ISRAEL JOURNAL OF MATHEMATICS 91 (1995), 273-284

A GALOIS-THEORETIC CHARACTERIZATION OF p-ADICALLY CLOSED FIELDS

BY

IDO EFRAT

The Institute of Mathematics, The Hebrew University of Jerusalem
Givat Ram, Jerusalem 91904, Israel
e-mail: efrat@math.huji.ac.il

ABSTRACT

Let p be an odd prime, K a field, and G_K its absolute Galois group. It is shown that K is p-adically closed if and only if G_K is isomorphic to an open subgroup of $G_{\mathbb{Q}_p}$. It is also shown that if $G_K \cong G_{\mathbb{F}_q((t))}$, with $q = p^r$, then K has a non-trivial henselian valuation.

Introduction

A (Krull) valuation v on a field K is called **p-adic** if $v(p) > 0$ and O_v/pO_v is finite, with O_v denoting the valuation ring of v. One says that a p-adically valued field (K, v) is **p-adically closed** if char $K = 0$ and there is no proper algebraic extension $(K_1, v_1)/(K, v)$ of valued fields such that $O_{v_1}/pO_{v_1} \cong O_v/pO_v$. The motivating examples of such fields are the finite extensions of the field $\mathbb{Q}_p$ of p-adic numbers.

The systematic study of p-adically valued fields that began in the mid-1960s revealed a beautiful analogy between their main arithmetic and model-theoretic features and those of the ordered fields, as described by Artin, Schreier and Tarski (see [PR, §1]). The Galois-theoretic aspects of the theory, however, turned out to be more difficult. It follows easily from the results of [PR] that the profinite groups occurring as the absolute Galois group $G_K = \mathrm{Gal}(\tilde{K}/K)$ of some p-adically closed field K (with $\tilde{K}$ denoting the algebraic closure of K) are precisely the open subgroups of $G_{\mathbb{Q}_p}$ (Remark 4.4). We call such a group a **p-adic group**. An explicit presentation of the p-adic groups by means of profinite generators

Received March 25, 1995

and relations was given for $p \neq 2$ by Jannsen and Wingberg [JW] (improving earlier results of Jakovlev and Koch). Diekert [Di] gave a similar presentation for the open subgroups of $G_{\mathbb{Q}_2(\sqrt{-1})}$ (and more generally for G_K where K is a finite extension of $\mathbb{Q}_2$ over which $\sqrt{-1}$ is tamely ramified).

Conversely, one came to the conjecture that if G_K is p-adic then K is p-adically closed. This stands in analogy with the classical result of Artin and Schreier [AS] which asserts that real closedness can be read off from the structure of G_K — namely, K is real closed if and only if $G_K \cong \mathbb{Z}/2\mathbb{Z}$. The first result in this direction was by Neukirch [N], who proved the conjecture for $K \subseteq \tilde{\mathbb{Q}}$. Pop [P1], in an ingenious combination of field-theoretic, geometric, and model-theoretic arguments, generalized Neukirch's result to fields K of characteristic 0 such that $\tilde{K} = K\tilde{\mathbb{Q}}$ (when $\operatorname{char} K > 0$, G_K cannot be p-adic — see §4). In addition, he proved the conjecture for fields of transcendence degree 1 over a p-adically closed field, as well as for fields which are henselian with respect to a valuation having positive residue characteristic. See [HJ, Cor. 15.2] for another special case. In this paper we prove the conjecture in general, leaving open only the case $p = 2$:

THEOREM A: *Let $p \neq 2$ and let K be a field with G_K p-adic. Then K is p-adically closed.*

The method of the proof is quite general and can be used to prove henselianity of other fields as well using only Galois-theoretic data. For instance, we prove (see Theorem 4.5 for a more precise statement):

THEOREM B: *Let q be an odd prime power and let K be a field with $G_K \cong G_{\mathbb{F}_q((t))}$. Then K is henselian with respect to a non-trivial valuation.*

Our proofs are based on a powerful valuation-theoretic construction due to Arason, Elman and Jacob [AEJ] (generalizing earlier constructions of Jacob [J] and Ware [W1]). In the p-adic case it enables us to use Pop's results.

After an earlier version of this paper had been submitted to publication and distributed, I received from Jochen Koenigsmann the preprint [Ko] in which he proves a partial analog of the construction of [AEJ] for an odd prime p. By this he proves an important case of a conjecture of the author, stating that, in general, p-rigid elements (in the sense of [W2]) give rise to p-henselian valuations with non-trivial inertia groups (relative to the maximal pro-p extension of the field). Using this Koenigsmann gives an independent proof of Theorem A which covers also the case $p = 2$.

ACKNOWLEDGEMENT: I thank Moshe Jarden and Dan Haran for carefully reading the earlier version of this paper and for several remarks concerning its presentation.

1. Preliminaries on valuation theory

We recall a few (well-known) facts which will be used in the sequel (see e.g. [E] or [P2, §1] for more details and proofs). Let $(L,u)/(K,v)$ be a Galois extension of valued fields with residue fields $\bar{L}, \bar{K}$ and value groups Δ, Γ, respectively. Let V, T, Z be the ramification, inertia and decomposition groups of u/v, respectively. Then V, T are normal subgroups of Z and $V \leq T$. If $p = \operatorname{char} \bar{K} > 0$ then V is the unique p-Sylow subgroup of T. If $\operatorname{char} \bar{K} = 0$ then $V = 1$. There is a split short exact sequence

$$1 \to T/V \to Z/V \to \operatorname{Aut}(\bar{L}/\bar{K}) \to 1$$

(where the fixed field of the image of a section is a maximal purely ramified subextension of $(L,u)/(K,v)$). As $\operatorname{Aut}(\bar{L}/\bar{K})$-modules, $T/V \cong \operatorname{Hom}(\Delta/\Gamma, \bar{L}^\times)$. In particular, T/V is abelian.

Let Ω be a set of prime numbers $\neq \operatorname{char} K$ and assume that L is closed under extracting lth roots for all $l \in \Omega$. Then the l-primary component of Δ is $\varinjlim \Gamma/l^r$. Let μ_{l^r} be the group of roots of unity over the prime field of $\bar{K}$ of order dividing l^r. Then $\mu_{l^r} \subseteq \bar{L}$ for all r. Also let $\delta_l = \dim_{\mathbb{F}_l} \Gamma/l$. For $l \neq \operatorname{char} \bar{K}$ the (unique) l-Sylow subgroup of T/V is thus isomorphic as an $\operatorname{Aut}(\bar{L}/\bar{K})$-module to

$$\operatorname{Hom}(\varinjlim \Gamma/l^r, \bar{L}^\times) \cong \varprojlim \operatorname{Hom}(\Gamma/l^r, \mu_{l^r}) \cong \left(\varprojlim \mu_{l^r}\right)^{\delta_l}.$$

We will need the following two special cases:

(i) Ω is the set of all primes $\neq \operatorname{char} K$ and L is the separable closure of K. Then $T/V \cong \prod_{l \neq \operatorname{char} \bar{K}} \left(\varprojlim \mu_{l^r}\right)^{\delta_l}$ as $G_{\bar{K}}$-modules.

(ii) $\Omega = \{l\}$, $l \neq \operatorname{char} \bar{K}$, K contains a primitive root of unity of order l, and L is the maximal pro-l Galois extension of K. By Kummer's theory, L is also the closure of K with respect to extracting lth roots. Then $V = 1$ and $T \cong \left(\varprojlim \mu_{l^r}\right)^{\delta_l}$ as $\operatorname{Aut}(\bar{L}/\bar{K})$-modules.

We denote the value group of a valuation ring O by $\Gamma(O)$.

PROPOSITION 1.1: *Let O be a henselian valuation ring on a field K with residue field $\bar{K}$ and let p be a prime number. Suppose that:*

(a) *there exists a prime number $l \neq \operatorname{char} \bar{K}$ such that $\Gamma(O)/l \neq 0$;*

(b) *every non-trivial normal closed subgroup of G_K has a non-abelian p-Sylow subgroup.*

Then $\operatorname{char} \bar{K} = p$.

Proof: Let T (resp., V) be the inertia (resp., ramification) group of (K, O) relative to the separable closure of K. As O is henselian, the corresponding decomposition group is G_K, so T is normal in G_K. From the discussion above and (a), the l-Sylow subgroup of T/V is non-trivial. Hence $T \neq 1$. By (b), T has a non-abelian p-Sylow subgroup. If $\operatorname{char} \bar{K} \neq p$ then the p-Sylow subgroup of T/V is isomorphic to that of T, yet is abelian. It follows that $\operatorname{char} \bar{K} = p$. ∎

We conclude this section with three computational observations:

LEMMA 1.2: *Let L/K be a finite extension of fields, let O be a valuation ring on L and let $n \in \mathbb{N}$. Then:*

$$(\Gamma(O){:}\, n\Gamma(O)) = (\Gamma(O \cap K){:}\, n\Gamma(O \cap K)).$$

Proof: Identify $\Gamma = \Gamma(O \cap K)$ as a subgroup of $\hat{\Gamma} = \Gamma(O)$ in the natural way. Since $\hat{\Gamma}$ is torsion-free, $\hat{\Gamma}/\Gamma \cong n\hat{\Gamma}/n\Gamma$. Hence

$$(n\hat{\Gamma}{:}\, n\Gamma) = (\hat{\Gamma}{:}\, \Gamma) \leq [L{:}\, K] < \infty.$$

Now use the fact that $(\hat{\Gamma}{:}\, n\hat{\Gamma})(n\hat{\Gamma}{:}\, n\Gamma) = (\hat{\Gamma}{:}\, \Gamma)(\Gamma{:}\, n\Gamma)$. ∎

LEMMA 1.3: *Let O be a valuation ring on a field K with residue field $\bar{K}$ and with 1-units group $U^{(1)}$. Then for every $n \in \mathbb{N}$,*

$$(\Gamma(O){:}\, n\Gamma(O)) \cdot (\bar{K}^\times{:}\, (\bar{K}^\times)^n) \leq (K^\times{:}\, (K^\times)^n).$$

When $(K^\times{:}\, (K^\times)^n) < \infty$ this is an equality if and only if $U^{(1)} \subseteq (O^\times)^n$.

Proof: The valuation map and the residue homomorphism induce (using the right-exactness of $\bullet \otimes \mathbb{Z}/n$) the exact sequences

$$1 \to O^\times/n \to K^\times/n \to \Gamma(O)/n \to 0, \quad U^{(1)}/n \to O^\times/n \to \bar{K}^\times/n \to 1,$$

respectively. The lemma follows. ∎

Valuation rings O_1, O_2 on a field K are called **comparable** if one of them contains the other.

LEMMA 1.4: *Let $O_1, \dots, O_n$ be pairwise incomparable valuation rings on a field K with residue fields $\bar{K}_1, \dots, \bar{K}_n$, respectively. Then for every $m \in \mathbb{N}$,*

$$(K^\times : (K^\times)^m) \geq \prod_{i=1}^{n} (\bar{K}_i^\times : (\bar{K}_i^\times)^m).$$

Proof: Let $S = O_1^\times \cap \cdots \cap O_n^\times$. The approximation theorem for incomparable valuations [R, p. 143, Prop. 1] says that the residue map $S \to \prod_{i=1}^n \bar{K}_i^\times$ is surjective. Therefore so is the induced map $S/S^m \to \prod_{i=1}^n \bar{K}_i^\times/(\bar{K}_i^\times)^m$. On the other hand, S/S^m embeds in $K^\times/(K^\times)^m$, whence the required inequality. ∎

2. A henselianity criterion

Let p be a prime number. We denote the maximal pro-p quotient of a profinite group G by $G(p)$. The maximal pro-p Galois extension of a field K will be denoted by $K(p)$. Thus $G_K(p) = \mathrm{Gal}(K(p)/K)$. Suppose now that $\mathrm{char}\, K \neq p$ and that K contains a primitive root of unity of order p. Consider the Galois cohomology exact sequence corresponding to the exact sequence

$$1 \to \mathbb{Z}/p \to K(p)^\times \xrightarrow{p} K(p)^\times \to 1$$

of $G_K(p)$-modules. Together with Hilbert's Theorem 90 it gives the Kummer isomorphism

$$K^\times/(K^\times)^p \cong H^1(G_K(p), \mathbb{Z}/p).$$

In particular, $\dim_{\mathbb{F}_p} K^\times/(K^\times)^p = \mathrm{rank}(G_K(p))$ [S2, I-38].

PROPOSITION 2.1: *Let p be a prime number and let (K, O) be a valued field with residue field $\bar{K}$ of characteristic $\neq p$ such that $G_{\bar{K}}(p)$ is infinite. Suppose that*

$$\sup_L \mathrm{rank}(G_L(p)) < \infty$$

with L ranging over all finite separable extensions of K. Then O is henselian.

Proof: First observe that for every finite extension L of K and for every extension of O to L, the residue field $\bar{L}$ is a finite extension of $\bar{K}$, hence $G_{\bar{L}}(p)$ is infinite. We further recall that henselianity goes down in Galois extensions, provided that the upper residue field is not separably closed [Eg, Cor. 3.5]. After replacing K by an appropriate finite Galois extension, we may therefore assume that it contains a primitive root of unity of order p. For the same reasons, if

O is not henselian then we can construct inductively a sequence of finite Galois extensions

$$(K,O) = (K_1,O_1) \subseteq (K_2,O_2) \subseteq \cdots$$

such that for each i, O has at least i extensions to K_i.

Now take n sufficiently large, let $O^{(1)},\dots,O^{(n)}$ be distinct extensions of O to $L = K_n$, and let $\bar{L}_1,\dots,\bar{L}_n$ be the corresponding residue fields. Note that $\mathrm{char}\,\bar{L}_i = \mathrm{char}\,\bar{K} \neq p$, $i = 1,\dots,n$. By [R, p. 158, Cor. 5], $O^{(1)},\dots,O^{(n)}$ are incomparable. Lemma 1.4 implies that

$$(L^\times : (L^\times)^p) \geq \prod_{i=1}^{n} (\bar{L}_i^\times : (\bar{L}_i^\times)^p).$$

Since K contains a primitive root of unity of order p, so do $L, \bar{L}_1,\dots,\bar{L}_n$. Hence,

$$\dim_{\mathbb{F}_p} L^\times/(L^\times)^p = \mathrm{rank}(G_L(p)),$$
$$\dim_{\mathbb{F}_p} \bar{L}_i^\times/(\bar{L}_i^\times)^p = \mathrm{rank}(G_{\bar{L}_i}(p)) \geq 1, \quad i = 0,\dots,n.$$

Consequently $\mathrm{rank}(G_L(p)) \geq n$, contrary to the boundness assumption. ∎

3. 2-rigidity

A non-zero element a of a field K is called **2-rigid** if $(K^\times)^2 + a(K^\times)^2 \subseteq (K^\times)^2 \cup a(K^\times)^2$. We denote the set of all $a \in K^\times$ such that a or $-a$ are *not* 2-rigid by B_K. Note that $(K^\times)^2 \cup -(K^\times)^2 \subseteq B_K$; indeed, $0 \in (K^\times)^2 - (K^\times)^2$ but $0 \notin (K^\times)^2 \cup -(K^\times)^2$, so the elements of $-(K^\times)^2$ are never 2-rigid. For a profinite group G and for $i \geq 0$ let $H^i(G) = H^i(G,\mathbb{Z}/2)$. Let B_G be the set of all $\varphi \in H^1(G)$ such that the cup product $\varphi \cup \psi = 0$ in $H^2(G)$ for some $\psi \neq 0, \varphi$.

3.1 Remarks: Let K be a field of characteristic $\neq 2$ such that $|K| \geq 7$ and let $G = G_K(2)$. For $a \in K^\times$ let $(a)_K$ be the element of $H^1(G)$ corresponding to the coset $a(K^\times)^2$ of $K^\times/(K^\times)^2$ under the Kummer isomorphism (§2).

(a) We have $K = (K^\times)^2 - (K^\times)^2$. Indeed, let $a \in K$. Since $|(K^\times)^2| \geq 3$ we can take $b \in K^\times$ such that $b^2 \neq \pm a$ to obtain:

$$a = \left(\frac{a+b^2}{2b}\right)^2 - \left(\frac{a-b^2}{2b}\right)^2 \in (K^\times)^2 - (K^\times)^2.$$

(b) Given $a, b \in K^\times$ we have $a \in (K^\times)^2 + b(K^\times)^2$ if and only if $1 \in a(K^\times)^2 - b(K^\times)^2$ and this is equivalent to $1 \in aK^2 - bK^2$ (use (a)). By [L, Ch. I, Prop.

5.1], the latter condition means that the quadratic forms $\langle a, -b\rangle$ and $\langle 1, -ab\rangle$ are K-isometric. Equivalently, $(a)_K \cup (-b)_K = 0$ in $H^2(G)$ [D].* Since $1 \in aK^2 - aK^2$ (by (a) again), we have in particular $(a)_K \cup (-a)_K = 0$ (the latter equality also holds for the exceptional fields $\mathbb{F}_3, \mathbb{F}_5$ since then $G \cong \mathbb{Z}_2$, whence $H^2(G) = 0$ [S2, I-37, Cor. 2]).

(c) Suppose that $-1 \in K^2$. By (b), $B_K/(K^\times)^2$ is mapped bijectively onto B_G via the Kummer isomorphism. ∎

Denote the multiplicative subgroup of $K^\times$ generated by B_K by $\langle B_K\rangle$. The following fundamental result is proved in [AEJ, Th. 3.8, Th. 3.9 and Lemma 4.4], taking there $T = (K^\times)^2$ (for (c) use also the remarks above; the same result but without part (c) was proved earlier by Ware in [W1, Th. 4.4]).

THEOREM 3.2 (Arason, Elman, Jacob, Ware): *Every field K has a valuation ring O_K such that:*

(a) *The 1-units of O_K are contained in $(O_K^\times)^2$.*
(b) *$\langle B_K\rangle$ is a subgroup of $O_K^\times(K^\times)^2$ of index ≤ 2.*
(c) *If $\mathrm{rank}(G_K(2)) \geq 2$ and $\mathrm{char}\, K \neq 2$ then the residue characteristic of O_K is $\neq 2$.*

Remark 3.3: (a) By a result of Berman ([B]; [M, Th. 5.8]), B_K is actually always a multiplicative group, but we shall not need this fact here.

(b) An analogous notion of a p-rigid element for an odd prime number p was given by Ware in [W2]. ∎

4. The main results

We now restrict ourselves to Galois groups of (non-archimedian) local fields, i.e., fields F which are complete with respect to a discrete valuation v with finite residue field $\mathbb{F}_q$, $q = p^n$, $n \in \mathbb{N}$. Suppose $p \neq 2$. Taking σ to be a lifting to $G_F(2)$ of the Frobenius generator of $G_{\mathbb{F}_q}(2)$, one gets from the considerations of §1 the Hasse–Iwasawa presentation

$$G_F(2) \cong \langle \sigma, \tau \mid \tau^\sigma = \tau^q\rangle_{\text{pro}-2}.$$

First we need the following group-theoretic observation:

* Delzant actually considers in [D] the cohomology groups $H^i(G_K)$, but his arguments hold literally also for $H^i(G)$.

LEMMA 4.1: *Let l be a prime number, let $\lambda \in \mathbb{Z}_l^\times$ be a non-torsion element, and let $G = \langle \sigma, \tau \mid \tau^\sigma = \tau^\lambda \rangle_{\text{pro}-l}$. Then $\mathbb{Z}_l \times \mathbb{Z}_l$ is not a closed subgroup of G.*

Proof: Let $\pi\colon G \to G/\langle \tau \rangle$ be the natural epimorphism and suppose that $\mathbb{Z}_l \times \mathbb{Z}_l \cong A \leq G$. Since $\pi(G) \cong \mathbb{Z}_l$, necessarily $A \cap \mathrm{Ker}(\pi) \neq 1$, i.e., $\tau^n \in A$ for some positive integer n. Also, $A \not\leq \langle \tau \rangle = \mathrm{Ker}(\pi)$, so there exists a positive integer m such that $\pi(\sigma^m) \in \pi(A)$. Thus $\sigma^m \in \tau^\mu A$ for some $\mu \in \mathbb{Z}_l$. Taking commutators we get:

$$[\tau^n, \sigma^{-m}\tau^\mu] = [\tau^n, \sigma^{-m}]^{\tau^\mu} = (\tau^{n(\lambda^m - 1)})^{\tau^\mu} \neq 1,$$

since $n(\lambda^m - 1) \neq 0$ in $\mathbb{Z}_l$. This contradicts the abelianity of A. ∎

LEMMA 4.2: *Let K be a field and suppose that*

$$G_K(2) \cong \langle \sigma, \tau | \, \tau^\sigma = \tau^\lambda \rangle_{\text{pro}-2}$$

with $\pm 1 \neq \lambda \in \mathbb{Z}_2^\times$. Let O_K be as in Theorem 3.2 and let $\bar{K}$ be its residue field. Then:

(a) $\mathrm{char}\, K \neq 2$;

(b) $\mathrm{char}\, \bar{K} \neq 2$.

If $-1 \in K^2$ then in addition:

(c) $B_K = (K^\times)^2$;

(d) $(\Gamma(O_K)\colon 2\Gamma(O_K)) = 2$;

(e) $G_{\bar{K}}(2) \cong \mathbb{Z}_2$.

Proof: Set $G = G_K(2)$.

(a) Apply [S2, II-5, Cor. 1].

(b) Use (a) and Theorem 3.2(c).

(c) We have $\dim_{\mathbb{F}_2} H^1(G) = \mathrm{rank}(G) = 2$ [S2, I-38]. [K, Satz 7.23] yields an $\mathbb{F}_2$-linear basis φ_1, φ_2 of $H^1(G)$ such that $\varphi_1 \cup \varphi_2 \neq 0$. As $-1 \in (K^\times)^2$ and by Remark 3.1(b), $(a)_K \cup (a)_K = (a)_K \cup (-a)_K = 0$ for every $a \in K^\times$, so $\varphi_1 \cup \varphi_1 = \varphi_2 \cup \varphi_2 = 0$. It is now straightforward to check that $B_G = 0$, so we are done by Remark 3.1(c) (note that K is infinite because of the structure of G).

(d) By the remarks in §2, $(K^\times\colon (K^\times)^2) = 4$. Therefore (c) and Theorem 3.2(b) give $(K^\times\colon O_K^\times (K^\times)^2) \geq 2$. The natural isomorphism $\Gamma(O_K)/2 \cong K^\times / O_K^\times (K^\times)^2$ hence implies that $(\Gamma(O_K)\colon 2\Gamma(O_K)) \geq 2$. Conversely, extend O_K to a valuation ring $O_K(2)$ on $K(2)$ and let V, T be the ramification and inertia group, respectively, of $O_K(2)/O_K$. As $\mathrm{char}\, \bar{K} \neq 2$ we have $V = 1$, and therefore $T \cong \mathbb{Z}_2^{\delta_2}$, where $\delta_2 = \dim_{\mathbb{F}_2} \Gamma(O_K)/2$ (see §1). Since the only roots of unity in $\mathbb{Z}_2$ are ± 1, Lemma 4.1 gives $\mathbb{Z}_2 \times \mathbb{Z}_2 \not\leq G$. Conclude that $\delta_2 \leq 1$, as required.

(e) By Theorem 3.2(a) and Lemma 1.3,

$$(\Gamma(O_K)\colon 2\Gamma(O_K)) \cdot (\bar{K}^\times\colon (\bar{K}^\times)^2) = (K^\times\colon (K^\times)^2) = 4.$$

Conclude from (d) that $(\bar{K}^\times\colon (\bar{K}^\times)^2) = 2$, i.e., $\mathrm{rank}(G_{\bar{K}}(2)) = 1$. By (b) again and the remarks in §1, $G_{\bar{K}}(2)$ embeds in $G_K(2)$. Since the latter group is a semi-direct product of $\mathbb{Z}_2$ with itself, it is torsion-free. Hence so is $G_{\bar{K}}(2)$, and we obtain $G_{\bar{K}}(2) \cong \mathbb{Z}_2$. ∎

Corollary 4.3: *Let K be a field and suppose that for every finite separable extension L of K,*

$$G_L(2) \cong \langle \sigma, \tau \mid \tau^\sigma = \tau^{\lambda_L} \rangle_{\text{pro}-2}$$

for some $\pm 1 \neq \lambda_L \in \mathbb{Z}_2^\times$. Then K has a henselian valuation ring O with residue field $\bar{K}$ satisfying $\mathrm{char}\,\bar{K} \neq 2$, $(\Gamma(O)\colon 2\Gamma(O)) = 2$ and $G_{\bar{K}}(2) \cong \mathbb{Z}_2$.

Proof: By Lemma 4.2(a), $\mathrm{char}\,K \neq 2$. Let $K_1 = K(\sqrt{-1})$ and let $\bar{K}_1$ be the residue field of O_{K_1} from Theorem 3.2. By Lemma 4.2(b), $\mathrm{char}\,\bar{K}_1 \neq 2$. We prove the corollary with $O = O_{K_1} \cap K$. For $\bar{K}$ as above, $\mathrm{char}\,\bar{K} \neq 2$. By Lemma 1.2 and Lemma 4.2(d),

$$(\Gamma(O)\colon 2\Gamma(O)) = (\Gamma(O_{K_1})\colon 2\Gamma(O_{K_1})) = 2.$$

By Lemma 4.2(e), $G_{\bar{K}_1}(2) \cong \mathbb{Z}_2$, so $G_{\bar{K}}(2)$ is infinite. Proposition 2.1 therefore shows that O is henselian. As $(K^\times\colon (K^\times)^2) = 4$, we conclude from Lemma 1.3 that $(\bar{K}^\times\colon (\bar{K}^\times)^2) \leq 2$, so $\mathrm{rank}(G_{\bar{K}}(2)) \leq 1$. It follows that $G_{\bar{K}}(2) \cong \mathbb{Z}_2$. ∎

Proof of Theorem A: Let K be a field with G_K p-adic and $p \neq 2$. By a theorem of Tate [S2, II-15, Prop. 12], $\mathrm{cd}_l(G_K) = 2$ for every prime number l. Since the absolute Galois group of a field of characteristic $l > 0$ has lth cohomological dimension ≤ 1 [S2, II-4, Prop. 3], $\mathrm{char}\,K = 0$.

By Corollary 4.3 and the Hasse–Iwasawa presentation, K is endowed with a henselian valuation O with residue field $\bar{K}$ such that $(\Gamma(O) : 2\Gamma(O)) = 2$ and $\mathrm{char}\,\bar{K} \neq 2$. By [P1, Kor. 1.5(1)], every non-trivial normal closed subgroup of a p-adic group has a closed subgroup which is a free pro-p group of countable rank. Proposition 1.1 (with $l = 2$) implies that $\mathrm{char}\,\bar{K} = p$. It follows from [P1, E9] that K is p-adically closed. ∎

Remark 4.4: As remarked in the introduction, the converse of the main theorem holds for all prime numbers p. This follows from the next two observations:
(i) If K is p-adically closed with respect to a valuation v, then $K_0 = K \cap \tilde{\mathbb{Q}}$ is p-adically closed with respect to $\mathrm{Res}_{K_0} v$ [PR, Th. 3.4] and $\mathrm{Res}_{\tilde{\mathbb{Q}}}\colon G_K \to G_{K_0}$ is an isomorphism [P1, E4].
(ii) If $K_0 \subseteq \tilde{\mathbb{Q}}$ is p-adically closed then its valuation is discrete and its completion $\hat{K}$ is thus an immediate extension of K_0. Being a complete discretely valued field of characteristic 0 with finite residue field of characteristic p, $\hat{K}$ is a finite extension of $\mathbb{Q}_p$, hence is p-adically closed. Since K_0 is henselian [PR, Th. 3.1] and the valuation is discrete, we get from the fundamental equality of valuation theory [E, Cor. 18.7] that $K_0 = \hat{K} \cap \tilde{\mathbb{Q}}$. ∎

From Corollary 4.3 and the Hasse–Iwasawa presentation we further obtain the following sharper form of Theorem B:

THEOREM 4.5: *Let q be an odd prime power and let K be a field with $G_K \cong G_{\mathbb{F}_q((t))}$. Then K is endowed with a henselian valuation O whose value group Γ and residue field $\bar{K}$ satisfy $(\Gamma\colon 2\Gamma) = 2$, $\mathrm{char}\,\bar{K} \neq 2$ and $G_{\bar{K}}(2) \cong \mathbb{Z}_2$.*

PROBLEM 4.6: *Characterize the fields K for which $G_K \cong G_{\mathbb{F}_q((t))}$ for a given prime power q.*

We remark that in general a field K with $G_K \cong G_{\mathbb{F}_q((t))}$, where $q = p^r$, need not have characteristic p. In fact we have:

PROPOSITION 4.7: *For every field K there exists a field L of characteristic 0 such that $G_K \cong G_L$.*

Proof: We may assume that $\mathrm{char}\,K > 0$. Since K and its inseparable closure have isomorphic absolute Galois groups, we may also assume that K is perfect. Let E be the quotient field of the ring of Witt vectors over K [S1, Th. II.3]. Then $\mathrm{char}\,E = 0$ and E is complete with respect to a discrete valuation v with residue field K. Denote the inertia and ramification groups of v relative to $\tilde{E}$ by T and V respectively (the decomposition group is G_E since v is necessarily henselian). By the discussion in §1, G_K embeds in G_E/V. Furthermore, by [KPR, Th. 2.2], G_E/V embeds in G_E. It follows that some algebraic extension L of E satisfies $G_K \cong G_L$. ∎

References

[AEJ] J.K. Arason, R. Elman and B. Jacob, *Rigid elements, valuations, and realization of Witt rings*, Journal of Algebra **110** (1987), 449–467.

[AS] E. Artin and O. Schreier, *Algebraische Konstruktion reeller Körper*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg **5** (1927), 85–99.

[B] L. Berman, *The Kaplansky radical and values of binary quadratic forms over fields*, Ph.D thesis, University of California, Berkeley, 1978.

[D] M. A. Delzant, *Définition des classes de Stiefel-Whitney d'un module quadratique sur un corps de charactéristique différente de* 2, Comptes Rendus de l'Academie des Sciences, Paris, Sér. A-B **255** (1962), 1366–1368.

[Di] V. Diekert, *Über die absolute Galoisgruppe dyadischer Zahlkörper*, Journal für die reine und angewandte Mathematik **350** (1984), 152–172.

[E] O. Endler, *Valuation Theory*, Springer, Berlin, 1972.

[Eg] A. Engler, *Fields with two incomparable Henselian valuation rings*, manuscripta mathematica **23** (1978), 373–385.

[HJ] D. Haran and M. Jarden, *The absolute Galois group of a pseudo p-adically closed field*, Journal für die reine und angewandte Mathematik **383** (1988), 147–206.

[J] B. Jacob, *On the structure of pythagorean fields*, Journal of Algebra **68** (1981), 247–267.

[JW] U. Jannsen and K. Wingberg, *Die Struktur der absoluten Galoisgruppe p-adischer Zahlkörper*, Inventiones mathematicae **70** (1982), 71–98.

[K] H. Koch, *Galoissche Theorie der p-Erweiterungen*, VEB, Berlin, 1970.

[Ko] J. Koenigsmann, *From p-rigid elements to valuations (with a Galois-characterisation of p-adic fields)*, preprint.

[KPR] F.-V. Kuhlmann, M. Pank and P. Roquette, *Immediate and purely wild extensions of valued fields*, manuscripta mathematica **55** (1986), 39–67.

[L] T. Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Reading, Massachusetts, 1973.

[M] M. Marshall, *Abstract Witt Rings*, Queen's Papers in Pure and Applied Mathematics, Vol. 57, Queen's University, Kingston, 1980.

[N] J. Neukirch, *Kennzeichnung der p-adischen und endlichen algebraischen Zahlkörper*, Inventiones mathematicae **6** (1969), 269–314.

[P1] F. Pop, *Galoissche Kennzeichnung p-adisch abgeschlossener Körper*, Journal für die reine und angewandte Mathematik **392** (1988), 145–175.

[P2] F. Pop, *On Grothendieck's conjecture of birational anabelian geometry*, Annals of Mathematical Logic **139** (1994), 145–182.

[PR] A. Prestel and P. Roquette, *Formally p-adic fields*, Lecture Notes in Mathematics **1050**, Springer, Berlin, 1984.

[R] P. Ribenboim, *Théorie des Valuations*, l'Université de Montréal, Montréal, 1968.

[S1] J.-P. Serre, *Local Fields*, Springer, Berlin, 1979.

[S2] J.-P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Mathematics **5**, Springer, Berlin, 1965.

[W1] R. Ware, *Valuation rings and rigid elements in fields*, Canadian Journal of Mathematics **33** (1981), 1338–1355.

[W2] R. Ware, *Galois groups of maximal p-extensions*, Transactions of the American Mathematical Society **333** (1992), 721–728.