ELSEVIER

Journal of Pure and Applied Algebra 138 (1999) 215–228

JOURNAL OF PURE AND APPLIED ALGEBRA

Finitely generated pro-p Galois groups of p-Henselian fields

Ido Efrat *

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

Communicated by M.-F. Roy; received 25 January 1997; received in revised form 22 July 1997

Abstract

Let p be a prime number, let K be a field of characteristic 0 containing a primitive root of unity of order p. Also let v be a p-henselian (Krull) valuation on K with residue characteristic p. We determine the structure of the maximal pro-p Galois group $G_K(p)$ of K, provided that it is finitely generated. This extends classical results of Demuškin, Serre and Labute.

AMS Classification: Primary 12J10; secondary 12F10, 11S20

0. Introduction

Fix a prime number p. Given a field K let $K(p)$ be the composite of all finite Galois extensions of K of p-power order and let $G_K(p) = \mathrm{Gal}(K(p)/K)$ be the maximal pro-p Galois group of K. When K is a finite extension of $\mathbb{Q}_p$ containing the roots of unity of order p the group $G_K(p)$ is generated (as a pro-p group) by $[K:\mathbb{Q}_p]+2$ elements subject to one relation, which has been completely determined by Demuškin [3, 4], Serre [20] and Labute [14].

In this paper we extend these classical results to the following more general situation: let K be a field of characteristic 0 containing the roots of unity of order p and suppose that $G_K(p)$ is finitely generated. Let v be a Krull valuation on K (of arbitrary rank) with residue characteristic p. We assume that (K,v) is *p-henselian*, i.e., that Hensel's lemma holds for all polynomials that split completely in $K(p)$ (equivalently, v has a unique prolongation to $K(p)$; cf. [2, Section 1]). We show that then $G_K(p)$ is a semi-direct product $\mathbb{Z}_p^m \rtimes G$, where m is a non-negative integer, and either:

* E-mail: efrat@math.bgu.ac.il.

0022-4049/99/$ – see front matter
PII: S0022-4049(98)00033-4

(i) $G \cong G_{K^*}(p)$ for some finite extension K^* of $\mathbb{Q}_p$ containing the pth roots of unity (and then the structure of G is known by the above-mentioned results); or

(ii) G is a finitely generated free pro-p group.

See Theorem 3.8 for a description of the action of G on $\mathbb{Z}_p^m$. Moreover, if v has rank 1 then $G_K(p) = G$ for G as in (i) or (ii) above (Theorem 3.7).

In Section 4 we apply these methods to characterize the finitely generated pro-p *absolute* Galois groups of henselian valued fields with residue characteristic p. These turn out to be the semi-direct products $\mathbb{Z}_p^m \rtimes G$ where m is a non-negative integer and G is as in (ii) above (see Theorem 4.3 for a description of the possible actions).

1. Cyclotomic pro-p pairs

In this section we introduce a formalism which will facilitate the presentation and proofs of the main results. It is motivated by the ideas of [9, 10].

Let $\mathbb{Z}_p$ and $\mathbb{Z}_p^\times$ be the additive and multiplicative groups, respectively, of the p-adic integers, and consider $1 + p\mathbb{Z}_p$ as a subgroup of $\mathbb{Z}_p^\times$.

Definition. A *cyclotomic pro-p pair* (G, θ) consists of a pro-p group G and a continuous homomorphism $\theta : G \to 1 + p\mathbb{Z}_p$. A *morphism* $\Phi : (G, \theta) \to (G', \theta')$ of cyclotomic pro-p pairs is a continuous homomorphism $\Phi : G \to G'$ such that $\theta = \theta' \circ \Phi$. We call a cyclotomic pro-p pair (G, θ) *finitely generated* if G is finitely generated as a pro-p group.

Let K be a field of characteristic $\neq p$. We denote the group of all roots of unity of order p^n (in the algebraic closure of the field K under consideration) by μ_{p^n}. Also let $\mu_{p^\infty} = \bigcup_{n=1}^{\infty} \mu_{p^n}$. Now suppose that $\mu_p \subseteq K$. Then $\mu_{p^\infty} \subseteq K(p)$. There is a natural isomorphism $\mathbb{Z}_p^\times \cong \mathrm{Aut}(\mu_p^\infty)$, where $\alpha \in \mathbb{Z}_p^\times$ corresponds to the automorphism $\zeta \mapsto \zeta^\alpha$. Therefore, the restriction $G_K(p) \to \mathrm{Aut}(\mu_{p^\infty})$ induces a continuous homomorphism $\chi_K : G_K(p) \to \mathbb{Z}_p^\times$. Since $\mu_p \subseteq K$ one has in fact $\mathrm{Im}(\chi_K) \subseteq 1 + p\mathbb{Z}_p$. We call $\mathcal{G}(K) = (G_K(p), \chi_K)$ the *cyclotomic pro-p pair of* K.

Given an extension L/K of fields of characteristic $\neq p$ containing μ_p one has $K(p) \subseteq L(p)$. Therefore, there is a continuous restriction homomorphism Res: $G_L(p) \to G_K(p)$. We observe that $\chi_L = \chi_K \circ \mathrm{Res}$ on $G_L(p)$, so Res induces a morphism Res: $\mathcal{G}(L) \to \mathcal{G}(K)$. This makes $K \mapsto \mathcal{G}(K)$ a contravariant functor from the category of fields of characteristic $\neq p$ containing μ_p to the category of cyclotomic pro-p pairs.

Definition. Let $\mathcal{G} = (\bar{G}, \bar{\theta})$ be a cyclotomic pro-p pair and let m be a cardinal number. The *semi-direct product* $\mathbb{Z}_p^m \rtimes (\bar{G}, \bar{\theta})$ is the cyclotomic pro-p pair $(\mathbb{Z}_p^m \rtimes \bar{G}, \bar{\theta} \circ \pi)$, with $\sigma \in \bar{G}$ acting on $\tau \in \mathbb{Z}_p^m$ by $\sigma\tau\sigma^{-1} = \tau^{\bar{\theta}(\sigma)}$, and where π is the natural projection $\mathbb{Z}_p^m \rtimes \bar{G} \to \bar{G}$.

Note that if $\mathcal{G}_1$ and $\mathcal{G}_2$ are isomorphic cyclotomic pro-p pairs then so are $\mathbb{Z}_p^m \rtimes \mathcal{G}_1$ and $\mathbb{Z}_p^m \rtimes \mathcal{G}_2$.

Recall that the *rank* of a profinite group G is the cardinality of a minimal set of (topological) generators of G which converges to 1. We denote the free pro-p product

of pro-p groups G_1, G_2 (i.e., their direct sum in the category of pro-p groups) by $G_1 *_p G_2$.

Lemma 1.1. *Let (F,θ) and (F',θ') be cyclotomic pro-p pairs, where F,F' are free pro-p groups of equal ranks and $\mathrm{Im}(\theta)=\mathrm{Im}(\theta')$. Then (F,θ) and (F',θ') are isomorphic.*

Proof. Let r be the rank of the pro-p group $\mathrm{Im}(\theta)=\mathrm{Im}(\theta')$ (by the structure of $1+p\mathbb{Z}_p$ one has $0\le r\le 2$). Choose $\sigma_i\in F$ such that $\theta(\sigma_i)$, $1\le i\le r$, generate $\mathrm{Im}(\theta)$, and choose elements $\sigma_i'\in F'$ such that $\theta'(\sigma_i')=\theta(\sigma_i)$ for each i. Thus $\theta'(\sigma_i)$, $1\le i\le r$, generate $\mathrm{Im}(\theta')$. Since F,F' are free pro-p groups,

$$F=\langle\sigma_1\rangle *_p\cdots *_p\langle\sigma_r\rangle *_p \mathrm{Ker}(\theta),\qquad F'=\langle\sigma_1'\rangle *_p\cdots *_p\langle\sigma_r'\rangle *_p \mathrm{Ker}(\theta').$$

In addition, $\langle\sigma_i\rangle\cong\langle\sigma_i'\rangle\cong\mathbb{Z}_p$ for each i. Since F,F' have equal ranks, $\mathrm{Ker}(\theta)\cong\mathrm{Ker}(\theta')$. Therefore there is a continuous isomorphism $\Phi:F\to F'$ such that $\Phi(\sigma_i)=\sigma_i'$, $i=1,\ldots,r$, and $\Phi(\mathrm{Ker}(\theta))=\mathrm{Ker}(\theta')$. Then $\theta=\theta'\circ\Phi$. □

2. Preliminaries in valuation theory

For a (Krull) valuation v on a field K we denote by $\bar{K}_v,\Gamma_v,O_v,\mathfrak{m}_v$ and U_v the corresponding residue field, value group, valuation ring, valuation ideal, and group of units, respectively. For an abelian group A and a positive integer n we write ${}_nA$ and A/n for the kernel and cokernel, respectively, of the map $A\xrightarrow{n}A$ of multiplication by n.

Lemma 2.1. *Let (K,v) be a valued field with $\mathrm{char}\,\bar{K}_v=p$. The valuation v and the residue homomorphism $U_v\to\bar{K}_v^\times$ induce natural exact sequences:*

$$1\to U_v/p\to K^\times/p\to\Gamma_v/p\to 0,$$

$$1\to(1+\mathfrak{m}_v)/p\to U_v/p\to\bar{K}_v^\times/p\to 1.$$

Proof. The exactness at $(1+\mathfrak{m}_v)/p$ follows from the fact that $\bar{K}_v$ does not contain pth roots of unity other than 1. The rest is straightforward from the right-exactness of the functor $\otimes\mathbb{Z}/p$ on abelian groups. □

Remark. A more general fact is proved in [18, Lemma 2.6] under the additional assumption that v is henselian.

For an abelian group Γ let $m_p(\Gamma)=\dim_{\mathbb{Z}/p}(\Gamma/p)$. The following is an immediate consequence of [6, Lemma 1.1]:

Proposition 2.2. *Let (K,v) be a p-henselian field such that $\mathrm{char}\,\bar{K}_v\ne p$ and $\mu_p\subseteq K$. Then $\mathcal{G}(K)\cong\mathbb{Z}_p^{m_p(\Gamma_v)}\rtimes\mathcal{G}(\bar{K}_v)$ naturally, where $\mathbb{Z}_p^{m_p(\Gamma_v)}$ corresponds under this isomorphism to the inertia group of v relative to $K(p)$.*

Given valuations v and u on a field K one says that v is *finer* than u, and that u is *coarser* than v, if $O_v \subseteq O_u$. When this happens, $O_v/\mathfrak{m}_u$ is a valuation ring on $\bar{K}_u$. We denote the corresponding valuation by v/u. Its residue field is $\bar{K}_v$. Moreover, for a fixed valuation u on K, the map $v \mapsto v/u$ is an order-preserving bijection between the refinements of u and the valuations on $\bar{K}_u$ (the partial order being "finer than"; cf. [1, Ch. VI, Section 4.1]). The valuation v is p-henselian if and only if both u and v/u are p-henselian [2, Lemma 1.3]. For valuations v, u on K such that v is finer than u one has a short exact sequence of ordered abelian groups

$$0 \to \Gamma_{v/u} \to \Gamma_v \to \Gamma_u \to 0,$$

and $\Gamma_{v/u}$ is an isolated (i.e., convex) subgroup of Γ_v [1, Ch. VI, Section 4.3]. Using the right-exactness of $\otimes \mathbb{Z}/p$ and the convexity of $\Gamma_{v/u}$ we obtain the exact sequence

$$0 \to \Gamma_{v/u}/p \to \Gamma_v/p \to \Gamma_u/p \to 0. \qquad (*)$$

There is an order-preserving bijection between the prime ideals of a valuation ring O_v and the coarsenings of v; it is given by $\mathfrak{p} \mapsto u$, where O_u is the localization $(O_v)_{\mathfrak{p}}$ of O_v at $\mathfrak{p}$ [1, Ch. VI, Section 4.1, Proposition 1].

A valuation v on a field K has *rank* 1 if it has no proper coarsenings other than the trivial valuation; equivalently, Γ_v embeds in $\mathbb{R}$ as an ordered group [1, Ch. VI, Section 4.5, Proposition 7]. It is often possible to reduce to such valuations by means of the following "slicing" technique:

Proposition 2.3. *Let (K, v) be a p-henselian field such that* $\operatorname{char} K = 0$, $\operatorname{char} \bar{K}_v = p$, *and $\mu_p \subseteq K$. There exists a p-henselian valuation u on K with residue field E such that*:

(i) *u is coarser than v;*
(ii) $\operatorname{char} E = 0$;
(iii) $\mu_p \subseteq E$;
(iv) $\mathcal{G}(K) \cong \mathbb{Z}_p^{m_p(\Gamma_u)} \rtimes \mathcal{G}(E)$ *naturally*;
(v) *E is p-henselian with respect to a valuation w of rank* 1 *such that* $\operatorname{char} \bar{E}_w = p$;
(vi) *Γ_u/p is a quotient of Γ_v/p;*
(vii) *Γ_w/p is a subquotient of Γ_v/p;*
(viii) $\operatorname{rank}(G_K(p)) = m_p(\Gamma_u) + \operatorname{rank}(G_E(p))$.

Proof. Denote the collection of all prime ideals $\mathfrak{p}$ in O_v with $p \in \mathfrak{p}$ (resp., $p \notin \mathfrak{p}$) by A^+ (resp., A^-). We have $\mathfrak{m}_v \in A^+$ and $0 \in A^-$. Moreover, $A^- \cup A^+$ is totally ordered by inclusion [1, Ch. VI, Section 4.1, Corollary to Proposition 1]. Consequently, A^+ contains a minimal element $\mathfrak{p}^+$ and A^- contains a maximal element $\mathfrak{p}^-$. Let u^+, u^- be the coarsenings of v corresponding to $\mathfrak{p}^+, \mathfrak{p}^-$, respectively. Note that u^- is coarser than u^+. We check the assertions with $u = u^-$, $E = \bar{K}_u = \bar{K}_{u^-}$, and $w = u^+/u^-$.

Assertion (i) is trivial, and the p-henselianity of u^- and w follows from the preceding remarks. Next we have $1/p \in (O_v)_{\mathfrak{p}^-} = O_{u^-}$ and $1/p \notin (O_v)_{\mathfrak{p}^+} = O_{u^+}$. This shows that $\operatorname{char} E \neq p$ and $\operatorname{char} \bar{E}_w = \operatorname{char} \bar{K}_{u^+} = p$. In particular we get (ii).

Also, (iii) follows from (ii), and (iv) follows from Proposition 2.2, (ii) and (iii).

To see that w has rank 1 use the natural order-preserving bijections between

(1) valuations on E which are coarser than v/u^-;

(2) valuations on K which are finer than u^- and coarser than v;

(3) prime ideals in O_v containing $\mathfrak{p}^-$.

Since there are no prime ideals between $\mathfrak{p}^-$ and $\mathfrak{p}^+$, there is no non-trivial valuation on E which is strictly coarser than $w = u^+/u^-$, as desired.

(vi) is immediate from (*) above.

To prove (vii) use (*) to obtain that Γ_w/p is a subgroup of Γ_{u^+}/p and that Γ_{u^+}/p is a quotient of Γ_v/p.

Finally, denote the maximal elementary p-abelian quotients of $G_K(p)$ and $G_E(p)$ by $G_K[p]$ and $G_E[p]$ respectively. Then $\operatorname{rank}(G_K(p)) = \operatorname{rank}(G_K[p])$ and $\operatorname{rank}(G_E(p)) = \operatorname{rank}(G_E[p])$ [21, I-37, Proposition 25]. But by (iv), $G_K[p] \cong \mathbb{Z}_p^{m_p(\Gamma_u)} \times G_E[p]$, so (viii) follows. □

The following is a pro-p version of the Hensel–Rychlik lemma for p-henselian fields.

Lemma 2.4. *Let (K,v) be a p-henselian valued field of characteristic $\neq p$ such that $\mu_p \subseteq K$. Then $1 + p^2\mathfrak{m}_v \subseteq K^p$.*

Proof. Let $0 \neq a \in \mathfrak{m}_v$ and consider the polynomial $f(X) = (1 + paX)^p - 1 - p^2a$. We have $f(X) = p^2a[-1 + X + aX^2g(X)]$ for some polynomial $g(X) \in O_v[X]$. Since $f(X)$ splits completely in $K(p)$, so does $h(X) = -1 + X + aX^2g(X)$. Moreover, $v(h(1)) > 0$ and $v(h'(1)) = 0$. The p-henselianity of (K,v) therefore yields $b \in K$ such that $h(b) = 0$. Then $f(b) = 0$, i.e., $1 + p^2a = (1 + pab)^p \in K^p$. □

3. Maximal pro-p Galois groups

In this section we compute the structure of the finitely generated groups $G_K(p)$ where (K,v) is a p-henselian field of characteristic 0 containing μ_p such that $\operatorname{char}\bar{K}_v = p$. We first consider the case where v has rank 1. As a starting point we record the following result which is implicit in [18, Kor. 2.7]; note that the assumption there that (K,v) is henselian is actually not needed in the proof (since it is not needed in Lemma 2.1 above).

Proposition 3.1 (Pop). *Let K be a valued field of characteristic 0 such that $(K^\times : (K^\times)^p) < \infty$. Let v be a valuation on K with $\operatorname{char}\bar{K}_v = p$. Then $\bar{K}_v$ is perfect. If in addition v has rank 1 then either:*

(a) *$\Gamma_v \cong \mathbb{Z}$ and $\bar{K}_v$ is finite; or*

(b) *$\Gamma_v = p\Gamma_v$.*

Accordingly, our computation for valuations of rank 1 will break into cases (a) and (b) of Proposition 3.1. We start with the easier case (a). Denote the p-adic valuation on $\mathbb{Q}_p$ by v_p.

Proposition 3.2. *Let (K,v) be a p-henselian field of characteristic 0. Suppose that $\Gamma_v \cong \mathbb{Z}$ and that $\bar{K}_v$ is a finite extension of $\mathbb{F}_p$. Let (K^*,v^*) be the completion of (K,v). Then:*

(a) *$G_{K^*}(p) \cong G_K(p)$ by restriction.*

(b) *(K^*,v^*) is a finite extension of $(\mathbb{Q}_p, v_p)$.*

(c) *If $\mu_p \not\subseteq K^*$ then $G_K(p)$ is a free pro-p group.*

Proof. By the p-henselianity, $\mathrm{Res}_{K^* \cap K(p)} v^*$ is the unique prolongation of v to $K^* \cap K(p)$. As v^*/v is immediate, so is $\mathrm{Res}_{K^* \cap K(p)} v^*/v$. Moreover, since $\Gamma_v \cong \mathbb{Z}$ this extension is defectless [1, Ch. VI, Section 8.5, Corollary 1]. It follows that $K = K^* \cap K(p)$. Therefore [11, Lemma 2.3] implies (a).

Now $(\overline{K^*})_{v^*} \cong \bar{K}_v$ and $\Gamma_{v^*} \cong \mathbb{Z}$. By the universal property of the ring $\mathcal{W}(\bar{K}_v)$ of Witt vectors over $\bar{K}_v$ [22, Ch. II, Section 5, Theorem 4], O_{v^*} is a free module of finite rank over $\mathcal{W}(\bar{K}_v)$. The quotient field K^* of O_{v^*} is therefore a finite extension of the quotient field of $\mathcal{W}(\bar{K}_v)$, hence also a finite extension of $\mathbb{Q}_p$. Furthermore, $O_{v^*} \cap \mathbb{Q}_p$ is a valuation ring on $\mathbb{Q}_p$ containing $\mathbb{Z}_p = \mathcal{W}(\bar{K}_v) \cap \mathbb{Q}_p$ and not containing $1/p$. Consequently, $\mathbb{Z}_p = O_{v^*} \cap \mathbb{Q}_p$. This proves (b).

Assertion (c) now follows from a result of Šafarevič ([19, 21, II-30, Theorem 3]). □

For the case $\Gamma_v = p\Gamma_v$ we first need the following technical lemma:

Lemma 3.3. *Let (K,v) be a valued field such that $(K^\times : (K^\times)^p) < \infty$ and $\bar{K}_v = \bar{K}_v^p$. There exists $0 < \lambda \in \Gamma_v$ such that for every $u \in U_v$ one can find $w \in U_v$ satisfying $v(w^p - u) \geq \lambda$.*

Proof. Let R be a system of representatives for the cosets of U_v/U_v^p. By Lemma 2.1, $|R| < \infty$. Since $\bar{K}_v^\times = (\bar{K}_v^\times)^p$, for every $a \in R$ we can find $w_a \in U_v$ such that the residues $\bar{a}$, $\bar{w}_a$ of a, w_a, respectively, satisfy $\bar{w}_a^p = \bar{a}$. Thus $\lambda = \min\{v(w_a^p - a) \mid a \in R\} > 0$.

Now given $u \in U_v$ we can write $u = az^p$ for some $a \in R$ and some $z \in U_v$. Let $w = w_a z$. We have $v(w^p - u) = v(w_a^p - a) \geq \lambda$. □

Recall that if $\mathrm{char}\, K \neq p$ and $\mu_p \subseteq K$ then $K^\times/p \cong H^1(G_K(p), \mathbb{Z}/p)$ (see e.g. [8, (1.7)]). In particular, $(K^\times : (K^\times)^p) < \infty$ if and only if $G_K(p)$ is finitely generated [21, I-38, Corollary].

Proposition 3.4. *Let K be a field of characteristic 0 containing μ_p and such that $G_K(p)$ is finitely generated. Let v be a p-henselian valuation on K satisfying $\mathrm{char}\, \bar{K}_v = p$ and $\Gamma_v = p\Gamma_v$. Then $G_K(p)$ is a free pro-p group.*

Proof.

Case I: v has rank 1. Let L/K be a cyclic extension of degree p and let $N : L \to K$ be the norm map. Let $\hat{v}$ be the unique prolongation of v to L. By the p-

henselianity,

$$p\Gamma_{\hat{v}} = \hat{v}(N(L^\times)) \leq \Gamma_v = p\Gamma_v \leq p\Gamma_{\hat{v}},$$

so $p\Gamma_{\hat{v}} = p\Gamma_v$. Since $\Gamma_{\hat{v}}$ is torsion-free this implies $\Gamma_v = \Gamma_{\hat{v}}$.

By [25, p. 725, Remark] it suffices to show that $N(L) = K$. By Proposition 3.1, $\bar{K}_v = \bar{K}_v^p$. Hence, in light of Lemma 2.1, $K^\times = (1 + \mathfrak{m}_v)(K^\times)^p$. It therefore suffices to show that $1 + \mathfrak{m}_v \subseteq N(1 + \mathfrak{m}_{\hat{v}})$.

Fix $\alpha \in L$ with $\alpha^p \in K$ and $L = K(\alpha)$. After dividing α by an appropriate element of K, we may thus assume that $\hat{v}(\alpha) = 0$. Let $0 < \lambda \in \Gamma_v$ be as in Lemma 3.3.

Now take $a \in 1 + \mathfrak{m}_v$ and assume that $a \notin N(1 + \mathfrak{m}_{\hat{v}})$. We construct inductively sequences $b_1, b_2, \ldots \in \mathfrak{m}_v$ and $c_1, c_2, \ldots \in 1 + \mathfrak{m}_{\hat{v}}$ such that for every n,

$$v(b_{n+1}) \geq v(b_n) + \lambda, \qquad a = (1 + b_n)N(c_n).$$

First we take $b_1 = a - 1$ and $c_1 = 1$. Suppose that b_n, c_n have already been defined. Necessarily, $b_n \neq 0$. Use the p-divisibility of Γ_v to choose $0 \neq \pi_n \in \mathfrak{m}_v$ such that $v(b_n) = pv(\pi_n)$ and let $u_n = b_n/(\pi_n\alpha)^p$. Then $u_n \in U_v$. By the choice of λ there exists $w_n \in U_v$ such that $v(w_n^p + u_n) \geq \lambda$. We define

$$b_{n+1} = \frac{(\pi_n\alpha)^p(w_n^p + u_n)}{1 - (\pi_n w_n \alpha)^p}, \qquad c_{n+1} = c_n(1 - \pi_n w_n \alpha).$$

Then

$$v(b_{n+1}) = pv(\pi_n) + v(w_n^p + u_n) \geq v(b_n) + \lambda > 0$$

and $c_{n+1} \in 1 + \mathfrak{m}_{\hat{v}}$. Furthermore,

$$1 + b_n = 1 + (\pi_n\alpha)^p u_n = (1 + b_{n+1})[1 - (\pi_n w_n \alpha)^p].$$

But $X^p - (\pi_n w_n \alpha)^p = \prod_{\sigma \in \mathrm{Gal}(L/K)}(X - \pi_n w_n \sigma(\alpha))$. In particular, $1 - (\pi_n w_n \alpha)^p = N(1 - \pi_n w_n \alpha)$. Therefore

$$a = (1 + b_n)N(c_n) = (1 + b_{n+1})N(1 - \pi_n w_n \alpha)N(c_n) = (1 + b_{n+1})N(c_{n+1}),$$

completing the construction.

Since v has rank 1, the group Γ_v embeds in $\mathbb{R}$. As $0 < \lambda$ we therefore have $v(b_n) > 2v(p)$ for n sufficiently large. Then $1 + b_n \in (K^\times)^p$ by Lemma 2.4. Moreover, $(1 + \mathfrak{m}_v) \cap (K^\times)^p = (1 + \mathfrak{m}_v)^p$ by Lemma 2.1. It follows that $1 + b_n \in (1 + \mathfrak{m}_v)^p$. Consequently, $a = (1 + b_n)N(c_n) \in N(1 + \mathfrak{m}_{\hat{v}})$, contradiction.

Case II: v arbitrary. Let u, E and w be as in Proposition 2.3. Thus $\mathrm{char}\, E = 0$, $\mu_p \subseteq E$, and w is a p-henselian valuation of rank 1 on E with residue characteristic p. By condition (viii) of Proposition 2.3, $G_E(p)$ is finitely generated. Furthermore, by conditions (vi) and (vii) of Proposition 2.3 and the assumptions, $\Gamma_u = p\Gamma_u$ and $\Gamma_w = p\Gamma_w$. By condition (iv), $G_K(p) \cong G_E(p)$. Case 1 (applied with respect to (E, w)) implies that this is a free pro-p group. □

Corollary 3.5. *Let K be a field of characteristic 0 containing μ_p and such that $G_K(p)$ is finitely generated. Let v be a p-henselian valuation on K and suppose that $\bar{K}_v = \bar{K}_v^p$ and $\Gamma_v = p\Gamma_v$. Then $G_K(p)$ is a free pro-p group.*

Proof. When $\operatorname{char}\bar{K} = p$ this follows from Proposition 3.4. When $\operatorname{char}\bar{K}_v \neq p$ the assumptions imply that $\mu_p \subseteq \bar{K}_v$ and $G_{\bar{K}_v}(p) = 1$, so we are done by Proposition 2.2. □

Combining Propositions 3.1, 3.2, and 3.4 we obtain:

Corollary 3.6. *Let K be a field of characteristic 0 containing μ_p and such that $G_K(p)$ is finitely generated. Let v be a p-henselian valuation on K of rank 1 and with $\operatorname{char}\bar{K}_v = p$. Then either:*

(a) *$\Gamma_v \cong \mathbb{Z}$, $\bar{K}_v$ is finite, the completion (K^*, v^*) of (K, v) is a finite extension of $(\mathbb{Q}_p, v_p)$, and* Res: $\mathcal{G}(K^*) \to \mathcal{G}(K)$ *is an isomorphism; or*

(b) *$\Gamma_v = p\Gamma_v$, $\bar{K}_v$ is perfect, and $G_K(p)$ is a free pro-p group.*

We now come to the first characterization theorem:

Theorem 3.7. *Let $\mathcal{G}$ be a finitely generated cyclotomic pro-p pair. The following conditions are equivalent:*

(a) *There exists a p-henselian valued field (K, v) such that v has rank 1, $\operatorname{char}K = 0$, $\operatorname{char}\bar{K}_v = p$, $\mu_p \subseteq K$, and $\mathcal{G}(K) \cong \mathcal{G}$;*

(b) *either $\mathcal{G} \cong \mathcal{G}(K^*)$ for some finite extension K^* of $\mathbb{Q}_p(\mu_p)$, or $\mathcal{G} \cong (F, \theta)$ for some finitely generated free pro-p group F and a continuous homomorphism θ: $F \to 1 + p\mathbb{Z}_p$.*

Proof. (a) $\Rightarrow$ (b): This follows from Corollary 3.6.

(b) $\Rightarrow$ (a): If $\mathcal{G} \cong \mathcal{G}(K^*)$ for some finite extension K^* of $\mathbb{Q}_p(\mu_p)$ then (a) is clear.

Next suppose that $\mathcal{G} \cong (F, \theta)$ with F and θ as in (b). Let K_0 be the inertia field of $\mathbb{Q}_p(\mu_p)$ relative to $(\mathbb{Q}_p(\mu_p))(p)$. The Galois extension $\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p(\mu_p)$ is totally ramified [22, Ch. IV, Proposition 17]. Hence K_0 and $\mathbb{Q}_p(\mu_{p^\infty})$ are linearly disjoint over $\mathbb{Q}_p(\mu_p)$. Moreover, it follows from [22, Ch. IV, Proposition] again that the map $\chi_{\mathbb{Q}_p(\mu_p)}: G_{\mathbb{Q}_p(\mu_p)}(p) \to 1 + p\mathbb{Z}_p$ is surjective. By the linear disjointness, $\chi_{K_0}: G_{K_0}(p) \to 1 + p\mathbb{Z}_p$ is also surjective.

Now take a subfield K_1 of $K_0(\mu_{p^\infty})/K_0$ such that $\operatorname{Im}(\chi_{K_1}) = \operatorname{Im}(\theta)$. Thus χ_{K_1} induces an isomorphism $\operatorname{Gal}(K_0(\mu_{p^\infty})/K_1) \xrightarrow{\sim} \operatorname{Im}(\theta)$. Let r be the rank of $\operatorname{Im}(\theta)$ (by the structure of $1 + p\mathbb{Z}_p$, $0 \leq r \leq 2$). Choose elements σ_i, $1 \leq i \leq r$, of $G_{K_1}(p)$ whose restrictions to $K_0(\mu_{p^\infty})$ generate $\operatorname{Gal}(K_0(\mu_{p^\infty})/K_1)$. Set $l = \operatorname{rank}(F)$ and observe that $l \geq r$. By local class field theory (cf. [6, Proposition 1.3] or [5, Proposition 2.3]), $G_{K_0}(p)$ is a free pro-p group of countable rank. We can therefore choose $\sigma_{r+1}, \ldots, \sigma_l \in \operatorname{Gal}(K_0(p)/K_0(\mu_{p^\infty}))$ such that $\langle \sigma_1, \ldots, \sigma_l \rangle$ is a free pro-p group of rank l. For the fixed field K of $\langle \sigma_1, \ldots, \sigma_l \rangle$ in $K_0(p)$ we have $\operatorname{Im}(\chi_K) = \operatorname{Im}(\theta)$. Lemma 1.1 therefore implies that $\mathcal{G}(K) \cong (F, \theta)$. □

For valuations of arbitrary rank we have:

Theorem 3.8. *The following conditions on a finitely generated cyclotomic pro-p pair $\mathcal{G}$ are equivalent*:

(a) $\mathcal{G} \cong \mathcal{G}(K)$ *for some p-henselian valued field* (K,v) *such that* $\operatorname{char} K = 0$, $\operatorname{char} \bar{K}_v = p$ *and* $\mu_p \subseteq K$;

(b) $\mathcal{G} \cong \mathbb{Z}_p^m \rtimes \bar{\mathcal{G}}$, *where* m *is a non-negative integer, and where either* $\bar{\mathcal{G}} \cong \mathcal{G}(K^*)$ *for some finite extension* K^* *of* $\mathbb{Q}_p(\mu_p)$, *or* $\bar{\mathcal{G}} \cong (F,\theta)$ *for some finitely generated free pro-p group* F *and a continuous homomorphism* $\theta : F \to 1 + p\mathbb{Z}_p$.

Proof. (a) $\Rightarrow$ (b): Let (K,v) be as in (a), take u, E, w be as in Proposition 2.3. Then $m = m_p(\Gamma_u) < \infty$, $G_E(p)$ is finitely generated, and $\mathcal{G}(K) \cong \mathbb{Z}_p^m \rtimes \mathcal{G}(E)$. By Theorem 3.7, $\bar{\mathcal{G}} = \mathcal{G}(E)$ is as in (b).

(b) $\Rightarrow$ (a): Theorem 3.7 yields a p-henselian valued field (E,w) such that $\operatorname{char} E = 0$, $\operatorname{char} \bar{E}_w = p$, $\mu_p \subseteq E$, and $\mathcal{G}(E) \cong \bar{\mathcal{G}}$. Set $\Gamma = \mathbb{Z}^m$ and order it lexicographically with respect to the usual ordering on $\mathbb{Z}$. Let $K = E((\Gamma))$ be the field of all formal power series $\alpha = \sum_{\gamma \in \Gamma} a_\gamma t^\gamma$ with $a_\gamma \in E$ and with $\{\gamma \in \Gamma \mid a_\gamma \neq 0\}$ well-ordered. When $\alpha \neq 0$ we define $u(\alpha) = \min\{\gamma \in \Gamma \mid a_\gamma \neq 0\}$. We also set $u(0) = \infty$. Then (K,u) is henselian with $\bar{K}_u \cong E$ and $\Gamma_u = \Gamma$. By Proposition 2.2,

$$\mathcal{G}(K) \cong \mathbb{Z}_p^{m_p(\Gamma)} \rtimes \mathcal{G}(E) \cong \mathbb{Z}_p^m \rtimes \bar{\mathcal{G}} \cong \mathcal{G}.$$

Let v be the unique valuation on K which is finer than u and such that $v/u = w$; it is p-henselian and $\bar{K}_v = \bar{E}_w$ has characteristic p (see Section 2). □

4. Absolute Galois groups

In this section we determine the structure of the finitely generated pro-p *absolute* Galois groups of henselian fields with residue characteristic p. This structure is somewhat simpler than that of the maximal pro-p Galois groups, as given in Theorem 3.8.

For a pro-p group G let $H^i(G) = H^i(G, \mathbb{Z}/p)$ be the ith pro-p cohomology group, with $\mathbb{Z}/p$ considered as a trivial G-module. For a field K we abbreviate $H^i(K) = H^i(G_K(p))$. We first need two computational facts.

Lemma 4.1. *Let* (K,v) *be a p-henselian valued field such that* $\operatorname{char} \bar{K}_v \neq p$, $\mu_p \subseteq K$, $\dim_{\mathbb{F}_p} H^1(K) \geq 3$, *and* $H^2(K) \cong \mathbb{Z}/p$. *Then* $m_p(\Gamma_v) = 0$.

Proof. Let $d = \dim_{\mathbb{F}_p} H^1(\bar{K}_v)$, $m = m_p(\Gamma_v)$ and $l = m(m-1)/2$ (when m is an infinite cardinal number, $l = m$). By [23, Theorem 3.6 and Remark 3.14],

$$H^1(K) \cong H^1(\bar{K}_v) \oplus H^0(\bar{K}_v)^m,$$

$$H^2(K) \cong H^2(\bar{K}_v) \oplus H^1(\bar{K}_v)^m \oplus H^0(\bar{K}_v)^l.$$

Taking $\mathbb{F}_p$-dimensions and observing that $H^0(\bar{K}_v)\cong\mathbb{Z}/p$ we obtain that $d+m\geq 3$ and $md+l\leq 1$. This can happen only when $m=0$. □

Given a field K we denote its absolute Galois group by G_K and its algebraic closure by $\tilde{K}$.

Proposition 4.2. *Let (K,v) be a henselian field such that G_K is a pro-p group of finite rank ≥ 3 and $H^2(K)\cong\mathbb{Z}/p$. Then* $\operatorname{char}\bar{K}_v\neq p$ *and* $m_p(\Gamma_v)=0$.

Proof. As $H^2(K)\cong\mathbb{Z}/p$ we have $\operatorname{char}K\neq p$ by [21, II-4, Proposition 3]. Since $[K(\mu_p):K]$ is prime to p and G_K is pro-p necessarily $\mu_p\subseteq K$. By [21, I-38, Corollary], $\dim_{\mathbb{F}_p}H^1(K)\geq 3$. In light of Lemma 4.1 it suffices to show that $\operatorname{char}\bar{K}_v\neq p$.

Suppose that $\operatorname{char}\bar{K}_v=p$ (whence $\operatorname{char}K=0$). Proposition 2.3 yields a p-henselian valuation u on K and a p-henselian valuation w of rank 1 on $E=\bar{K}_u$ such that $\operatorname{char}E=0$, $\mu_p\subseteq E$, and $\mathcal{G}(K)\cong\mathbb{Z}_p^{m_p(\Gamma_u)}\rtimes\mathcal{G}(E)$. But by Lemma 4.1 again (applied with respect to (K,u)), $m_p(\Gamma_u)=0$. Thus $\mathcal{G}(K)\cong\mathcal{G}(E)$. As G_K is pro-p, the p-henselian field (K,u) is in fact henselian. Therefore there is a natural epimorphism $G_K\to G_E$, implying that G_E is pro-p and $G_K\cong G_E$. Consequently, G_E is not a free pro-p group [21, I-37, Corollary 2]. Corollary 3.6 now implies that (E,w) embeds inside a finite extension (E^*,w^*) of $(\mathbb{Q}_p,v_p)$. By Krasner's lemma, $\widetilde{E^*}=\tilde{\mathbb{Q}}E^*=\tilde{E}E^*$. It follows that $\operatorname{Res}:G_{E^*}\to G_E$ is injective. However G_E is a pro-p group while G_{E^*} is not. We thus obtain the desired contradiction. □

Theorem 4.3. *The following conditions on a cyclotomic pro-p pair $\mathcal{G}$ are equivalent:*

(a) *There exists a henselian valued field (K,v) such that G_K is a finitely generated pro-p group,* $\operatorname{char}\bar{K}_v=p$, *and $\mathcal{G}(K)\cong\mathcal{G}$;*

(b) *$\mathcal{G}\cong\mathbb{Z}_p^m\rtimes(F,\theta)$ for some non-negative integer m, a finitely generated free pro-p group F, and a continuous homomorphism $\theta:F\to 1+p\mathbb{Z}_p$.*

Proof. (a)$\Rightarrow$(b): If G_K is a finitely generated free pro-p group then (b) holds with $m=0$ and $(F,\theta)=\mathcal{G}(K)$. So suppose that G_K is not a free pro-p group. As in the proof of Proposition 4.2, $\operatorname{char}K=0$ and $\mu_p\subseteq K$.

Let u, $E=\bar{K}_u$ and w be as in Proposition 2.3. Then $m_p(\Gamma_u)<\infty$ and $G_E(p)$ is finitely generated. As G_K is pro-p, so is G_E, whence (E,w) is henselian. Applying Proposition 4.2 with respect to (E,w) we obtain that G_E cannot be a pro-p group of finite rank ≥ 3 such that $H^2(E)\cong\mathbb{Z}/p$. In particular, it is not of the form $G_{K^*}(p)$, with K^* a finite extension of $\mathbb{Q}_p(\mu_p)$ [21, II-30, Theorem 4]. It follows from Theorem 3.7 that $\mathcal{G}(E)\cong(F,\theta)$ with F, θ as in (b). Then $\mathcal{G}\cong\mathbb{Z}_p^{m_p(\Gamma_u)}\rtimes(F,\theta)$.

(b)$\Rightarrow$(a): For $\mathcal{G}$ as in (b) Theorem 3.8 yields a p-henselian valued field (K,v) such that $\operatorname{char}K=0$, $\operatorname{char}\bar{K}_v=p$, $\mu_p\subseteq K$ and $\mathcal{G}\cong\mathcal{G}(K)$. In fact, in the construction there, v is henselian. Let $\tilde{v}$ be a prolongation of v to $\tilde{K}$. Since $G_K(p)$ is a free pro-p group this epimorphism has a homomorphic section $s:G_K(p)\to G_K$. Let K' be the fixed field in $\tilde{K}$ of the image of s. Then $G_{K'}$ is a finitely generated pro-p group

and $\mathrm{Res}\,\mathcal{G}(K') \to \mathcal{G}(K)$ is an isomorphism. Consequently, $\mathcal{G}(K') \cong \mathcal{G}$. Since $(K, \mathrm{Res}_K \tilde{v})$ is henselian so is its algebraic extension $(K', \mathrm{Res}_{K'} \tilde{v})$. Furthermore, the residue field of $(K', \mathrm{Res}_{K'} \tilde{v})$ is an algebraic extension of $\bar{K}_v$, hence has characteristic p. This proves (a). □

In a similar manner one obtains:

Theorem 4.4. *The following conditions on a cyclotomic pro-p pair $\mathcal{G}$ are equivalent:*

(a) *There exists a henselian valued field (K, v) such that G_K is a finitely generated pro-p group,* $\mathrm{char}\,\bar{K}_v = p$, *$v$ has rank* 1, *and $\mathcal{G}(K) \cong \mathcal{G}$;*

(b) *$\mathcal{G} \cong (F, \theta)$ for some finitely generated free pro-p group F and a continuous homomorphism $\theta : F \to 1 + p\mathbb{Z}_p$.*

Proof. (a) $\Rightarrow$ (b): As in the proof of Theorem 4.2 we may assume that $\mathrm{char}\,K = 0$ and $\mu_p \in K$. By Proposition 4.2 and [21, II-30, Theorem 4], G_K cannot be isomorphic to $G_{K^*}(p)$ for any finite extension K^* of $\mathbb{Q}_p(\mu_p)$. By Theorem 3.7, $\mathcal{G}$ is as in (b).

(b) $\Rightarrow$ (a): This can be shown precisely like the corresponding part of the proof of Theorem 4.3, using in the proof Theorem 3.7 instead of Theorem 3.8 (note that an algebraic extension of a valued field of rank 1 also has rank 1 [1, Ch. VI, Section 8.1, Corollary 1]). □

5. Applications

5.1. Ramification groups

Recall that the ramification group of a Galois extension $(L, u)/(K, v)$ of valued fields consists of all $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(x)/x \in 1 + \mathfrak{m}_u$ for all $0 \neq x \in L$. When K a finite extension of $\mathbb{Q}_p$ and $L = K(p)$, it follows from local class field theory that the ramification group of the canonical valuations is a free pro-p group [5, Proposition 2.3]. The following result extends this fact.

Theorem 5.1. *Let K be a field of characteristic* 0 *containing μ_p and such that $G_K(p)$ is finitely generated. Let v be a p-henselian valuation on K of rank* 1. *Then the ramification group of v relative to $K(p)$ is a free pro-p group.*

Proof. In an arbitrary Galois extension of valued fields with residue characteristic $l > 0$ the ramification group is pro-l; when the residue characteristic is 0, this group is trivial [7, Theorem 20.18]. Therefore, if in our case $\mathrm{char}\,\bar{K}_v \neq p$ then the ramification group of v in the pro-p extension $K(p)/K$ is trivial. We may thus assume that $\mathrm{char}\,\bar{K}_v = p$. Then the ramification group coincides with the inertia group of v in $K(p)/K$ [7, Theorem 20.18]. In light of Corollary 3.6 we may also assume that $(K, v) \subseteq (K^*, v^*)$ for some finite extension (K^*, v^*) of $(\mathbb{Q}_p, v_p)$ containing μ_p such that $\mathrm{Res} : G_{K^*}(p) \to G_K(p)$ is an isomorphism and v^*/v is immediate. Let T, T^* be the ramification groups of

$(K,v),(K^*,v^*)$ relative to $K(p),K^*(p)$, respectively. One has a natural commutative diagram of group extensions:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & T^* & \longrightarrow & G_{K^*}(p) & \longrightarrow & G_{\bar{K}_v}(p) & \longrightarrow & 1 \\ & & \Big\downarrow{\scriptstyle \mathrm{Res}} & & \Big\downarrow{\scriptstyle \mathrm{Res}} & & \Big\| & & \\ 1 & \longrightarrow & T & \longrightarrow & G_K(p) & \longrightarrow & G_{\bar{K}_v}(p) & \longrightarrow & 1\ . \end{array}$$

Since the middle vertical map is an isomorphism, so is the left vertical map. But as remarked above, T^* is a free pro-p group. □

5.2. Finitely generated Demuškin groups as pro-p Galois groups

Recall that a pro-p group G is a *Demuškin group* if $H^2(G)\cong\mathbb{Z}/p$ and the cup-product $\bigcup: H^1(G)\times H^1(G)\to H^2(G)$ is non-degenerate. For example, if K is a finite extension of $\mathbb{Q}_p(\mu_p)$ then $G_K(p)$ is a pro-p Demuškin group, by local class field theory [21, II-30, Theorem 4]. It is an open problem to characterize the pro-p Demuškin groups of finite rank ≥ 3 which can be realized as $G_K(p)$ for some field K of characteristic $\neq p$ containing μ_p, say (cf. [17, p. 339; 9, Remark 5.5]). The following result may shed some light on this question.

Proposition 5.2. *Let G be a pro-p group of finite rank ≥ 3 such that $H^2(G)\cong\mathbb{Z}/p$. The following conditions are equivalent:*

(a) *$G\cong G_K(p)$ for some p-henselian field (K,v) such that* $\mathrm{char}\, K=0$, $\mathrm{char}\,\bar{K}_v=p$, *and $\mu_p\subseteq K$;*

(b) *$G\cong G_{K^*}(p)$ for some finite extension K^* of $\mathbb{Q}_p(\mu_p)$.*

Proof. (a)$\Rightarrow$(b): We have $\dim_{\mathbb{F}_p} H^1(K)=\mathrm{rank}(G)\geq 3$ [21, I-38, Corollary]. It follows from Proposition 2.3 and Lemma 4.1 that $G_K(p)\cong G_E(p)$ for some field E of characteristic 0 containing μ_p which is p-henselian with respect to a valuation w of rank 1 satisfying $\mathrm{char}\,\bar{E}_w=p$. Now $G\cong G_E(p)$ is not a free pro-p group [21, I-32, Corollary]. Corollary 3.6 therefore shows that $G_E(p)\cong G_{K^*}(p)$ with K^* as in (b).

(b)$\Rightarrow$(a): Immediate. □

Question 5.3. Let K be a field such that $G_K(p)$ is a pro-p Demuškin group of finite rank ≥ 3. Is K necessarily p-henselian with respect to a valuation having residue characteristic p?

Remark 5.4. (a) In light of Proposition 5.2, an affirmative answer to Question 5.3 would imply that the pro-p Demuškin groups of finite rank ≥ 3 which occur as $G_K(p)$

for some field K of characteristic $\neq p$ containing μ_p are precisely the groups $G_{K^*}(p)$, where K^* is a finite extension of $\mathbb{Q}_p(\mu_p)$.

(b) In light of Proposition 4.2, an affirmative answer to Question 5.3 would also imply that pro-p Demuškin groups of finite rank ≥ 3 do not occur as absolute Galois groups of fields. The question whether this is indeed the case was posed to me by Jochen Koenigsmann. Note however that pro-p Demuškin groups of *countable* rank do occur as absolute Galois groups (cf. [13, Theorem 5; 17,16]).

(c) There exist fields K with $G_K(p)$ a pro-p Demuškin group of countable rank which are not p-henselian with respect to any valuation with residue characteristic p. In fact, Mináč and Ware construct in [16, Remark 2.6(i)] a field K of characteristic 0 such that $G_K = G_K(p)$ is a pro-p Demuškin group of countable rank and K does not contain any henselization of $\mathbb{Q}$ with respect to its p-adic valuation. Hence K cannot be (p-)henselian with respect to a valuation as above.

5.3. *Elementary type Witt rings*

We conclude by an application to the theory of quadratic forms. Here we fix $p=2$ and denote the Witt ring of a field K of characteristic $\neq 2$ by $W(K)$. For the basic notions of the category of abstract Witt rings we refer to [15]. An abstract Witt ring is said to have *elementary type* if it can be constructed in finitely many steps from the abstract Witt rings $\mathbb{Z}$, $\mathbb{Z}/2$, $\mathbb{Z}/4$, and the Witt rings of the finite extensions of $\mathbb{Q}_2$ by means of the two standard constructions in that category, namely, direct products and extensions. The long-standing "elementary type conjecture" predicts that if $(K^\times : (K^\times)^2) < \infty$ then $W(K)$ has elementary type. Our final result proves this conjecture in an important test-case:

Theorem 5.5. *Let (K,v) be a 2-henselian field of characteristic 0 such that* $\operatorname{char} \bar{K}_v = 2$ *and $(K^\times : (K^\times)^2) < \infty$. Then $W(K)$ has elementary type.*

Proof. We combine the methods of [9, 10] with the results of Section 3. Proposition 2.3 gives a 2-henselian valuation u on K such that $E = \bar{K}_u$ has characteristic 0 and is 2-henselian with respect to a valuation w of rank 1 with residue characteristic 2. Then $W(K)$ is the extension $W(E)[\Gamma_u/2\Gamma_u]$ of $W(E)$ by the elementary abelian 2-group $\Gamma_u/2\Gamma_u$ [12, Section 12]. Furthermore, by condition (vii) of Proposition 2.3, the latter group is finite and $G_E(2)$ is finitely generated. It thus remains to show that $W(E)$ has elementary type.

By Corollary 3.6 one of the following cases holds:

Case (I): $\Gamma_w \cong \mathbb{Z}$, the completion (E^*, w^*) of (E,w) is a finite extension of $(\mathbb{Q}_2, v_2)$, and $\mathrm{Res}: \mathcal{G}(E^*) \to \mathcal{G}(E)$ is an isomorphism. By [24, Corollary 2.5] this implies that $W(E) \cong W(E^*)$, and we are done.

Case (II): $G_E(2)$ is a finitely generated free pro-2 group. In this case we take subextensions $E_1, \ldots, E_n$ of $E(2)/E$ such that $G_E(2) = G_{E_1}(2) *_2 \cdots *_2 G_{E_n}(2)$ and $G_{E_i}(2) \cong \mathbb{Z}_2$, $i = 1, \ldots, n$. Then $W(E)$ is the direct product of $W(E_1), \ldots, W(E_n)$ in the category of

abstract Witt rings [9, Remark 3.5]. Finally, for each $1 \leq i \leq n$ either $W(E_i) \cong \mathbb{Z}/4$ or $W(E_i) \cong \mathbb{Z}/2[\mathbb{Z}/2]$ [9, Table 5.1], completing the proof. □

Acknowledgements

I would like to thank Antonio José Engler for his valuable remarks on an earlier version of this paper.

References

[1] N. Bourbaki, Commutative Algebra, Addison-Wesley, Reading, MA, 1972.
[2] L. Bröcker, Characterization of fans and hereditarily pythagorean fields, Math. Z. 151 (1976) 149–163.
[3] S.P. Demuškin, The group of a maximal p-extension of a number field, Izv. Akad. Nauk SSSR Ser. Mat. 25 (1961) 329–346 (in Russian).
[4] S.P. Demuškin, On 2-extensions of a local field, Sibirian Math. J. 4 (1963) 951–955 (in Russian).
[5] I. Efrat, Pro-p Galois groups of algebraic extensions of $\mathbb{Q}$, J. Number Th. 64 (1997) 84–99.
[6] I. Efrat, Free pro-p product decompositions of Galois groups, Math. Z. 225 (1997) 245–261.
[7] O. Endler, Valuation Theory, Springer, Berlin, 1972.
[8] B. Jacob, A. Wadsworth, A new construction of noncrossed product algebras, Trans. Amer. Math. Soc. 293 (1986) 693–721.
[9] B. Jacob, R. Ware, A recursive description of the maximal pro-2 Galois group via Witt rings, Math. Z. 200 (1989) 379–396.
[10] B. Jacob, R. Ware, Realizing dyadic factors of elementary type Witt rings and pro-2 Galois groups, Math. Z. 208 (1991) 193–208.
[11] C.U. Jensen, A. Prestel, Finitely generated pro-p-groups as Galois groups of maximal p-extensions of function fields over $\mathbb{Q}_q$, Manuscripta Math. 90 (1996) 225–238.
[12] M. Knebusch, Grothendieck- und Wittringe von nichtausgearteten symmetrichen Bilinearformen, Sitzungsber. Heidelb. Akad. Wiss. Math.-Natur. Kl., 1969/70, 3 Abh. (1970) 93–157.
[13] J.P. Labute, Demuškin groups of rank $\aleph_0$, Bull. Soc. Math. France 94 (1966) 211–244.
[14] J.P. Labute, Classification of Demushkin groups, Canad. J. Math. 19 (1967) 106–132.
[15] M. Marshall, Abstract Witt Rings, Queen's Pap. Pure Appl. Math., vol. 57, Queen's University, Kingston, 1980.
[16] J. Mináč, R. Ware, Demuškin groups of rank $\aleph_0$ as absolute Galois groups, Manuscripta Math. 73 (1991) 411–421.
[17] J. Mináč, R. Ware, Pro-2 Demuškin groups of rank $\aleph_0$ as Galois groups of maximal 2-extensions of fields, Math. Ann. 292 (1992) 337–353.
[18] F. Pop, Galoissche Kennzeichnung p-adisch abgeschlossener Körper, J. Reine Angew. Math. 392 (1988) 145–175.
[19] I.R. Šafarevič, On p-extensions, Math. Sbornik, N.S. 20 (1947) 351–363 (Russian); Amer. Math. Soc. Transl. Ser. 2 4 (1956) 59–72.
[20] J.-P. Serre, Structure de certains pro-p-groupes (d'aprés Demuškin), Sém. Bourbaki 252 (1962/63) 1–11.
[21] J.-P. Serre, Cohomologie Galoisienne, Lecture Notes Math., vol. 5, Springer, Berlin, 1965.
[22] J.-P. Serre, Local Fields, Springer, Berlin, 1979.
[23] A.R. Wadsworth, p-henselian fields: K-theory, Galois cohomology, and graded Witt rings, Pac. J. Math. 105 (1983) 473–496.
[24] R. Ware, Quadratic forms and profinite 2-groups, J. Algebra 58 (1979) 227–237.
[25] R. Ware, Galois groups of maximal p-extensions, Trans. Amer. Math. Soc. 333 (1992) 721–728.