau\rangle\}$$

has measure 1, see Theorem 18.6.1 in [4] and Corollary 2.3 in [2]. Here $\mathbb{Q}^{alg}(\tau)$ denotes the subfield of $\mathbb{Q}^{alg}$ fixed by τ. Moreover, it is easy to see that with probability 1, $\mathbb{Q}^{alg}(\tau)$ does not contain μ_{p^∞} for any prime p. Hence, with probability 1 for $\tau \in G(\mathbb{Q})$, if σ extends τ to $\mathbb{Q}(t)^{alg}$, if $B = \mathbb{Q}(t)^{alg}(\sigma)$ and $F_0 = B \cap \mathbb{Q}^{alg}$, then $\mathrm{Aut}(B/F_0(t)) = 1$, the centraliser of $\langle\sigma\rangle$ in $G(\mathbb{Q}(t))$ is $\langle\sigma\rangle$, and the theory of the pseudo-finite field F_0 does not geometrically represent any prime.

§3. **Acknowledgments.** Both authors would like to thank the Mathematical Sciences Research Institute in Berkeley for its hospitality and support during the spring 2014, when part of this research was conducted. Research at MSRI was supported by NSF grant DMS-0932078 000. The first author was partially supported by Boğaziçi BAP 14B06P1-7840. The second author was partially supported by PITN-2009-238381 and by ANR-13-BS01-0006.

REFERENCES

[1] Ö. Beyarslan and E. Hrushovski, *On algebraic closure in pseudo-finite fields*, this Journal, vol. 77 (2012), pp. 1057–1066.

[2] Z. Chatzidakis, *Some properties of the absolute Galois group of a Hilbertian field*. ***Israel Journal of Mathematics***, vol. 55 (1986), no. 2, pp. 173–183.

[3] A. J. Engler and A. Prestel, ***Valued Fields***, Springer Monographs in Mathematics, vol. 11, Springer-Verlag, Berlin, 2005.

[4] M. Fried and M. Jarden, ***Field Arithmetic***, Ergebnisse der Mathematik und ihrer Grenzgebiet, vol. 11, Springer-Verlag, Berlin, 2005.

[5] E. Hrushovski, *Pseudo-finite fields and related structures*, ***Model Theory and Applications*** (L. Bélair, Z. Chatzidakis, P. D'Aquino, D. Marker, M. Otero, F. Point, and A. Wilkie, editors), Quaderni di Matematica, vol. 11, Aracne, Rome, 2005, pp. 151–212.

[6] J. Koenigsmann, *Products of Absolute Galois Groups*. ***International Mathematics Research Notices***, vol. 24 (2005), no. 24, pp. 1465–1486.

BOĞAZIÇI UNIVERSITY
FACULTY OF ARTS AND SCIENCE
DEPARTMENT OF MATHEMATICS
34342, BEBEK-ISTANBUL, TURKEY
E-mail: ozlem.beyarslan@boun.edu.tr

CNRS (UMR 8553) - ECOLE NORMALE SUPÉRIEURE
45 RUE D'ULM
75230 PARIS CEDEX 05, FRANCE
E-mail: zchatzid@dma.ens.fr