Fields Galois-equivalent to a local field of positive characteristic

by

Ido Efrat and Ivan Fesenko

Introduction

A celebrated theorem of Artin and Schreier [AS] characterizes the fields K whose absolute Galois group G_K is isomorphic to that of $\mathbb{R}$ as the real closed fields. In the present paper we consider the analogous problem for non-archimedean local fields of positive characteristic $F = \mathbb{F}_{p^n}((t))$. We show that a field K with absolute Galois group isomorphic to G_F possesses a Henselian valuation v such that:

(1) the value group Γ of v satisfies $\Gamma/l \cong \mathbb{Z}/l$ for all prime numbers $l \neq p$;

(2) the residue field $\bar{K}$ of v has characteristic p;

(3) the maximal prime to p Galois group $G_{\bar{K}}(p')$ of $\bar{K}$ is $\hat{\mathbb{Z}}/\mathbb{Z}_p$;

(4) if $\operatorname{char} K = 0$ then $\Gamma = p\Gamma$ and $\bar{K}$ is perfect.

For every positive integer r we construct such fields K of characteristic p with $\Gamma/p \cong (\mathbb{Z}/p)^r$. Likewise we construct examples with $\Gamma \cong \mathbb{Z}$, $G_{\bar{K}} \not\cong \hat{\mathbb{Z}}$ and $\bar{K}$ imperfect.

The similar problem for p-adic fields was answered by Koenigsmann [Kn] and the first named author [E1] (for $p \neq 2$), extending earlier results by Neukirch [N2] and Pop [P1]: the fields K such that $G_K \cong G_F$ for some finite extension F of $\mathbb{Q}_p$ are precisely the p-adically closed fields in the sense of [PR].

Acknowledgement: This research was partly carried out during the first author's visit in the University of Nottingham in July 1998. He thanks the university for its hospitality.

1991 Mathematics Subject Classification: primary 11S20, secondary 12J10
Math. Res. Lett. 6 (1999), 345-356

Notation

We denote the algebraic, separable, and inseparable closures of a field K by $\tilde{K}$, $K_{\rm sep}$, and $K_{\rm ins}$, respectively. For a positive integer m with ${\rm char}\, K \not| m$ let μ_m be the group of roots of unity of order dividing m in $\tilde{K}$. For a prime l with $l \neq {\rm char}\, K$ let $\mu_{l^\infty} = \varinjlim_r \mu_{l^r}$. Given a profinite group G and a prime number l, denote the quotient $\varprojlim G/N$, where N ranges over all open normal subgroups of G with G/N abelian (resp., of l-power order, of order prime to l) by $G({\rm ab})$ (resp., $G(l)$, $G(l')$). We define $G({\rm ab}, l)$, $G({\rm ab}, l')$ similarly. For a (Krull) valuation v on K let Γ_v, O_v, and $\bar{K}_v$ be the corresponding value group, valuation ring, and residue field, respectively.

1. Galois groups of Henselian fields

We first recall several basic facts about the structure of the decomposition group of (K, v) relative to $K_{\rm sep}$ (see e.g. [Ed], [P2, §1] or [E1, §1] for more details and proofs). For simplicity we assume here that v is Henselian, i.e., the decomposition group is G_K. Let $K_{\rm ur}$ and $K_{\rm tr}$ be the maximal unramified and maximal tamely ramified Galois extensions of (K, v), respectively. If $p = {\rm char}\, \bar{K}_v > 0$ then $G_{K_{\rm tr}}$ is the unique p-Sylow subgroup of $G_{K_{\rm ur}}$. If ${\rm char}\, \bar{K}_v = 0$ then $G_{K_{\rm tr}} = 1$. There are natural short exact sequences

$$1 \to {\rm Gal}(K_{\rm tr}/K_{\rm ur}) \to {\rm Gal}(K_{\rm tr}/K) \to G_{\bar{K}_v} \to 1$$

$$1 \to G_{K_{\rm tr}} \to G_K \to {\rm Gal}(K_{\rm tr}/K) \to 1$$

which are split, by [N1] and [KPR], respectively. For a prime number l let $\delta_l = \dim_{\mathbb{F}_l} \Gamma_v/l$. Then ${\rm Gal}(K_{\rm tr}/K_{\rm ur}) \cong \prod_{l \neq {\rm char}\, \bar{K}_v} \big(\varprojlim_r \mu_{l^r}\big)^{\delta_l}$ as $G_{\bar{K}_v}$-modules. In particular, if $\Gamma_v \cong \mathbb{Z}$ and ${\rm char}\, \bar{K}_v = p > 0$ then $\delta_l = 1$ for all primes l, so the $G_{\bar{K}_v}$-module ${\rm Gal}(K_{\rm tr}/K_{\rm ur})$ is $\hat{\mu} = \varprojlim_{(m,p)=1} \mu_m$, and ${\rm Gal}(K_{\rm tr}/K) \cong \hat{\mu} \rtimes G_{\bar{K}_v}$ with the Galois action.

The analogous result for the maximal pro-l Galois group $G_K(l)$ of K is the following: If $l \neq {\rm char}\, \bar{K}_v$ is prime and $\mu_l \subseteq K$ then $G_K(l) \cong \mathbb{Z}_l^{\delta_l} \rtimes G_{\bar{K}_v}(l)$, where $\sigma \in G_{\bar{K}_v}(l)$ acts on $\tau \in \mathbb{Z}_l^{\delta_l}$ according to $\sigma\tau\sigma^{-1} = \chi_{\bar{K}_v, l}(\sigma)\tau$; here $\chi_{\bar{K}_v, l} \colon G_{\bar{K}_v}(l) \to 1 + l\mathbb{Z}_l$ is the pro-l cyclotomic character of $\bar{K}_v$, induced by the restriction homomorphism $G_{\bar{K}_v}(l) \to {\rm Aut}(\mu_{l^\infty}) \cong \mathbb{Z}_l^\times$.

Now fix a prime number p. Given a pro-p group H and a cardinal number $\mathfrak{c}$ let $F_p(H;\mathfrak{c})$ be the free H-operator pro-p group on $\mathfrak{c}$ generators, in the sense of [K1], [MSh]. The following is a modest generalization of the main result of [MSh] (which treats Laurent series fields).

Theorem 1.1: *Let (K,v) be a Henselian discretely valued field of characteristic p and let $\mathfrak{c} = \max\{\aleph_0, |\bar{K}_v|\}$. Then $G_{K_{\rm tr}} \cong F_p(\mathrm{Gal}(K_{\rm tr}/K);\mathfrak{c})$ as $\mathrm{Gal}(K_{\rm tr}/K)$-operator pro-$p$ groups; in particular, $G_K \cong F_p(\mathrm{Gal}(K_{\rm tr}/K);\mathfrak{c})\rtimes\mathrm{Gal}(K_{\rm tr}/K)$ with the canonical action.*

When $k = \bar{K}_v$ is perfect, this theorem can be proven using precisely the same argument as in [MSh, Th. 1]. We therefore omit the details. When k is not perfect, one can prove it as follows: Let u be the unique prolongation of v to $L = k_{\rm ins}K$. The restriction $G_L \to G_K$ is an isomorphism mapping $G_{L_{\rm ur}}$, $G_{L_{\rm tr}}$ onto $G_{K_{\rm ur}}$, $G_{K_{\rm tr}}$, respectively. By the result for perfect residue fields, $G_{L_{\rm tr}} \cong F_p(\mathrm{Gal}(L_{\rm tr}/L);\mathfrak{c})$ as $\mathrm{Gal}(L_{\rm tr}/L)$-operator groups. It follows that $G_{K_{\rm tr}} \cong F_p(\mathrm{Gal}(K_{\rm tr}/K);\mathfrak{c})$ as $\mathrm{Gal}(K_{\rm tr}/K)$-operator groups, as desired.

Corollary 1.2: *Let $(K_1,v_1),(K_2,v_2)$ be Henselian discretely valued fields of characteristic p, and let $\bar{K}_1,\bar{K}_2$ be the corresponding residue fields. Suppose that $G_{\bar{K}_1} \cong G_{\bar{K}_2}$, that this isomorphism is compatible with the Galois actions on the roots of unity, and that $\max\{\aleph_0,|\bar{K}_1|\} = \max\{\aleph_0,|\bar{K}_2|\}$. Then $G_{K_1} \cong G_{K_2}$.*

Proof: We have $\mathrm{Gal}(K_{1,\rm tr}/K_1) \cong \hat{\mu}\rtimes G_{\bar{K}_1} \cong \hat{\mu}\rtimes G_{\bar{K}_2} \cong \mathrm{Gal}(K_{2,\rm tr}/K_2)$ with the Galois actions. Now apply Theorem 1.1. $\square$

Proposition 1.3: *Let (K,v) be a Henselian discretely valued field of characteristic p. Suppose that $|K| = \max\{\aleph_0,|\bar{K}_v|\}$. Let L be a maximal totally tamely ramified extension of (K,v). Let (E,u) be a Henselian discretely valued field of characteristic p with $\bar{E}_u = L$. Then $G_E \cong G_K$.*

Proof: Let $\mathfrak{c} = |K| = \max\{\aleph_0,|\bar{K}_v|\}$, let $H = \hat{\mu}\rtimes G_{\bar{K}_v}$ with the Galois action, and let $V = F_p(H;\mathfrak{c})$. By Theorem 1.1, $V \cong G_{K_{\rm tr}}$ and $G_K \cong V\rtimes H$. Since $\tilde{\mathbb{F}}_p \subseteq K_{\rm tr}$, the Galois action of V on $\hat{\mu}$ is trivial. Further, the unique prolongation of v to L has residue field $\bar{K}_v$. Hence $G_L \cong V\rtimes G_{\bar{K}_v}$, and this isomorphism is compatible with the Galois action on

$\hat{\mu}$. Therefore

$$\mathrm{Gal}(E_{\mathrm{tr}}/E) \cong \hat{\mu} \rtimes G_L \cong \hat{\mu} \rtimes (V \rtimes G_{\bar{K}_v}) \cong V \rtimes (\hat{\mu} \rtimes G_{\bar{K}_v}) = V \rtimes H \quad .$$

Now from [MSh, §1, Prop. 1] we deduce that

$$\begin{aligned} F_p(V \rtimes H; \mathfrak{c}) \rtimes (V \rtimes H) &\cong (F_p(H; \mathfrak{c}) * V) \rtimes H \\ &= (F_p(H; \mathfrak{c}) * F_p(H; \mathfrak{c})) \rtimes H \cong F_p(H; \mathfrak{c}) \rtimes H = V \rtimes H \quad , \end{aligned}$$

where $*$ denotes free pro-p product. Since $|L| = |K|$, from Theorem 1.1 we deduce

$$G_E \cong F_p(\mathrm{Gal}(E_{\mathrm{tr}}/E); \mathfrak{c}) \rtimes \mathrm{Gal}(E_{\mathrm{tr}}/E) \cong F_p(V \rtimes H; \mathfrak{c}) \rtimes (V \rtimes H) \cong V \rtimes H \cong G_K \quad . \qquad \square$$

2. Existence of Henselian valuations

Let $K_2^M(E)$ be the second Milnor K-group of the field E, and let $\{\cdot,\cdot\}\colon E^\times \times E^\times \to K_2^M(E)$ be the natural symbolic map. The following theorem combines powerful constructions of Ware [Wr], Arason–Elman–Jacob [AEJ] (for $l = 2$), and Hwang–Jacob [HJ] (for $l \neq 2$); see also [E3] and [Kn].

Theorem 2.1: *Let l be a prime number, let E be a field of characteristic $\neq l$, let T be a subgroup of $E^\times$ containing $(E^\times)^l$ and -1. Suppose that:*

(i) *For every $x, y \in E^\times$ which are $\mathbb{F}_l$-linearly independent in $E^\times/T$ one has $\{x, y\} \neq 0$ in $K_2^M(E)$;*

(ii) *For every $x \in E^\times \setminus T$ and $y \in T \setminus (E^\times)^l$ one has $\{x, y\} \neq 0$ in $K_2^M(E)$.*

Then there exists a valuation u on E such that $(\Gamma_u : l\Gamma_u) \geq (E^\times : T)/l$ and $u(l) \neq 0$. Furthermore, if $\bar{E}_u = \bar{E}_u^l$ then $(\Gamma_u : l\Gamma_u) \geq (E^\times : T)$.

The **rank** of a profinite group is the minimal number (possibly ∞) of topological generators of it.

Proposition 2.2 ([E1, Prop. 2.1]): *Let l be a prime number and let (E, u) be a valued field such that* char $\bar{E}_u \neq l$ *and $G_{\bar{E}_u}(l)$ is infinite. Suppose that*

$$\sup_M \operatorname{rank} G_M(l) < \infty \quad ,$$

where M ranges over all finite separable extensions of E. Then (E, u) is Henselian.

Combining the previous two facts, we obtain the following result (which is essentially proven in [E1] for $l = 2$).

Proposition 2.3: *Let l,p be distinct prime numbers and let K be a field of characteristic $\neq l$. Let E_0 be a finite extension of K containing μ_l and containing $\sqrt{-1}$ if $l=2$. Suppose that for every finite separable extension E of E_0 one has*

$$G_E(l)\cong\langle\sigma,\tau\mid\sigma\tau\sigma^{-1}=\tau^{p^s}\rangle_{\mathrm{pro}-l}$$

for some $s=s(E)\geq 1$ such that $p^s\equiv 1 \mod l$. Then there exists a Henselian valuation v on K such that $\Gamma_v/l\cong\mathbb{Z}/l$, $\mathrm{char}\,\bar{K}_v\neq l$, and $\bar{K}_v$ is not algebraically closed.

Proof: For E as above denote $H^i(E)=H^i(G_E(l),\mathbb{Z}/l)$. We consider the cup product $H^1(E)\times H^1(E)\to H^2(E)$. Let φ_1,φ_2 be an $\mathbb{F}_l$-linear basis of $H^1(E)$ which is dual to the basis of $G_E(l)/G_E(l)^l[G_E(l),G_E(l)]$ consisting of the images of σ and τ. From the defining relation $\tau^{p^s-1}[\tau,\sigma]=1$ of $G_E(l)$ we deduce that $\varphi_1\cup\varphi_2\neq 0$ [K2, §7.8]. Furthermore, when $l\neq 2$ one has $\varphi_1\cup\varphi_1=\varphi_2\cup\varphi_2=0$ by the anti-commutativity of $\cup$. When $l=2$ we may identify $\varphi_i\cup\varphi_i$ with the class of a quaternion algebra $(a_i,a_i/E)$ in the Brauer group $\mathrm{Br}(E)$; here $a_i(E^\times)^2$ corresponds to φ_i under the Kummer isomorphism $E^\times/(E^\times)^2\cong H^1(E)$. Since $(a_i,a_i/E)=(a_i,-1/E)$ in $\mathrm{Br}(E)$ and $\sqrt{-1}\in E$ we obtain that $\varphi_i\cup\varphi_i=0$, $i=1,2$, in this case as well. Consequently, $H^2(E)\cong\wedge^2H^1(E)$.

By the Kummer theory and the Merkur'ev–Suslin theorem [MSu], this implies that $K_2^M(E)/l\cong\wedge^2(E^\times/l)$ naturally. Hence (i) and (ii) of Theorem 2.1 hold for $T=(E^\times)^l$. Since $\dim_{\mathbb{F}_l}(E^\times/(E^\times)^l)=\mathrm{rank}\,G_E(l)=2$, Theorem 2.1 therefore gives rise to a valuation u on E such that $\dim_{\mathbb{F}_l}(\Gamma_u/l)\geq 1$ and $\mathrm{char}\,\bar{E}_u\neq l$.

Furthermore, if $\bar{E}_u=\bar{E}_u^l$ then $\delta_l=\dim_{\mathbb{F}_l}(\Gamma_u/l)\geq 2$ by the last statement of Theorem 2.1. From the discussion in §1 this would imply $\mathbb{Z}_l^2\leq G_E(l)$, which is not the case [E1, Lemma 4.1]. We conclude that $G_{\bar{E}_u}(l)\neq 1$. This implies that the latter group is in fact infinite ([B]; note that when $l=2$, $\sqrt{-1}\in\bar{E}_u$). Proposition 2.2 therefore shows that (E,u) is Henselian.

Now take $E=E_0$, let u be as above, and let $v=\mathrm{Res}_K u$. Then $\dim_{\mathbb{F}_l}(\Gamma_v/l)=\dim_{\mathbb{F}_l}(\Gamma_u/l)\geq 1$ [E1, Lemma 1.2] and $\mathrm{char}\,\bar{K}_v\neq l$. Since the finite extension $\bar{E}_u$ of $\bar{K}_v$ is not algebraically closed, neither is $\bar{K}_v$. Also, Henselianity goes down in finite extensions, provided that the upper residue field is not separably closed [Eg, Cor. 3.5]. Therefore (K,v) is Henselian. □

Valuations v, v' are called **comparable** if one of $O_v, O_{v'}$ contains the other.

Proposition 2.4 (Endler–Engler [EE, Prop.]): *Let v, v' be valuations on a field K. Suppose that v is Henselian and that $\bar{K}_{v'}$ is not algebraically closed. Then v, v' are comparable.*

Lemma 2.5: *Let $(L,w)/(K,v)$ be a Galois extension of Henselian valued fields of degree n. Suppose that the norm homomorphism $N_{L/K}\colon L^\times \to K^\times$ is surjective. Then $(\Gamma_v : n\Gamma_v) = (\Gamma_w : \Gamma_v)$.*

Proof: By the Henselianity, one has a well-defined commutative square

$$\begin{array}{ccc} L^\times & \xrightarrow{w} & \Gamma_w \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle n} \\ K^\times & \xrightarrow{v} & \Gamma_v \end{array} \quad .$$

By assumption, the left vertical map is surjective. Hence so is the right vertical map; i.e., $\Gamma_v = n\Gamma_w$. By [E1, Lemma 1.2] again,

$$(\Gamma_v : n\Gamma_v) = (\Gamma_w : n\Gamma_w) = (\Gamma_w : \Gamma_v) \quad . \qquad \square$$

3. The absolute Galois group of a local field of characteristic p

From now on we fix a local field $F = \mathbb{F}_q((t))$ of characteristic $p > 0$. Let $G = G_F$, $T = G_{F_{\rm ur}}$, and $V = G_{F_{\rm tr}}$, taken with respect to the canonical discrete valuation on F. The group structure of G was described by Koch [K1] (and follows from the general considerations in §1); namely:

(i) $G = V \rtimes (G/V)$;

(ii) $T/V \cong \hat{\mathbb{Z}}/\mathbb{Z}_p$;

(iii) $G/T \cong \hat{\mathbb{Z}}$;

(iv) $G/V \cong (T/V) \rtimes (G/T)$, where a generator σ of G/T acts on a generator τ of T/V according to the Hasse–Iwasawa relation $\sigma\tau\sigma^{-1} = \tau^q$;

(v) $V \cong F_p(G/V; \aleph_0)$; in particular, V is a free pro-p group on countably many generators [MSh, §1, Lemma 4].

Proposition 3.1: (a) *T/V intersects non-trivially every non-trivial normal closed subgroup of G/V.*

(b) *T intersects non-trivially every non-trivial normal closed subgroup of G.*

Proof: (a) We need to show that if L is a Galois extension of F such that $LF_{\mathrm{ur}} = F_{\mathrm{tr}}$ then $L = F_{\mathrm{tr}}$. To this end, denote $L' = L \cap F_{\mathrm{ur}}$. Then $\mathrm{Gal}(F_{\mathrm{tr}}/L') \cong \mathrm{Gal}(F_{\mathrm{tr}}/F_{\mathrm{ur}}) \times \mathrm{Gal}(F_{\mathrm{ur}}/L')$. In particular, $\mathrm{Gal}(F_{\mathrm{tr}}/L')$ is abelian, by (ii) and (iii) above. For each positive integer m which is prime to p choose $t_m \in F_{\mathrm{tr}}$ such that $t_m^m = t$. The abelianity implies that $L'(t_m)/L'$ is normal. Since L'/F is unramified it follows that $\mu_m \subseteq L'$. Conclude that $F_{\mathrm{ur}} = \bigcup_{(m,p)=1} F(\mu_m) \subseteq L'$, whence $L = LF_{\mathrm{ur}} = F_{\mathrm{tr}}$.

(b) follows from (a). □

Lemma 3.2: *Let E be a totally ramified extension of F of prime degree l and let σ be a generator of $\mathrm{Gal}(E/F)$. Let v be the canonical valuation on E and let π be a prime element of E. Let s be the maximal integer such that the sth ramification group of $\mathrm{Gal}(E/F)$ is non-trivial. Then:*

(a) *$v((\sigma - 1)(\pi^n)) = s + n$ for every integer n relatively prime to pl;*

(b) *$E/(F + \wp(E))$ is infinite.*

Proof: (a) When $l = p$ this is proven in [FV, Ch. III, (1.4)]. Suppose $l \neq p$. Then $s = 0$ [FV, Ch. II, §4.4, Cor. 1] and $\sigma(\pi) = \zeta\pi$ for a primitive lth root of unity ζ. Hence $(\sigma - 1)(\pi^n) = (\zeta^n - 1)\pi^n$. It remains to observe that $v(\zeta^n - 1) = 0$.

(b) In all cases except $l = p = 2$ let I be the set of all integers n such that $n < -s$ and $(pl, n(s+n)) = 1$. When $l = p = 2$ let I be the set of all integers n such that $2 \not| n$ and $4 \not| s + n < 0$. Using again [FV, Ch. II, §4.4, Cor. 1] we see that I is always infinite.

We claim that the elements π^n, where $n \in I$, are distinct modulo $F + \wp(E)$. Indeed, suppose that $\pi^n - \pi^{n'} = y + \wp(x)$, with $y \in F$, $x \in E$, $n, n' \in I$, and $n < n'$. By (a),

$$0 > s + n = v((\sigma - 1)(\pi^n - \pi^{n'})) = v(\wp((\sigma - 1)(x))) \quad .$$

However, negative elements of $v(\wp(E))$ are divisible by p. Thus, we get a contradiction in all cases except $l = p = 2$.

In the remaining case $l = p = 2$ we obtain $v(x) < 0$ and hence $v((\sigma - 1)(\wp(x))) = 2v((\sigma - 1)(x))$. Since π is a primitive element for the extension E/F, we can write $x = c_0 + c_1\pi$ with $c_0, c_1 \in F$. Then

$$v((\sigma - 1)(x)) = v(c_1) + v((\sigma - 1)(\pi)) = v(c_1) + s + 1 \quad ,$$

by (a). But $2|v(c_1)$ and $2 \not| s$ [FV, Ch. III, Prop. 2.3], so $v((\sigma-1)(x))$ is even. We conclude that $4|s + n$, a contradiction. $\square$

Proposition 3.3: *V intersects non-trivially every non-trivial normal closed subgroup of G.*

Proof: (Compare [P1, Satz 1.4].) Let H be a non-trivial normal closed subgroup of G and let L be its fixed field. It follows from Proposition 3.1(b) that $LF_{\mathrm{ur}} \neq F_{\mathrm{sep}}$. Hence we can take a finite Galois extension N of F such that $N \not\subseteq LF_{\mathrm{ur}}$. Denote the maximal elementary p-abelian Galois extension of N by $N[p]$. It is a Galois extension of F. Set $K = L \cap N$ and $M = L \cap N[p]$. Then $N \not\subseteq KF_{\mathrm{ur}}$, i.e., the extension N/K has a non-trivial inertia group. Since $\mathrm{Gal}(N/K)$ is solvable, we may therefore find an intermediate field $K \subseteq N_0 \subset N$ such that N/N_0 is a totally ramified extension of prime degree. By Lemma 3.2(b), $N/(N_0 + \wp(N))$ is infinite. Hence so is $N/(K + \wp(N))$.

By the Artin–Schreier theory, the dual of the natural homomorphism $K/\wp(K) \to N/\wp(N)$ may be canonically identified with the restriction homomorphism $\mathrm{Gal}(N[p]/N) \to \mathrm{Gal}(K[p]/K)$. Since the cokernel $N/(K + \wp(N))$ of the former homomorphism is infinite, so is the kernel $\mathrm{Gal}(N[p]/K[p]N)$ of the latter homomorphism.

Now the group $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(MN/N)$ is an epimorphic image of $\mathrm{Gal}(N[p]/N)$, hence $M \subseteq K[p]$. It follows that $\mathrm{Gal}(N[p]/MN)$ is infinite. Since it is an elementary abelian p-group, it is not cyclic. Therefore the p-Sylow subgroups of $\mathrm{Gal}(LN[p]/L) \cong \mathrm{Gal}(N[p]/M)$ are not cyclic (note that as $N[p]/F$ is Galois, so are $LN[p]/L$ and $N[p]/M$). It follows that $\mathrm{Syl}_p(G_L)$ is not cyclic. On the other hand, $G_L/(G_L \cap V)$ embeds in $G/V \cong (\hat{\mathbb{Z}}/\mathbb{Z}_p) \rtimes \hat{\mathbb{Z}}$, hence its p-Sylow subgroups *are* cyclic. Conclude that $H \cap V = G_L \cap V \neq 1$, as required. $\square$

4. The main results

We still fix a local field $F = \mathbb{F}_q((t))$ of characteristic $p > 0$.

Theorem 4.1: *Let K be a field with $G_K \cong G_F$. There exists a Henselian valuation v on K such that:*

(a) $(\Gamma_v : l\Gamma_v) = l$ *for all primes* $l \neq p$*;*

(b) $\mathrm{char}\, \bar{K}_v = p$.

Proof: Fix an isomorphism $\sigma\colon G_K \to G_F$. For a separable extension E of K let E' denote the separable extension of F such that $\sigma G_E = G_{E'}$.

Let $l \neq p$ be a prime number. Then $\mathrm{cd}_l(G_K) = \mathrm{cd}_l(G_F) = 2$ [S, II-15, Prop. 12], so $\mathrm{char}\, K \neq l$ [S, II–4, Prop. 3]. Fix a finite separable extension E_l of K such that E_l, E_l' contain μ_l, and contain $\sqrt{-1}$ if $l = 2$. Then for every finite separable extension E of E_l one has

$$G_E(l) \cong G_{E'}(l) \cong \langle \sigma, \tau \mid \ \sigma\tau\sigma^{-1} = \tau^{p^s} \rangle_{\mathrm{pro}-l}$$

for some $s = s(E) \geq 1$ such that $p^s \equiv 1 \bmod l$ (namely, p^s is the cardinality of the residue field of E'; see §1). Proposition 2.3 gives rise to a Henselian valuation v_l on K such that $\Gamma_{v_l}/l \cong \mathbb{Z}/l$, $\mathrm{char}\, \bar{K}_{v_l} \neq l$, and $\bar{K}_{v_l}$ is not algebraically closed.

By Proposition 2.4, the valuations v_l, $l \neq p$, are pairwise comparable. It follows that $\bigcap_{l \neq p} O_{v_l}$ is a Henselian valuation ring on K. Let v be the corresponding valuation on K. For every prime number $l \neq p$ the fact that $O_v \subseteq O_{v_l}$ implies that Γ_{v_l} is an epimorphic image of Γ_v; hence $\dim_{\mathbb{F}_l}(\Gamma_v/l) \geq \dim_{\mathbb{F}_l}(\Gamma_{v_l}/l) = 1$. Moreover, $\mathbb{Z}_l^2 \not\leq G_{E_l}(l)$ [E1, Lemma 4.1]. We conclude as before using [E1, Lemma 1.2] and the considerations of §1 that $\dim_{\mathbb{F}_l}(\Gamma_v/l) = 1$, proving (a).

To prove (b), let T_v, V_v be the inertia and ramification groups, respectively, of v in K_{sep}/K. For every prime number $l \neq p, \mathrm{char}\, \bar{K}_v$, part (a) gives $\mathrm{Syl}_l(T_v/V_v) \cong \mathbb{Z}_l$. In particular, T_v/V_v is non-trivial. Now the closed normal subgroup $\sigma^{-1}(V)$ of G_K is free pro-p of infinite rank. According to Proposition 3.3 it intersects every non-trivial closed normal subgroup of G_K. Thus $T_v \cap \sigma^{-1}(V) \neq 1$. Since a free pro-$p$ group of rank ≥ 2 does not have non-trivial abelian closed normal subgroups, $T_v \cap \sigma^{-1}(V)$ is non-abelian. Therefore $\mathrm{Syl}_p(T_v)$ is non-abelian, which can happen only when $\mathrm{char}\, \bar{K}_v = p$. $\square$

Lemma 4.2: *Let H be a profinite group such that $\mathrm{cd}_p(H) \le 1$ and such that $\mathrm{Syl}_l(H) \cong \mathbb{Z}_l$ for all primes $l \ne p$. Then $H(p') \cong \hat{\mathbb{Z}}/\mathbb{Z}_p$.*

Proof: By [S, I-23, Prop. 16] and [FJ, Cor. 20.14], H embeds as a closed subgroup of a free profinite group $\hat{F}$. Now any closed subgroup of $\hat{F}$ isomorphic to $\mathbb{Z}_l$, $l \ne p$, is mapped bijectively by the canonical projection $\hat{F} \to \hat{F}(\mathrm{ab}, p')$. Since the induced homomorphism $H \to \hat{F}(\mathrm{ab}, p')$ breaks through $H(\mathrm{ab}, p')$, any l-Sylow subgroup of H is mapped bijectively onto an l-Sylow subgroup of $H(\mathrm{ab}, p')$. It follows that $H(\mathrm{ab}, p') \cong \prod_{l \ne p} \mathbb{Z}_l \cong \hat{\mathbb{Z}}/\mathbb{Z}_p$. Since $\mathrm{cd}(\hat{\mathbb{Z}}/\mathbb{Z}_p) \le 1$, the projection $H(p') \to H(\mathrm{ab}, p')$ has a continuous homomorphic section. Then $H(p')$ and the image of this section have the same l-Sylow subgroups, hence they coincide. Thus $H(p') \cong \hat{\mathbb{Z}}/\mathbb{Z}_p$. □

Proposition 4.3: *Let K and v be as in Theorem 4.1 and let $l \ne p$ be a prime number. Then:*

(a) $G_{\bar{K}_v}(p') \cong \hat{\mathbb{Z}}/\mathbb{Z}_p$.

(b) *For $s \ge 0$, $\mu_{l^s} \subseteq \bar{K}_v(\mu_l)$ if and only if $\mu_{l^s} \subseteq \mathbb{F}_q(\mu_l)$.*

(c) *If $\mu_l \subseteq \bar{K}_v$ then $\mu_l \subseteq \mathbb{F}_q$.*

(d) $\mathrm{Syl}_p(G_{\bar{K}_v})$ *is a non-trivial free pro-p group.*

Proof: Fix an l-Sylow extension (E_l, v_l) of (K, v) relative to K_{sep}. Denote its residue field by $\bar{E}_l$. Then $G_{\bar{E}_l} \cong \mathrm{Syl}_l(G_{\bar{K}_v})$. One has $\mu_l \subseteq E_l$ and $\mu_l \subseteq \bar{E}_l$. Also, the l-primary component of Γ_{v_l}/Γ_v is trivial. Hence [E2, Lemma 2.4(b)] and Theorem 4.1(a) give $(\Gamma_{v_l} : l\Gamma_{v_l}) = (\Gamma_v : l\Gamma_v) = l$. Take $1 \le s \le \infty$ such that $\mathrm{Im}(\chi_{\bar{E}_l, l}) = 1 + l^s\mathbb{Z}_l$ (where we make the convention $l^\infty = 0$). Then $G_{E_l} \cong \mathbb{Z}_l \rtimes G_{\bar{E}_l}$, where any $\sigma \in G_{\bar{E}_l}$ acts on the generator τ of $\mathbb{Z}_l$ according to $\sigma\tau\sigma^{-1} = \chi_{\bar{E}_l, l}(\sigma)\tau$ (see §1). It follows that $G_{E_l}(\mathrm{ab}) \cong (\mathbb{Z}_l/l^s) \times G_{\bar{E}_l}(\mathrm{ab})$.

The same analysis holds for F, so we obtain that $G_{F_l}(\mathrm{ab}) \cong (\mathbb{Z}_l/l^{s'}) \times \mathbb{Z}_l$, where F_l and s' are defined in a similar manner. Since the residue field $\bar{F}_l$ of F_l is the l-Sylow extension of $\mathbb{F}_q$, it does not contain μ_{l^∞}. Hence $s' < \infty$. If $s = \infty$ then we would obtain that $G_{\bar{E}_l}(\mathrm{ab}) \cong \mathbb{Z}_l/l^{s'}$, which is impossible at positive characteristic. We conclude that $s = s' < \infty$ and $G_{\bar{E}_l}(\mathrm{ab}) \cong \mathbb{Z}_l$. It follows that $\bar{E}_l, \bar{F}_l$ contain the same roots of unity of l-power order, and $G_{\bar{E}_l} \cong \mathbb{Z}_l$. As $\mathrm{cd}_p(G_{\bar{K}_v}) \le 1$ [S, II-4, Prop. 3], (a) follows from Lemma

4.2.

To prove (b) it remains to observe that $\mu_{l^s} \subseteq \bar{K}_v(\mu_l)$ if and only if $\mu_{l^s} \subseteq \bar{E}_l$, and likewise for $\mathbb{F}_q$ and $\bar{F}_l$.

To prove (c) assume that $\mu_l \subseteq \bar{K}_v$ and $\mu_l \not\subseteq \mathbb{F}_q$. Then $G_K(l) \cong \mathbb{Z}_l \rtimes \mathbb{Z}_l \not\cong \mathbb{Z}_l$ (§1). On the other hand, $G_F(l) \cong G_{\mathbb{F}_q}(l) \cong \mathbb{Z}_l$ [E2, Lemma 2.1], a contradiction.

Finally, we prove (d). By [S, I-37, Cor. 2], $\mathrm{Syl}_p(G_{\bar{K}_v})$ is indeed a free pro-p group. Suppose that it is trivial. Then the maximal pro-p Galois extension of $\mathbb{F}_p$ is contained in $\tilde{\mathbb{F}}_p \cap \bar{K}_v$. However, (b) and (c) imply that $\tilde{\mathbb{F}}_p \cap \bar{K}_v \subseteq \mathbb{F}_q$, a contradiction. □

Theorem 4.4: *Let K and v be as in Theorem 4.1 and suppose that* $\mathrm{char}\, K = 0$. *Then:*

(a) $\Gamma_v = p\Gamma_v$;

(b) $\bar{K}_v$ *is perfect.*

Proof: For any algebraic extension E of $K(\mu_p)$ the p-torsion part of $\mathrm{Br}(E)$ is isomorphic to $H^2(G_E, \mathbb{Z}/p) = H^2(G_{E'}, \mathbb{Z}/p) = 0$ ([S, II–4, Prop. 3]; here E' is as before the extension of F corresponding to E with respect to a fixed isomorphism $\sigma\colon G_K \to G_F$). It follows that for every Galois extension M of E of degree p, the norm homomorphism $N_{M/E}\colon M^\times \to E^\times$ is surjective (see e.g. [M, Th. 15.7]).

To prove (a), let $E = K(\mu_p)$ and let u be the unique extension of v to E. By Proposition 4.3, $\bar{K}_v$ contains only finitely many roots of unity. Hence so does its finite extension $\bar{E}_u$. It follows that $\mathrm{Gal}(\tilde{\mathbb{F}}_p\bar{E}_u/\bar{E}_u) \cong \hat{\mathbb{Z}}$. Therefore there is an unramified extension (L, w) of (E, u) of degree p; thus $\Gamma_w = \Gamma_u$. By [E1, Lemma 1.2] and by Lemma 2.5 (for the extension L/E), $(\Gamma_v : p\Gamma_v) = (\Gamma_u : p\Gamma_u) = 1$, as required.

To prove (b), let T_v, V_v be again the inertia and ramification groups, respectively, of v in G_K. By Proposition 3.3, $T_v \cap \sigma^{-1}(V) \neq 1$. From Theorem 4.1(b) we get $p \nmid (T_v : V_v)$. Since V is pro-p, these two facts imply that the pro-p group V_v is non-trivial. Therefore we can take a tower of finite extensions $K(\mu_p) \subseteq E \subset M$ such that M/E is a wildly ramified extension of degree p. Then the residue field extension $\bar{M}/\bar{E}$ is trivial. The surjectivity of $N_{M/E}\colon M^\times \to E^\times$ established above implies that $\bar{E} = \bar{M}^p = \bar{E}^p$; i.e., $\bar{E}$ is perfect. Hence so is $\bar{K}_v$. □

5. Constructions

We conclude by showing that various restrictions made in our main results in §4 are indeed necessary.

Example 5.1: For every positive integer r we construct a Henselian valued field (K_r, u_r) of characteristic p such that $G_{K_r} \cong G_F$ and $\Gamma_{u_r}/p \cong (\mathbb{Z}/p)^r$.

We first construct inductively countable Henselian discretely valued fields (K_r, v_r) as follows: Let (K_1, v_1) be a Henselization of $\mathbb{F}_q(t_1)$ with respect to the discrete valuation with uniformizer t_1. Assuming that (K_r, v_r) has already been defined, let L_r be a maximal totally tamely ramified extension of it. Then the (supernatural) degree $[L_r : K_r]$ is prime to p. Let (K_{r+1}, v_{r+1}) be a Henselization of $L_r(t_{r+1})$ with respect to its discrete valuation with uniformizer t_{r+1}. Since both L_r and K_r are countable, Proposition 1.3 implies that $G_{K_{r+1}} \cong G_{K_r}$.

Next we construct the valuations u_r on K_r inductively as follows: Take $u_1 = v_1$. Assuming that u_r has already been defined, let w_r be its unique prolongation to L_r. Let u_{r+1} be the refinement of v_{r+1} such that the residue valuation u_{r+1}/v_{r+1} on L_r is w_r [R]. Since both w_r and v_{r+1} are Henselian, so is u_{r+1} [R, pp. 210–211]. One has an exact sequence

$$0 \to \Gamma_{w_r} \to \Gamma_{u_{r+1}} \to \Gamma_{v_{r+1}} \to 0$$

of ordered abelian groups, and Γ_{w_r} is convex in $\Gamma_{u_{r+1}}$. We obtain an exact sequence of abelian groups

$$0 \to \Gamma_{w_r}/p \to \Gamma_{u_{r+1}}/p \to \Gamma_{v_{r+1}}/p \to 0 \quad .$$

Since the p-primary part of $\Gamma_{w_r}/\Gamma_{u_r}$ is trivial, $\Gamma_{w_r}/p \cong \Gamma_{u_r}/p \cong (\mathbb{Z}/p)^r$ [E2, Lemma 2.4(b)]. Combining this with $\Gamma_{v_{r+1}}/p \cong \mathbb{Z}/p$, we conclude that $\Gamma_{u_{r+1}}/p \cong (\mathbb{Z}/p)^{r+1}$, as desired.

In fact, K_r, L_r embed in a maximal totally tamely ramified extension (M_r, w_r) of the r-dimensional local field $\mathbb{F}_q((t_1))\cdots((t_r))$ with its canonical discrete valuation of rank r (see [FV, Appendix B]). By considering the restrictions of w_r to these fields one can obtain an alternative proof that $\Gamma_{u_r}/p \cong (\mathbb{Z}/p)^r$.

Example 5.2: There exists a Henselian discretely valued field (K,v) of characteristic p such that $G_K \cong G_F$, $\bar{K}_v$ is imperfect, and $G_{\bar{K}_v} \not\cong \hat{\mathbb{Z}}$. Indeed, take $(K,v)=(K_2,v_2)$ (with terminology as in Example 5.1). Then $\bar{K}_v = L_1$. Since K_1 is imperfect, so is its separable extension L_1. According to §1, $G_{L_1} \cong F_p(\hat{\mu}\rtimes G_{\mathbb{F}_q};\aleph_0)\rtimes G_{\mathbb{F}_q}$. In particular, $\mathrm{Syl}_p(G_{L_1})$ has infinite rank. Conclude that $G_{\bar{K}_v} = G_{L_1} \not\cong \hat{\mathbb{Z}}$.

Example 5.3: Let (K,v) be a complete discretely valued field. Suppose that $\mathrm{char}\,\bar{K}_v = p$, $|\bar{K}_v| \leq \aleph_0$, $G_{\bar{K}_v} \cong \hat{\mathbb{Z}}$, and $\bar{K}_v$ has the same group of roots of unity as $\mathbb{F}_q$ (e.g., this happens when K is a finite extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$). Let L/K be an arithmetically profinite totally ramified extension (for the definitions see [Wi] or [FV, Ch. III, §5]). In particular, if $[L:K]=\prod_l l^{n(l)}$, then $n(p)=\infty$ and $\sum_{l\neq p} n(l)<\infty$. The theory of fields of norms of Fontaine–Wintenberger [Wi, 3.2.3] implies that $G_L \cong G_{\bar{K}_v((X))}$. By Corollary 1.2, the latter group is isomorphic to G_F. If u is the extension of v to L, then $\Gamma_u = p\Gamma_u$ and $\Gamma_u/l \cong \mathbb{Z}/l$ for $l \neq p$ prime.

Remark 5.4: Let M be an n-dimensional local field such that its canonical valuation of rank n has residue characteristic p (cf. [FV, Appendix B]). From the discussion in §1 it follows that for every prime number $l \neq p$ one has

$$G_M(l) \cong \langle \sigma, \tau_1, \dots, \tau_n \mid \sigma\tau_i\sigma^{-1} = \tau_i^q \ ,\ \tau_i\tau_j = \tau_j\tau_i \rangle_{\mathrm{pro}-l} \quad .$$

Now let K be a field such that $G_K \cong G_M$. Similarly to the proof of Theorem 4.1 one can show that there is a Henselian valuation v on K such that $(\Gamma_v : l\Gamma_v) = l^n$ for all primes $l \neq p$ and such that $\mathrm{char}\,\bar{K}_v = p$ or 0.

References

[AS] E. Artin and O. Schreier, *Eine Kennzeichnung der reell abgeschlossenen Körper,* Abh. Math. Sem. Univ. Hamburg **5** (1927), 225–231.

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

[B] E. Becker, *Euklidische Körper und euklidische Hüllen von Körpern,* J. reine angew. Math. **268–269** (1974), 41–52.

[E1] I. Efrat, *A Galois-theoretic characterization of p-adically closed fields,* Isr. J. Math. **91** (1995), 273–284.

[E2] I. Efrat, *Pro-p Galois groups of algebraic extensions of* $\mathbb{Q}$, J. Number Th. **64** (1997), 84–99.

[E3] I. Efrat, *Construction of valuations from K-theory*, Mathematical Research Letters, to appear.

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

[EE] O. Endler and A.J. Engler, *Fields with Henselian valuation rings*, Math. Z. **152** (1977), 191–193.

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

[HJ] Y.S. Hwang and B. Jacob, *Brauer group analogues of results relating the Witt ring to valuations and Galois theory*, Canad. J. math. **47** (1995), 527–543.

[FV] I. Fesenko and S. Vostokov, *Local Fields and Their Extensions: A Constructive Approach*, AMS 1993.

[FJ] M. Fried and M. Jarden, *Field Arithmetic*, Springer, Heidelberg, 1986.

[K1] H. Koch, *Über die Galoissche Gruppe der algebraischen Abschliessung eines Potenzreihenkörpers mit endlichem konstantenkörper*, Math. Nachr. **35** (1967), 323–327.

[K2] H. Koch, *Galoissche Theorie der p-Erweiterungen*, VEB Deutscher Verlag der Wissenschaften, Berlin 1970.

[Kn] J. Koenigsmann, *From p-rigid elements to valuations (with a Galois-characterisation of p-adic fields)* (with an Appendix by F. Pop), J. reine angew. Math. **465** (1995), 165–182.

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

[M] J. Milnor, *Introduction to algebraic K-theory*, Princeton Univ. Press and Univ. Tokyo Press 1971.

[MSh] O.V. Mel'nikov and A.A. Sharomet, *The Galois group of a multidimensional local field of positive characteristic*, Matem. Sbornik **180** (1989), 1132–1147 (Russian); Math. USSR-Sb. **67** (1990), 595–610 (English translation).

[MSu] A.S. Merkur'ev and A.A. Suslin, *K-cohomology of Brauer-Severi varieties and the norm residue homomorphism*, Izv. Akad. Nauk SSSR, Ser. Mat. **46** (1982), 1011–1046 (Russian); Math. USSR Izv. **21** (1983), 307–340 (English translation).

[N1] J. Neukirch, *Zur Verzweigungstheorie der allgemeinen Krullschen Bewertungen*, Abh. Math. Sem. Univ. Hamburg **32** (1968), 207–215.

[N2] J. Neukirch, *Kennzeichnung der p-adischen und endlichen algebraischen Zahlkörper*, Invent. math. **6** (1969), 269–314.

[P1] F. Pop, *Galoissche Kennzeichnung p-adisch abgeschlossener Körper*, J. reine angew. Math. **392** (1988), 145–175.

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

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

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

[S] J.-P. Serre, *Cohomologie Galoisienne*, Lect. Notes Math. **5**, Springer 1965.

[Wi] J.-P. Wintenberger, *Le corps des normes de certaines extensions infinies des corps locaux, applications*, Ann. Sc. Ec. Norm. Sup. **16** (1983), 59–89.

[Wr] R. Ware, *Valuation rings and rigid elements in fields*, Canad. J. Math. **33** (1981), 1338–1355.

Authors' Addresses:

Department of Mathematics and Computer Science
Ben Gurion University of the Negev
P.O. Box 653, Be'er-Sheva 84105
ISRAEL

Department of Mathematics
University of Nottingham
NG7 2RD Nottingham
ENGLAND