TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 350, Number 6, June 1998, Pages 2473–2485
S 0002-9947(98)02063-7

ABELIAN SUBGROUPS OF PRO-p GALOIS GROUPS

ANTONIO JOSÉ ENGLER AND JOCHEN KOENIGSMANN

Abstract. It is proved that non-trivial normal abelian subgroups of the Galois group of the maximal Galois p-extension of a field F (where p is an odd prime) arise from p-henselian valuations with non-p-divisible value group, provided $\#(\dot{F}/\dot{F}^p) \geq p^2$ and F contains a primitive p-th root of unity. Also, a generalization to arbitrary prime-closed Galois-extensions is given.

Introduction

For a prime number p and a field F, let $G_F(p)$ denote the Galois group of the maximal Galois p-extension $F(p)$ of F, and for a (Krull) valuation v on F we denote its value group and residue field by Γ_v (written additively) and $\kappa(v)$. The valuation v is said to be p**-henselian** if it extends uniquely to $F(p)$.

It is proved in [EN] and [Ef] that (disregarding one exceptional case) a field F with $[\dot{F} : \dot{F}^2] \geq 4$ admits a 2-henselian valuation with $char\,\kappa(v) \neq 2$ and $\Gamma_v \neq 2\Gamma_v$ iff $G_F(2)$ contains a non-trivial normal abelian subgroup. In this note we prove that the same holds (without exception) for any prime $p > 2$:

Main Theorem. *A field F with $[\dot{F} : \dot{F}^p] \geq p^2$ containing a primitive p-th root ζ_p of unity admits a p-henselian valuation with $char\,\kappa(v) \neq p$ and $\Gamma_v \neq p\Gamma_v$ if and only if $G_F(p)$ contains a non-trivial normal abelian subgroup.*

In the next section we recall from well-known facts about the Galois theory of valued fields how normal abelian subgroups arise from p-henselian valuations (the easy direction of the Main Theorem). Moreover, we explicitly describe the structure of $G_F(p)$ when F admits a p-henselian valuation.

In section 2, using the methods developed in [K2] for detecting p-henselianity of a field F (the existence of some non-trivial p-henselian valuation) via 'p-rigid' and 'strongly p-rigid' elements in F (definitions below), we complete Ware's Galois-theoretic characterization of 'hereditarily p-rigid' fields (cf. [W2]), obtaining a very simple description of these fields (Prop. 2.2).

From there the link between p-henselian valuations and normal abelian subgroups of $G_F(p)$ will be established, proving the harder direction of the Main Theorem in section 3. For fields of finite absolute transcendence degree, this link has (under further additional assumptions) already been discovered by Pop in his 'q-Lemma' ([Po], 1.12), using local-global-principles for Brauer groups of number fields and

Received by the editors December 20, 1995 and, in revised form, September 11, 1996.
1991 *Mathematics Subject Classification.* Primary 12F10; Secondary 12J20.
Key words and phrases. p-henselian, p-rigid, strongly p-rigid.
The contents of this paper were developed while the first author enjoyed the hospitality of Konstanz University supported by GMD-CNPq.

function fields in one variable. So our Main Theorem may as well be regarded as a generalization of Pop's result. As a consequence, we deduce that, in general, $G_F(p)$ contains a unique maximal normal abelian subgroup, i.e., one containing all normal abelian subgroups of $G_F(p)$ (Cor. 3.3).

In section 4 we shall generalize the Main Theorem to arbitrary p-closed Galois extensions Ω/F, instead of $F(p)/F$ (Thm. 4.3).

Finally, in an appendix, following a suggestion of Y. Ershov, we give an alternative proof of the Main Theorem under the additional hypothesis that every $a \in \dot{F} \setminus \dot{F}^p$ is rigid. We deduce from this a new proof of the Galois characterization of p-adic fields ([K2], Thm. 4.1) which avoids the model theoretic reasoning used in [K2].

1. A description of $G_F(p)$ for p-henselian fields

Throughout this paper F will be a field containing a primitive p-th root of unity. Therefore, the characteristic of F is $\neq p$ and $F(p)$ contains all p-power roots of unity. For any valuation v of F we denote the valuation ring, the maximal ideal and the value group by $\mathcal{O}_v$, $\mathcal{M}_v$ and Γ_v respectively, writing Γ_v additively. The residue field will be denoted by $\kappa(v)$, or just κ if there is no ambiguity about the valuation v. If v is a valuation with $char\,\kappa(v) \neq p$, then the residue field of an extension w of v to $F(p)$ is the maximal Galois p-extension of κ and the value group Γ_w is the p-divisible hull of Γ_v.

Assume now that v is p-henselian and $char\,\kappa(v) \neq p$. Then F contains all p-power roots of unity which lie in κ. Denoting the inertia and the ramification subgroup of $G_F(p)$ (w.r.t. v) by T_v and V_v respectively, we deduce from [E], 20.11, p. 161 that V_v is trivial: if $char\,\kappa = q$, then either $q = 0$ and V_v is trivial, or $q > 0$ and V_v is the unique Sylow q-subgroup of T_v; but by assumption $q \neq p$ and T_v is a pro-p-group as a subgroup of $G_F(p)$.

In order to study T_v it is convenient to consider the canonical pairing

$$T_v \times \Gamma_w/\Gamma_v \mapsto \kappa(w),$$

$$(\tau, w(x) + \Gamma_v) \longmapsto \overline{\tau(x)/x},$$

where the bar means the image $\underline{\text{in } \kappa(w)}$. We know from valuation theory that Γ_w/Γ_v is a p-torsion group and so $\overline{\tau(x)/x}$ is a p-power root of unity. In our case the ramification group is trivial and so the pairing is non-degenerate. Therefore, there exists a canonical isomorphism $T_v \cong Hom(\Gamma_w/\Gamma_v, \mu_{p^\infty})$, where μ_{p^∞} is the group of *all* p-power roots of unity (see [E], §20, for the details). Consequently, T_v is an abelian group. On the other side, the canonical projection $\mathcal{O}_v \longrightarrow \kappa$ gives rise to a canonical split short exact sequence

$$(\dagger) \qquad 1 \longrightarrow T_v \longrightarrow G_F(p) \longrightarrow G_\kappa(p) \longrightarrow 1.$$

We may conclude from the above discussion that, for fields admitting a p-henselian valuation as in the Main Theorem, the existence of a non-trivial normal abelian subgroup of $G_F(p)$ follows from general valuation theory. Our result provides the converse.

Furthermore, going back to the pairing above, we know that it is compatible with the action of $G_\kappa(p)$ on T_v. Hence, for every $\tau \in T_v$, $\sigma \in G_\kappa(p)$ and $x \in \dot{F}(p)$,

$$(\tau^\sigma, w(x) + \Gamma_v) = \bar{\sigma}(\tau, w(x) + \Gamma_v),$$

where $\bar{\sigma}$ is the image of σ in $G_\kappa(p)$. Consequently, the determination of τ^σ follows from the action of $\bar{\sigma}$ on the group μ_{p^∞}. We claim that (topological) generators $\bar{\sigma}$ for the Galois group $Gal(\kappa(\mu_{p^\infty})/\kappa)$ may be chosen such that $\bar{\sigma}(\zeta) = \zeta^r$ for some number r and every $\zeta \in \mu_{p^\infty}$. Hence

$$(\tau^\sigma, w(x) + \Gamma_v) = (\tau, w(x) + \Gamma_v)^r = (\tau^r, w(x) + \Gamma_v),$$

for every $\tau \in T_v$ and $x \in \dot{F}(p)$. From the non-degeneracy of the pairing it follows that $\tau^\sigma = \tau^r$, for every $\tau \in T_v$. Finally, let us observe that the p-henselianity of v implies that F (and the extensions of F inside $F(p)$) contains all the p-power roots of unity which lie in the residue field. Therefore, we may find out the action of σ on μ_{p^∞} without going down to $G_\kappa(p)$. To this end, let us fix inside $F(p)$ a system of primitive p^n-th roots of unity ζ_{p^n}, $n \geq 1$, such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$ for every $n \geq 1$.

We shall now present generators for $G_\kappa(p)$ with a suitable action on μ_{p^∞}, and describe $G_F(p)$.

We first consider the case where F contains μ_{p^∞}. Then the action is trivial and so $G_F(p) \cong T_v \times G_\kappa(p)$.

If $\zeta_{p^m} \in F$ and $\zeta_{p^{m+1}} \notin F$, where $m \geq 1$ for $p \neq 2$ and $m \geq 2$ for $p = 2$, then $Gal(F(\mu_{p^\infty})/F) \cong \mathbb{Z}_p$, and this group has a generator σ such that $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{p^m+1}$ for every $n \geq m$. Therefore, σ acts on T_v by $\tau^\sigma = \tau^{p^m+1}$ for each $\tau \in T_v$.

As *char* $\kappa \neq p$, $F(\mu_{p^\infty})/F$ is purely inert, i.e. unramified and defectless. Thus, by ([E], Thm. 22.7, p. 182), $T_v \subset G_{F(\mu_{p^\infty})}(p)$, and by the first case above $G_{F(\mu_{p^\infty})}(p) \cong T_v \times G_{\kappa(\mu_{p^\infty})}(p)$ (T_v is also the inertia group corresponding to the unique extension of v to $F(\mu_{p^\infty})$) and $G_F(p) \cong G_{F(\mu_{p^\infty})}(p) \rtimes \mathbb{Z}_p$.

If $p = 2$ and $i := \sqrt{-1} \notin F$, the above arguments apply to $F(i)$, but not to F. We shall use the exact sequence

$$1 \longrightarrow G_{F(i)}(2) \longrightarrow G_F(2) \longrightarrow Gal(F(i)/F) \longrightarrow 1$$

which splits iff F is formally real ([Be], Thm. 3, p. 76). The description of $G_F(2)$ now depends on whether or not $F(i)$ contains all 2^n-th roots of unity.

Let us first discuss the case $\mu_{2^\infty} \subseteq F(i)$. In this case $G_{F(i)}(2) \cong T_v \times G_{\kappa(i)}(2)$ and $\tau^\phi = \tau^{-1}$ for each $\tau \in T_v$ and $\phi \in G_F(2) \setminus G_{F(i)}(2)$: note that such a ϕ induces on μ_{2^∞} the automorphism $\zeta_{p^m} \mapsto \zeta_{p^m}^{-1}$ for every $m \geq 1$. In particular, if F is formally real, we have

$$G_F(2) \cong G_{F(i)}(2) \rtimes \langle \rho \rangle \cong (T_v \times G_{\kappa(i)}(2)) \rtimes \langle \rho \rangle,$$

where ρ is an involution with $\tau^\rho = \tau^{-1}$ for each $\tau \in T_v$.

Now consider the case $\mu_{2^\infty} \not\subseteq F(i)$, i.e. for some $m \geq 2$, $\zeta_{2^m} \in F(i)$ and $\zeta_{2^{m+1}} \notin F(i)$, so $Gal(F(\mu_{2^\infty})/F(i)) \cong \mathbb{Z}_2$. In this case $Gal(F(\mu_{2^\infty})/F) \cong \mathbb{Z}_2$ or $\cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$ (cyclotomic extensions are abelian).

If $Gal(F(\mu_{2^\infty})/F) \cong \mathbb{Z}_2$, F cannot be formally real: $\mathbb{Z}_2$ does not contain involutions, but if F is real, the subextension $F(\{\zeta_{2^n} + \zeta_{2^n}^{-1} \mid n \in \mathbb{N}\})$ of $F(\mu_{2^\infty})/F$ which has index ≤ 2 in $F(\mu_{2^\infty})$ is also real, hence of index $= 2$. Also, $m \geq 3$, because $\zeta_{2^3} = (1+i)/\sqrt{2} \in F(i)$: note that $\sqrt{2} \in F(\mu_{2^\infty})$ and thus $\sqrt{2} \in F(i)$. Furthermore, if $\mathcal{N}$ denotes the norm function for the extension $F(i)/F$, one has $\mathcal{N}(\zeta_{2^m}) = -1$: otherwise $\mathcal{N}(\zeta_{2^m}) = 1$ and thus, by Hilbert's Theorem 90, $\zeta_{2^m} = z/\bar{z} = z^2/\bar{z}z$ for some $z \in F(i)$, where the bar generates $Gal(F(i)/F)$, but $\bar{z}z \in F \cap F(\mu_{2^\infty})^2 \subseteq F(i)^2$, so $\zeta_{2^m} \in F(i)^2$, contradicting the assumption $\zeta_{2^{m+1}} \notin F(i)$. So for $\sigma \in Gal(F(\mu_{2^\infty})/F) \setminus Gal(F(\mu_{2^\infty})/F(i))$, $\sigma(\zeta_{2^m}) = -\zeta_{2^m}^{-1} = \zeta_{2^m}^{2^{m-1}-1}$. In this case we can find a generator σ for $Gal(F(\mu_{2^\infty})/F)$ such that $\sigma(\zeta_{2^n}) = \zeta_{2^n}^{2^{m-1}-1}$ for every $n \geq m$. Arguing as above, we then get $G_{F(\mu_{2^\infty})}(2) \cong T_v \times G_{\kappa(\mu_{2^\infty})}(2)$ and $G_F(2) \cong G_{F(\mu_{2^\infty})}(2) \rtimes \langle\sigma\rangle$, where $\langle\sigma\rangle$ acts on T_v by $\tau^\sigma = \tau^{2^{m-1}-1}$ for each $\tau \in T_v$.

If $Gal(F(\mu_{2^\infty})/F) \cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$, the fixed field F' of the $\mathbb{Z}/2\mathbb{Z}$ factor comes under the first $p = 2$-case of our discussion, i.e. $\mu_{2^\infty} \subseteq F'(i) = F(\mu_{2^\infty})$. So each $\phi \in G_{F'}(2) \setminus G_{F'(i)}(2)$, that is each $\phi \in G_F(2) \setminus G_{F(i)}(2)$ with $\phi^2 \in G_{F(\mu_{2^\infty})}(2)$, satisfies $\tau^\phi = \tau^{-1}$ for any $\tau \in T_v$.

Putting things together, we have thus proved:

Proposition 1.1. *Let p be any prime and let (F, v) be a p-henselian valued field with char $\kappa \neq p$. Then:*

(a) *If $\mu_{p^\infty} \subseteq F$, then $G_F(p) \cong T_v \times G_\kappa(p)$.*

(b) *If $\zeta_{p^m} \in F$ and $\zeta_{p^{m+1}} \notin F$, where $m \geq 1$ for $p \neq 2$ and $m \geq 2$ for $p = 2$, then*

$$G_F(p) \cong G_{F(\mu_{p^\infty})}(p) \rtimes Gal(F(\mu_{p^\infty})/F) \cong (T_v \times G_{\kappa(\mu_{p^\infty})}(p)) \rtimes \mathbb{Z}_p,$$

where $\mathbb{Z}_p$ has a generator σ such that $\tau^\sigma = \tau^{p^m+1}$ for every $\tau \in T_v$.

(c) *If $p = 2$, $i \notin F$ and $\mu_{2^\infty} \subseteq F(i)$, then $G_{F(i)}(2) \cong T_v \times G_{\kappa(i)}(2)$ and $\tau^\phi = \tau^{-1}$ for each $\tau \in T_v$ and $\phi \in G_F(2) \setminus G_{F(i)}(2)$.*

If, in addition, F is formally real, then

$$G_F(2) \cong (T_v \times G_{\kappa(i)}(2)) \rtimes \langle\rho\rangle,$$

where ρ is an involution with $\tau^\rho = \tau^{-1}$ for each $\tau \in T_v$.

(d) *If $p = 2$, $i \notin F$, and for some $m \geq 2$, $\zeta_{2^m} \in F(i)$ and $\zeta_{2^{m+1}} \notin F(i)$, then $G_{F(i)}(2)$ can be described as in (b) and either*

(d$_1$) *$Gal(F(\mu_{2^\infty})/F) \cong \mathbb{Z}_2$, $m \geq 3$, F is not formally real and*

$$G_F(2) \cong G_{F(\mu_{2^\infty})}(2) \rtimes Gal(F(\mu_{2^\infty})/F) \cong (T_v \times G_{\kappa(\mu_{2^\infty})}(2)) \rtimes \mathbb{Z}_2,$$

where $\mathbb{Z}_2$ has a generator σ such that $\tau^\sigma = \tau^{2^{m-1}-1}$ for every $\tau \in T_v$, or

(d$_2$) *$Gal(F(\mu_{2^\infty})/F) \cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$, and for each $\phi \in G_F(2) \setminus G_{F(i)}(2)$ with $\phi^2 \in G_{F(\mu_{2^\infty})}(2)$ one has $\tau^\phi = \tau^{-1}$ for any $\tau \in T_v$. In particular, if F is formally real,*

$$G_F(2) \cong ((T_v \times G_{\kappa(\mu_{2^\infty})}(2)) \rtimes \mathbb{Z}_2) \rtimes \langle\rho\rangle,$$

where ρ is an involution with $\tau^\rho = \tau^{-1}$ for each $\tau \in T_v$ and $\mathbb{Z}_2$ has a generator σ such that $\tau^\sigma = \tau^{2^m+1}$ for each $\tau \in T_v$.

Observation 1.2. (a) If F is a field with $Gal(F(\mu_{2^\infty})/F) \cong \mathbb{Z}/2\mathbb{Z}$ or $\cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$, then char $F = 0$.

This is because the restriction map

$$Res : Gal(F(\mu_{2^\infty})/F) \longrightarrow Gal(F_{alg}(\mu_{2^\infty})/F_{alg}),$$

where $F_{alg} := F \cap \tilde{\mathbb{Q}}$ or $F \cap \tilde{\mathbb{F}}_p$ is the algebraic part of F, is an isomorphism. But an algebraic extension of $\mathbb{F}_p$ containing μ_{2^∞} is quadratically closed, so it has no subfields of index 2, as its Sylow-2-subgroup is the pro-2 cyclic group, which itself has no subgroups of finite order.

(b) Nevertheless, there are non-formally real fields with $Gal(F(\mu_{2^\infty})/F) \cong \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.

Clearly, there are real fields with that property, e.g. $K = \mathbb{R}$ or $K = \mathbb{Q}$. Now take $F = K(T)(\sqrt{-1 - T^2})$, and use the fact that Res is an isomorphism, as above.

For fields F with $Gal(F(\mu_{2^\infty})/F) \cong \mathbb{Z}/2\mathbb{Z}$, there are examples which are even 'less formally real', i.e. not showing any 'real heritage': for each $n \geq 4$, we find, by Dirichlet, a prime $p_n \equiv -1(mod\, 2^n)$; hence $4 \nmid p_n - 1$, but $2^n \mid p_n^2 - 1 = (p_n - 1)(p_n + 1)$, so $i \notin \mathbb{F}_{p_n}$, but $\zeta_{2^n} \in \mathbb{F}_{p_n}(i)$. Taking F to be a non-trivial ultraproduct of the $\mathbb{F}_{p_n}$ implies $i \notin F$, but $\mu_{2^\infty} \subseteq F(i)$, i.e. $Gal(F(\mu_{2^\infty})/F) \cong \mathbb{Z}/2\mathbb{Z}$. F is non-real, not because each of the $\mathbb{F}_{p_n}$ was (the ultra-product of a sequence of non-real fields of increasing level, e.g., is real!), but because the level of each $\mathbb{F}_{p_n}$ is 2, i.e. $-1 \in \mathbb{F}_{p_n}^2 + \mathbb{F}_{p_n}^2$ for each n. This, by the way, also shows that

(c) the property $Gal(F(\mu_{2^\infty})/F) \cong \mathbb{Z}_2$ is — unlike the property $G_F(2) \cong \mathbb{Z}_2$ — not elementary (in the language of fields).

2. p-RIGIDITY REVISITED

Throughout this section we shall fix a prime $p > 2$.

Let us recall from [W2] and [K2] that an element $a \in F \setminus F^p$ is called **p-rigid** if the image of the norm $F(\sqrt[p]{a}) \to F$ is $\bigcup_{i=0}^{p-1} a^i F^p$, and **strongly p-rigid** if $F^p + a^i F^p \subseteq F^p \cup a^i F^p$ for all $i \in \{1, 2, \dots, p-1\}$.

It was proved in [K2] that strongly p-rigid elements in a field F containing a primitive pth root ζ_p of unity give rise to a p-henselian valuation v with $char\,\kappa(v) \neq p$ and $\Gamma_v \neq p\Gamma_v$. We still do not know whether on a field F with $\zeta_p \in F$ and $[\dot{F} : \dot{F}^p] \geq p^2$, p-rigid elements already lead to p-henselian valuations.

However, if F has enough p-rigid elements, the existence of some strongly p-rigid element (and thus of a non-trivial p-henselian valuation) can be deduced. This was proved in [K2], Prop. 3.1, under the additional hypotheses that $\zeta_p \in F$ and that $[\dot{F} : \dot{F}^p] < \infty$. But both hypotheses are unnecessary. The first one is not used at all in the course of the proof, and the second one can be avoided by omitting the 'subclaim' entirely, but otherwise carrying out the same 'p-rigid calculus' only under the assumption that for some $u, v \in \dot{F}$ one has $u^p + av^p \in a^k \dot{F}^p$. With these changes in the proof of [K2], 3.1, together with the remark following it which points out that only a consequence of p-rigidity is actually used, namely that for p-rigid elements $c \in F$ in particular $F^p + cF^p \subseteq \bigcup_{i=0}^{p-1} c^i F^p$, we obtain the following stronger result:

Proposition 2.1. *Let F be a field with $char\,F \neq p$. If $\dot{F}$ contains elements a, b which are p-independent (i.e. $\mathbb{F}_p$-linearly independent modulo $\dot{F}^p$) such that $c \in \langle a, b\rangle \setminus \dot{F}^p \Rightarrow 1 - c \in \bigcup_{i=0}^{p-1} c^i \dot{F}^p$, then a or b is strongly p-rigid.*

In [W2], Ware calls a field F **p-rigid** if every $a \in F \setminus F^p$ is p-rigid, and **hereditarily p-rigid** if every subextension of $F(p)/F$ is p-rigid. He gives a Galois-theoretic description of hereditarily p-rigid fields. Using the above proposition and the main theorem of [K2], it follows even that p-rigidity and hereditary p-rigidity are the same and that p-rigid fields have a very simple structure:

Proposition 2.2. *Let F be a field such that $\zeta_p \in F$ and $F \neq F(p)$. Then the following conditions are equivalent:*

(i) *F is hereditarily p-rigid.*
(ii) *F is p-rigid.*
(iii) *$a \notin F^p \Rightarrow 1 - a \in \bigcup_{i=0}^{p-1} a^i \dot{F}^p$ for all $a \in F$.*
(iv) *F has a p-henselian valuation v with $char\,\kappa(v) \neq p$ and $G_{\kappa(v)}(p) \cong 1$ or $\cong \mathbb{Z}_p$.*
(v) *There is an exact sequence $1 \to \mathbb{Z}_p^I \to G_F(p) \to \mathbb{Z}_p \to 1$ for some index set I.*

(vi) *$G_F(p)$ is solvable.* Recall that a profinite group is called 'solvable' if it has a **finite** normal series with abelian factors ($\neq$ 'pro-solvable').

Proof. [W2], Theorems 1 and 3 give the equivalences (i) $\Leftrightarrow$ (v) $\Leftrightarrow$ (vi). With the trivial implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) and (iv) $\Rightarrow$ (v), we only have to prove (iii) $\Rightarrow$ (iv).

If $[\dot{F} : \dot{F}^p] = p$ then $G_F(p) \cong \mathbb{Z}_p$, and the trivial valuation on F satisfies (iv). So we may assume that $[\dot{F} : \dot{F}^p] \geq p^2$. Then there are two p-independent elements in F satisfying, by (iii), the hypothesis of Prop. 2.1. Hence we find strongly p-rigid elements in F, and thus, by [K2], a p-henselian valuation w with $char\,\kappa(w) \neq p$ and $\Gamma_w \neq p\Gamma_w$.

We recall, from [K1], that among the p-henselian valuations of a field there is a **canonical** valuation v_p. If F has p-henselian valuations where the residue field is **p-closed**, i.e. it admits no Galois-p-extensions, then v_p is the coarsest among those. Otherwise all p-henselian valuations are comparable and v_p is the finest such. (A valuation v is **finer** than w — or w is **coarser** than v — iff $\mathcal{O}_v \subseteq \mathcal{O}_w$.)

In case $char\,\kappa(v_p) \neq p$, we let $v = v_p$. If $char\,\kappa(v_p) = p$, we must have $char\,F = 0$ and v_p is finer than w. Then we choose v such that $\mathcal{O}_v = \mathcal{O}_{v_p}[p^{-1}]$. This choice of v makes sure that v is the finest p-henselian valuation on F with $char\,\kappa(v) \neq p$. As v is finer than w, $\Gamma_v \neq p\Gamma_v$. But this also ensures that $[\dot{\kappa}(v) : \dot{\kappa}(v)^p] \leq p$, because otherwise, as condition (iii) passes down to $\kappa(v)$, by the same reasoning as above, a p-henselian valuation v' on $\kappa(v)$ could be found with $\Gamma_{v'} \neq p\Gamma_{v'}$ and residue characteristic not p, inducing, by ([Br], Lemma 1.3), a proper p-henselian refinement of v, which would not be in accord with the choice of v. So v, indeed, satisfies condition (iv). □

Corollary 2.3. *Let F be a field with $\zeta_p \in F$. Then $G_F(p)$ is abelian iff either $G_F(p)$ is cyclic or F is p-rigid and $\mu_{p^\infty} \subseteq F$.*

Proof. For $p = 2$, this is [W1], Thm. 3.6; for $p > 2$, it follows from Prop. 2.2 and Prop. 1.1. □

Remark 2.4. For further reference we shall give a name to the valuation v constructed in the proof above: we call it the **special** p-henselian valuation on F and denote it by v^p. So v^p is the finest p-henselian valuation on F with residue characteristic $\neq p$ which is coarser than any p-henselian valuation with p-closed residue field. If some p-henselian valuation of residue characteristic $\neq p$ has a p-closed residue field, then so does v^p.

It is convenient to point out that v^p may be trivial, even if v_p is not (e.g. on $\mathbb{Q}_p$).

3. Proof of the main theorem

We prove a refined version of our main theorem giving a valuation-theoretic, a Galois-theoretic and an 'arithmetic' characterization of p-henselianity:

Theorem 3.1. *For any prime $p > 2$ and any field F containing ζ_p with $[\dot{F} : \dot{F}^p] \geq p^2$ the following conditions are equivalent:*

(i) *F admits a p-henselian valuation v with $char\,\kappa(v) \neq p$ and $\Gamma_v \neq p\Gamma_v$.*

(ii) *F contains a strongly p-rigid element.*

(iii) *$G_F(p)$ contains a non-trivial normal abelian subgroup.*

Proof. The equivalence (i) $\Leftrightarrow$ (ii) follows immediately from the main theorem of [K2], and (i) $\Rightarrow$ (iii) is obvious after the comments preceding Proposition 1.1.

So we assume (iii) and find a non-trivial normal abelian subgroup N of $G_F(p)$. As $p > 2$, by Kummer Theory $G_F(p)$ contains no torsion. Therefore we may write $N \cong \mathbb{Z}_p^I$ for some index set I. Set $L := Fix\, N$. If $\#I \geq 2$ (**case 1**), Proposition 2.2 guarantees the existence of some p-henselian valuation w on L with $char\, \kappa(w) \neq p$ and $\Gamma_w \neq p\Gamma_w$. If $\#I = 1$ (**case 2**), we claim that there exists $\sigma \in G_F(p) \setminus N$ such that the subgroup H_σ of $G_F(p)$ generated by σ and N is non-cyclic. Since the closed subgroups of a cyclic group are comparable and $\sigma \notin N$, H_σ is a cyclic group if and only if $N \subset \langle\sigma\rangle$. Therefore we have to show that $N \not\subset \langle\sigma\rangle$ for some $\sigma \in G_F(p) \setminus N$. To this end let K be a normal extension of F such that $Gal(K/F) \cong \mathbb{Z}_p$. Observe that if $\zeta_{p^n} \notin F$ for some $n > 1$, then $K = F(\mu_{p^\infty})$ has this property. Otherwise, take $K = \bigcup K_n$, $n \geq 1$, where K_n is the splitting field of the polynomial $X^{p^n} - a$, for a fixed $a \in \dot{F} \setminus \dot{F}^p$. For such an extension K it follows that $G_F(p) \cong G_K(p) \rtimes U$, where $U \cong \mathbb{Z}_p$, since the exact sequence $1 \longrightarrow G_K(p) \longrightarrow G_F(p) \longrightarrow \mathbb{Z}_p \longrightarrow 1$ splits. Now, to finish the proof of the claim observe that if $N \subset U$ or $U \subset N$, for $\sigma \in G_K(p) \setminus N$, $N \not\subset \langle\sigma\rangle$. If N and U are not comparable and σ is a generator of U, then $N \not\subset \langle\sigma\rangle$. Consequently in both cases we can find $\sigma \notin N$ for which H_σ is non-cyclic, and the claim is proved.

Let us now pick σ with H_σ non-cyclic. As $N \cong \mathbb{Z}_p$ and H_σ/N is generated by the image of σ in the quotient, we conclude that H_σ is solvable. Therefore, for the corresponding fixed field E we have that $[\dot{E} : \dot{E}^p] \geq p^2$, and so Proposition 2.2 implies that E has a *non-trivial* p-henselian valuation w with $char\, \kappa(w) \neq p$ and $\Gamma_w \neq p\Gamma_w$. But p-henselianity extends to algebraic extensions within $F(p)$, so the unique prolongation of w to L is again p-henselian.

We have then proved in both cases, 1 and 2, that L admits a non-trivial p-henselian valuation.

We now have to observe that, like henselianity (cf. [En]), p-henselianity goes down to normal subfields:

Lemma 3.2. *If L/F is a normal field extension with $L \subsetneqq F(p)$ and if L admits a non-trivial p-henselian valuation, then so does F. In fact, any p-henselian valuation on L which is coarser than the canonical p-henselian valuation v_p on L restricts to a p-henselian valuation on F.*

Proof. By ([K1], Prop. 3.1), any coarsening v of the canonical p-henselian valuation v_p on L is comparable to any p-henselian valuation on L. If $v \mid F$ would allow an extension $v' \neq v$ to L, v and v' would have to be conjugate, since L/F is normal. Thus v' is also p-henselian, and so v and v' are comparable. On the other side, as different extensions of $v \mid F$ they are not comparable, a contradiction. □

Therefore, back in the proof of the theorem, F admits a non-trivial p-henselian valuation. Let v be the restriction of the special p-henselian valuation v^p of L to F (see Remark 2.4). Then, by the lemma, v is p-henselian, as the special p-henselian valuation is coarser than the canonical. Also, $char\, \kappa(v) \neq p$. So we only have to show that $\Gamma_v \neq p\Gamma_v$.

If $\Gamma_{v^p} \neq p\Gamma_{v^p}$, this follows since L/F is an *algebraic* extension. So assume that $\Gamma_{v^p} = p\Gamma_{v^p}$. Then the inertia group T_{v^p} is trivial, and so Proposition 1.1 implies that $\kappa(v^p)$ is not p-closed. By the choice of v^p, no other p-henselian valuation of residual characteristic $\neq p$ can have a p-closed residue field (Remark 2.4). Hence all such valuations are coarsenings of v^p and have p-divisible value group. As this cannot happen in case 1, we are in case 2. The unique prolongation to L of the p-henselian valuation w on E with $char\,\kappa(w) \neq p$ and $\Gamma_w \neq p\Gamma_w$ is then a coarsening of v^p. Hence $v^p \mid E$ is finer than w. In particular, the value group of $v^p \mid E$ is not p-divisible. So the same holds for Γ_v, since $v^p \mid E$ restricts to v and E/F is an algebraic extension. □

Corollary 3.3. *For any prime p and any field F with $\zeta_p \in F$, $G_F(p)$ has a unique maximal normal abelian subgroup (i.e., one containing all normal abelian subgroups of $G_F(p)$).*

Proof. The case $p = 2$ has been dealt with in [EN]. Also, if $G_F(p)$ is abelian, or if $G_F(p)$ has no non-trivial normal abelian subgroup, there is nothing to show.

So we may assume that $p > 2$, that $G_F(p)$ is non-abelian and that $G_F(p)$ has a non-trivial normal abelian subgroup. We claim that then the inertia subgroup T_{v^p} of the special p-henselian valuation v^p on F contains all normal abelian subgroups of $G_F(p)$.

As $G_F(p)$ is non-abelian, $\kappa(v^p)$ is not p-closed (Prop. 1.1). If $G_{\kappa(v^p)}(p) \cong \mathbb{Z}_p$, then the split exact sequence (†) and Prop. 2.2 imply that F is p-rigid. Thus, by Corollary 2.3, $\mu_{p^\infty} \not\subseteq F$ and consequently $T_{v^p} = G_{F(\mu_{p^\infty})}(p)$. By Prop. 1.1 (b), $G_F(p) \cong T_{v^p} \rtimes \mathbb{Z}_p$. We now prove that any normal abelian subgroup N of $G_F(p)$ satisfies $N \leq T_{v^p}$. If N is non-cyclic, this is again Corollary 2.3. If N is cyclic, it has a generator $\rho = \tau\sigma^\alpha$, for some $\tau \in T_{v^p},\ \alpha \in \mathbb{Z}_p$, and σ the automorphism described in Prop. 1.1 (b). We have then to show that $\alpha = 0$. The action of σ on T_{v^p} implies that $\rho^\sigma = \tau^{p^m+1}\sigma^\alpha$. Thus $\tau^{p^m} = \rho(\rho^\sigma)^{-1} \in N$. Hence there exists $\lambda \in \mathbb{Z}_p$ such that $\tau^{p^m} = (\tau\sigma^\alpha)^\lambda$. Observe now that N is a normal subgroup of $\langle\tau\rangle \rtimes \langle\sigma\rangle$. Hence there exists $\tau_1 \in \langle\tau\rangle$ for which $(\tau\sigma^\alpha)^\lambda = \tau_1\sigma^{\lambda\alpha}$. So $\tau^{p^m}\tau_1^{-1} = \sigma^{\lambda\alpha} \in \langle\tau\rangle \cap \langle\sigma\rangle = \{1\}$, which implies $\alpha = 0$, as desired.

If F is not p-rigid, then $G_{\kappa(v^p)}(p)$ contains no non-trivial normal abelian subgroup: any such subgroup would, by our Main Theorem, imply the existence of a p-henselian valuation on $\kappa(v^p)$ with residue characteristic $\neq p$ and non-p-divisible value group, thus inducing a proper refinement of v^p with these properties, but v^p was already as fine as possible. Therefore, any abelian normal subgroup of $G_F(p)$ projects to the trivial group on $G_{\kappa(v^p)}(p)$, so from the exactness of the sequence (†) (with $v = v^p$) it must be contained in T_{v^p}. □

4 A Galois-theoretic criterion for Ω-henselianity

In [Br], Bröcker introduces the notion of Ω-henselianity (cf. also [Be]): Given a normal algebraic field extension Ω/F, a valuation v on F is called **Ω-henselian** if v has a unique prolongation to Ω. Hensel's Lemma, Newton's Lemma and Krasner's Lemma, applied to polynomials splitting over Ω, generalize to Ω-henselian valuations ([Br], 1.2 and [K1], 1.2). Also, the collection of all Ω-henselian valuations presents the same picture w.r.t. dependence and comparability as in the henselian setting, if only Ω is p-closed for some prime $p \mid \#Gal(\Omega/F)$.

Lemma 4.1. *Let Ω/F be a normal field extension and assume that Ω is p-closed for some prime $p \mid \#Gal(\Omega/F)$. Then:*

(a) *Any two Ω-henselian valuations are dependent.*

(b) *Ω-henselian valuations for which the residue field is not separably closed in the residue field of the unique prolongation to Ω are comparable; all other*

Ω-henselian valuations (if there are any) are finer than those and there is a coarsest valuation among them.

Proof. (b) follows from (a) as in the henselian case (cf. [EE]). And (a) follows from the corresponding statement for p-henselian valuations ([K1], Prop. 3.1): two independent valuations on F extend to independent valuations on the fixed field of some Sylow p-subgroup of $Gal(\Omega/F)$. □

Note that (a) generalizes [Br], 1.4, by assuming only p-closedness of Ω, and this only for one prime p. Some such assumption, however, must be made: one easily constructs finite Galois extensions Ω/F with independent Ω-henselian valuations on F: e.g. if $\Omega/F = \mathbb{Q}(i)/\mathbb{Q}$, all p-valuations with $p \equiv 3 \ mod\ 4$ are Ω-henselian.

With an identical proof, Lemma 3.2 has now its Ω-henselian pendant:

Corollary 4.2. *Let Ω/F be a Galois extension with normal subextension L/F. Assume that Ω is p-closed for some prime $p \mid \#Gal(\Omega/L)$. Then L admits a non-trivial Ω-henselian valuation if and only if F does.*

Before we state a result concerning abelian normal subgroups of an arbitrary Galois extension of fields, let us review the case $p = 2$, which was studied in [EN]. For a field F such that $Gal(F(2)/F) \not\cong \mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$, if there exists a non-trivial normal abelian subgroup N of $Gal(F(2)/F)$, then F admits a 2-henselian valuation v satisfying $char\, \kappa(v) \neq 2$ and $\Gamma_v \neq 2\Gamma_v$. If $rank\, N \geq 2$, the statement follows from Cor. 4.2 and Cor. 2.16 of [EN]. For $rank\, N = 1$ there are two cases to be considered. If $N = C(N)$ (= the centralizer of N), the assertion follows from Thm. 3.4 and Cor. 3.5 of [EN]. In the case $N \neq C(N)$, Prop. 3.1, Cor. 4.2 and Cor. 2.16 imply the statement.

The excluded case corresponds to fields which may or may not have a 2-henselian valuation. This case will be treated separately by subsequent propositions.

Let us also denote by $rank_p G$ the rank of a Sylow p-group of G.

Theorem 4.3. *Let Ω/F be a Galois extension of fields for which $G := Gal(\Omega/F)$ contains an abelian normal subgroup N.*

(a) *If for some prime p the condition*

$$(\star)_p \quad \begin{array}{l} \zeta_p \in \Omega,\ \Omega = \Omega(p),\ rank_p G \geq 2,\ p \mid \#N \\ \text{and if } p = 2,\ G \text{ has no Sylow 2-subgroup } \cong \mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z} \end{array}$$

is satisfied, then F admits an Ω-henselian valuation v with $\Gamma_v \neq p\Gamma_v$ and $char\, \kappa(v) \neq p$.

(b) *If $\mathbb{P} := \{p \text{ prime } \mid p \text{ satisfies } (\star)_p\} \neq \emptyset$, then F admits an Ω-henselian valuation v such that $\Gamma_v \neq p\Gamma_v$ for each $p \in \mathbb{P}$.*

Proof. (a) The Sylow-p-subgroup N_p of N is a non-trivial normal abelian subgroup of some Sylow-p-subgroup G_p of G.

For $p = 2$, $Fix\, G_2$ admits some 2-henselian valuation w with residue characteristic $\neq 2$, and $\Gamma_w \neq 2\Gamma_w$ by the above discussion.

For $p \neq 2$, our main theorem yields a valuation w on $Fix\, G_p$ with the required properties (note that $\zeta_p \in \Omega$ implies $\zeta_p \in Fix\, G_p$).

In any case $Fix\, G_p$ admits some p-henselian (= Ω-henselian) valuation w with the desired properties. The unique prolongation of w to $Fix\, N_p$ is then again Ω-henselian.

But as a Sylow-p-subgroup of a normal abelian subgroup of G, N_p is normal in G, so, by the above corollary, F admits an Ω-henselian valuation v. Choosing v as the restriction of the special p-henselian valuation of $Fix\, N_p$ to F, we can, as in the proof of the main theorem, deduce that $char\, \kappa(v) \neq p$ and $\Gamma_v \neq p\Gamma_v$.

(b) By the hypothesis of (b), the assumption of Lemma 4.1 is satisfied for Ω/F. On the other hand, if we choose for each $p \in \mathbb{P}$ an Ω-henselian valuation $v(p)$ as in the proof of (a), i.e. $v(p)$ is the restriction of the special p-henselian valuation of $Fix\, N_p$ to F, then either $\kappa(v(p))$ is not p-closed, or if it is, no proper coarsening has p-closed residue field. Thus, by 4.1, $v(p)$ is comparable to any other Ω-henselian valuation on F. But now the intersection of all $\mathcal{O}_{v(p)}$ $(p \in \mathbb{P})$ corresponds to an Ω-henselian valuation v of F with $\Gamma_v \neq p\Gamma_v$ for each $p \in \mathbb{P}$: note that $\Gamma_{v(p)} \neq p\Gamma_{v(p)}$. □

Remark 4.4. It may be worth mentioning that there are fields admitting for each prime p a henselian valuation v with $\Gamma_v \neq p\Gamma_v$ and $char\, \kappa(v) \neq p$, but no henselian valuation satisfying these conditions for all primes simultaneously: e.g. the generalized power series field $F = \mathbb{Q}_p((\mathbb{Z}_{(p)}))$.

Corollary 4.5. *Let Ω/F be a Galois extension which is p-closed and contains ζ_p for each prime p dividing the order of $G := Gal(\Omega/F)$. Assume that F does not admit non-trivial Ω-henselian valuations. Then every normal abelian subgroup of G is cyclic.*

Proof. The assumption on F and Thm. 4.3 imply that $rank_p G = 1$ for any odd prime p dividing the order of some normal abelian subgroup N of G. If $2 \mid \#N$, G has a Sylow-2-subgroup $\cong \mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$. Since N is abelian, the corresponding fixed field could not be formally real, and so N does not contain involutions. Therefore $rank_p N \leq 1$ for all primes p, as desired. □

Remark 4.6. There exist formally real fields whose order structure does not allow non-trivial 2-henselian valuations, as in the case of fields with an archimedean ordering or fields admitting two independent orderings ([E], Prop. 6 or [Pr], Thm. 8.3: note that the proofs only depend on 2-henselianity). Recall that two orderings of a field F are called *independent* if the corresponding topologies defined on F are different.

For a field F as above we can conclude that if Ω/F is a Galois extension which is 2-closed and 2 divides the order of $Gal(\Omega/F)$, then there do not exist non-trivial Ω-henselian valuations on F.

Let us finally describe those prime-closed Galois extensions which are excluded from Theorem 4.3 by the assumptions about $p = 2$. We recall that a 2-closed Galois extension Ω over a real field F is called hereditarily pythagorean w.r.t. Ω if every real extension of F in Ω is pythagorean (i.e. sums of squares are squares). The class of hereditarily pythagorean fields is of particular interest for us because Theorem 1 of Becker ([Be], p. 86) states that F is hereditarily pythagorean w.r.t. Ω if and only if $Gal(\Omega/F(i))$ is an abelian group. Hence $Gal(\Omega/F) \cong Gal(\Omega/F(i)) \rtimes \langle\sigma\rangle$, where σ has order 2 and $\tau^\sigma = \tau^{-1}$ for every $\tau \in Gal(\Omega/F(i))$.

Proposition 4.7. *Let Ω/F be a Galois extension of fields which is p-closed and $\zeta_p \in \Omega$ for each prime p dividing the order of $G := Gal(\Omega/F)$. Then the following conditions are equivalent:*

(i) *G has Sylow-2-subgroups $\cong \mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$ or $\cong \mathbb{Z}/2\mathbb{Z}$.*

(ii) $2 \mid \#G$ *and* F *is hereditarily pythagorean w.r.t.* Ω *admitting at most two orderings.*

If, in addition, F *has an archimedean ordering or two independent orderings, then* $Gal(\Omega/F(i))$ *is cyclic, i.e.* $G \cong H \rtimes \mathbb{Z}/2\mathbb{Z}$ *for some* $H \leq \hat{\mathbb{Z}}$*. In this case* $F = R \cap R'$*, where* R *and* R' *are real closures of* F *in* Ω*.*

Proof. (i) $\Longrightarrow$ (ii) follows immediately from the facts that the order structure of F is the same as that of the fixed field of a Sylow 2-subgroup of G and that a subfield L of Ω over F is real maximal in Ω w.r.t. two orderings iff $Gal(\Omega/F) \cong \mathbb{Z}_2 \rtimes \mathbb{Z}/2\mathbb{Z}$ (cf. [BEK]).

The converse is a consequence of ([Be], Thm. 15, p. 118 and Thm. 16, p. 120) since for a field F hereditarily pythagorean w.r.t. Ω admitting at most two orderings we have that $(\dot{F} : \dot{F}^2) \leq 4$.

The first part of the last statement is a direct consequence of Cor. 4.5 and Remark 4.6. Finally, let R be a real closure of F in Ω, σ a generator of $Gal(\Omega/R)$ and h a generator of H. The action of σ on H implies that $h\sigma$ is also an involution. Let R' be the fixed field of $h\sigma$. Then $F = R \cap R'$. □

The next proposition completes Theorem 4.3 and also answers the question proposed by Brőcker [Br] after his Proposition 3.5.

Proposition 4.8. ([Br], Proposition 3.5) *Let* F *be a formally real field and let* Ω/F *be a Galois extension as in Corollary 4.5 such that* 2 *divides the order of* $Gal(\Omega/F)$*. The following conditions are equivalent:*

(i) F *is hereditarily pythagorean w.r.t.* Ω*.*
(ii) F *admits an* Ω*-henselian valuation* v *such that* $\kappa(v)$ *is the intersection of at most two real closures of* $\kappa(v)$ *in* $\kappa(w)$*, where* w *is the unique extension of* v *to* Ω*.*

Proof: (i) $\Longrightarrow$ (ii) By ([Br], Prop. 3.5) F admits Ω-henselian valuations with formally real residue field. Take v as the finest among those and let w be the extension of v to Ω. As a quotient of $Gal(\Omega/F(i))$, the Galois group $Gal(\kappa(w)/\kappa(v)(i))$ is abelian. Thus $\kappa(v)$ is hereditarily pythagorean w.r.t. $\kappa(w)$, as remarked above. On the other side, the choice of v makes sure that $\kappa(v)$ does not admit $\kappa(w)$-henselian valuations. Indeed, in a formally real field a 2-henselian valuation has formally real residue field. Therefore any $\kappa(w)$-henselian valuation of $\kappa(v)$ would induce, by ([Br], Lemma 1.3), a proper refinement of v. Thus, Cor. 4.5 implies that $Gal(\kappa(w)/\kappa(v)(i))$ is cyclic. Hence, as in the proof of the previous proposition, we can deduce that $\kappa(v)$ is the intersection of two real closures.

The other direction follows from ([Br], Prop. 3.5) (or Thm. 4.3). □

Appendix

As Y. Ershov pointed out to us, there is an alternative approach for deducing the existence of a p-henselian valuation with non-p-divisible value group from condition (iii) in 2.2.

Proposition A.1. *Let* F *be a field such that* $\zeta_p \in F$ *and* $(F : \dot{F}^p) > p$ $(p \neq 2)$*. Then (iii) of Proposition 2.2 implies that* F *admits a* p*-henselian valuation* v *such that* $char\, \kappa(v) \neq p$ *and* $\Gamma_v \neq p\Gamma_v$*.*

Proof. By 2.1, condition (iii) of 2.2 implies that for the subgroup $H \leq \dot{F}$ generated by the not strongly p-rigid elements one has $\dot{F}^p \leq H$ and $[H : \dot{F}^p] \leq p$.

We shall now make use of the results of [AEJ] with $T = \dot{F}^p$. Clearly every strongly p-rigid element is T-birigid (see Definition 1.8 of [AEJ]). Therefore the set $B_F(T)$ of the T-basic elements is contained in H. It then follows immediately from [AEJ], Thm. 2.16, that F admits a valuation v such that $1 + \mathcal{M}_v \subseteq \dot{F}^p$ and $\mathcal{O}_v^\times \cdot \dot{F}^p \subseteq H$ (observe that as $p \neq 2$, $\hat{H} = H$ ([AEJ], Thm. 2.16)). But $1 + \mathcal{M}_v \subseteq \dot{F}^p$ implies that v is p-henselian (since $\zeta_p \in F$), and $\mathcal{O}_v^\times \cdot \dot{F}^p \subseteq H \neq \dot{F}$ implies that $\Gamma_v \neq p\Gamma_v$. It remains to be checked that $char\, \kappa(v) \neq p$. Going for a contradiction, let us assume that $char\, \kappa(v) = p$. By Lemma 3.1 of [AEJ], $v(H)$ contains no non-trivial divisible convex subgroup. Therefore the same is true for $v(\dot{F}^p) \subset v(H)$, i.e. Γ_v contains no non-trivial p-divisible convex subgroup. Hence it would be possible to find some $a \in \mathcal{M}_v$ with $v(a) \leq v(p)$ and $v(a) \notin p\Gamma_v$. Indeed, if $v(p) \notin p\Gamma_v$ we take $a = p$. If $v(p) \in p\Gamma_v$, let Δ be the convex hull of the subgroup generated by $v(p)$. As $\Delta \not\subset p\Gamma_v$, there exists $\delta \in \Delta$ such that $\delta \notin p\Gamma_v$. Clearly we may assume $\delta > 0$. Now, for $n \geq 1$, the smallest number satisfying $\delta \leq nv(p)$, we take $a \in F$ such that $v(a) = \delta$ if $n = 1$, and $v(a) = \delta - (n-1)v(p)$ otherwise.

Now, $1 + a \in 1 + \mathcal{M}_v \subseteq \dot{F}^p$. Say $1 + a = (1+b)^p = 1 + p \cdot b + \ldots + b^p$ for some $b \in \mathcal{M}_v$. So $v(a) \leq v(p) < v(p \cdot b) < \ldots < v(p \cdot b^{p-1})$ implies $v(a) = v(b^p)$, contradicting $v(a) \notin p\Gamma_v$. □

For a similar analysis see Theorem 2.11 of [HJ].

The above approach at the same time gives an alternative proof of the Galois characterization of p-adic fields (Thm. 4.1 in [K2]) which does not depend on model theoretic arguments. To be precise, the crucial point in the proof of Thm. 4.1 of [K2] is the following proposition.

Proposition A.2 [[K2], Proposition 4.4]**.** *Let K be a field whose total Galois group is p-adic. Then, for every prime number q different from 2 and p, K admits a valuation w with $\Gamma_w \neq q\Gamma_w$.*

Proof. Just replace in the proof of the Proposition 4.4 of [K2] the occurrence of the Main Theorem of [K2] by the above result. □

References

[AEJ] J. Arason, R. Elman, and B. Jacob, *Rigid elements, valuations and realization of Witt rings*, J. Algebra **110** (1987), 449–467. MR **89a:**11041

[Be] E. Becker, *Hereditarily-pythagorean fields and orderings of higher level*, Monografias de Matemática 29, IMPA, Rio de Janeiro, 1978. MR **80f:**12021

[BEK] S. Bredikhin, Y. Ershov and V. E. Kal'nei, *Fields with two linear orderings*, Mat. Zametki **7** (1970), 319–325 (Russian); English transl., Math. Notes **7** (1970), 319–325. MR **42:**1812

[Br] L. Bről̋cker, *Characterization of fans and hereditarily pythagorean fields*, Math. Z. **151** (1976), 149–163. MR **54:**10224

[E] O. Endler, *On henselizations of valued fields*, Bol. Soc. Brasil. Mat. **4** (1973), 97–109. MR **54:**5203

[EE] O. Endler and A. J. Engler, *Fields with henselian valuation rings*, Math. Z. **152** (1977), 191–193. MR **55:**318

[Ef] I. Efrat, *Abelian subgroups of pro-2 Galois groups*, Proc. Amer. Math. Soc. **123** (1995), 1031–1035. MR **95e:**12007

[En] A. J. Engler, *Fields with two incomparable henselian valuation rings*, Manuscripta Math. **23** (1978), 373–385. MR **57:**3108

[EN] A. J. Engler and J. B. Nogueira, *Maximal abelian normal subgroups of Galois pro-2-groups*, J. Algebra **166** (1994), 481–505. MR **95b:**12004

[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. MR **97a:**12004

[K1] J. Koenigsmann, *p-henselian fields*, Manuscripta Math. **87** (1995), 89–99. MR **96c:**12010

[K2] ———, *From p-rigid elements to valuations (with a Galois-characterization of p-adic fields)*, J. Reine Angew. Math. **465** (1995), 165–182. MR **96m:**12003

[Po] F. Pop, *On Grothendieck's conjecture of birational anabelian geometry*, Ann. of Math. **139** (1994), 145–182. MR **94m:**12007

[Pr] A. Prestel, *Lectures on Formally Real Fields*, IMPA, Rio de Janeiro, 1975; and Springer Lecture Notes 1093, Berlin/New York, 1984. MR **86h:**12013

[W1] R. Ware, *When are Witt rings group rings?* II, Pacific J. Math. **76** (1978), 541–564. MR **58:**27920

[W2] ———, *Galois groups of maximal p-extensions*, Trans. Amer. Math. Soc. **333** (1992), 721–728. MR **92m:**12008

IMECC-UNICAMP, Caixa Postal 6065, 13083-970, Campinas, SP, Brasil
E-mail address: engler@ime.unicamp.br

Fakultät für Mathematik, Universität Konstanz, Postfach 5560, D-78434 Konstanz, Germany
E-mail address: jochen.koenigsmann@uni-konstanz.de