# DEMUSHKIN GROUPS AND INVERSE GALOIS THEORY FOR PRO-$p$-GROUPS OF FINITE RANK AND MAXIMAL $p$-EXTENSIONS

I.D. CHIPCHAKOV

Abstract. This paper proves that if $E$ is a field, such that the Galois group $\mathcal{G}(E(p)/E)$ of the maximal $p$-extension $E(p)/E$ is a Demushkin group of finite rank $r(p)_E \geq 3$, for some prime number $p$, then $\mathcal{G}(E(p)/E)$ does not possess nontrivial proper decomposition groups. When $r(p)_E = 2$, it describes the decomposition groups of $\mathcal{G}(E(p)/E)$. The paper shows that if $(K, v)$ is a $p$-Henselian valued field with $r(p)_K \in \mathbb{N}$ and a residue field of characteristic $p$, then $P \cong \widetilde{P}$ or $P$ is presentable as a semidirect product $\mathbb{Z}_p^\tau \rtimes \widetilde{P}$, for some $\tau \in \mathbb{N}$, where $\widetilde{P}$ is a Demushkin group of rank $\geq 3$ or a free pro-$p$-group. It also proves that when $\widetilde{P}$ is of the former type, it is continuously isomorphic to $\mathcal{G}(K'(p)/K')$, for some local field $K'$ containing a primitive $p$-th root of unity.

## 1. Introduction and statements of the main results

Let $P$ be a pro-$p$-group, for some prime number $p$, and let $r(P)$ be the rank of $P$, i.e. the cardinality of any minimal system of generators of $P$ as a profinite group. This paper is devoted to the study of $P$ in case $r(P) \in \mathbb{N}$ and $P$ is admissible, i.e. (continuously) isomorphic to the Galois group $\mathcal{G}(E(p)/E)$ of the maximal $p$-extension $E(p)$ of a field $E$ (in a separable closure $E_{\rm sep}$ of $E$). Denote for brevity by $r(p)_E$ the rank of $\mathcal{G}(E(p)/E)$. It is known that if $p = {\rm char}(E)$, then $\mathcal{G}(E(p)/E)$ is a free pro-$p$-group (cf. [33], Ch. II, Proposition 2), so we consider fields of characteristic different from $p$. Recall that if $r(P) = 1$, then $P$ is admissible if and only if it is isomorphic to the additive group $\mathbb{Z}_p$ of $p$-adic integers or $p = 2$ and $P$ is of order 2 (cf. [39], Theorem 2). Admissible $P$ have been described, up-to isomorphisms, in the special case where $r(P) = 2$ and the ground field contains a primitive $p$-th root of unity (see [24], page 107, and [17]). The description relies on the fact that then $P$ is a free pro-$p$-group or a Demushkin group unless $p = 2$ and $E$ is a formally real field, in the sense of Artin-Schreier (cf. [38], Lemma 7, [26], Ch. XI, Sect. 2, and [32], Ch. I, 3.3 and 4.5).

In this paper, we focus our attention on the case where $r(P) \geq 3$ and the considered ground fields are endowed with $p$-Henselian valuation. Our starting point is the following result of local class field theory concerning $r(p)_F = r$, for an arbitrary finite extension $F$ of the field $\mathbb{Q}_p$ of $p$-adic numbers of degree $N$ (see [3] and [33], Ch. II, Theorems 3 and 4):

*Key words and phrases.* Maximal $p$-extension, Demushkin group, $p$-Henselian field, immediate extension, Brauer group, norm group, symbol algebra. MSC 2010 Subject Classification: 12J10 (Primary); 12F10 12E30.

(1.1) (i) $r = N + 2$ in case $F$ contains a primitive $p$-th root of unity; $r = N + 1$, otherwise.

(ii) The index of $F^{*p}$ in the multiplicative group $F^*$ of $F$ is equal to $p^r$.

The structure of $\mathcal{G}(F(p)/F)$ is determined as follows:

(1.2) $\mathcal{G}(F(p)/F)$ is a free pro-$p$-group, if $F$ does not contain a primitive $p$-th root of unity (Shafarevich [35], see also [33], Ch. II, Theorem 3); $\mathcal{G}(F(p)/F)$ is a Demushkin group, otherwise (Demushkin [10, 11], Labute [24] and Serre [32], see also [33], Ch. II, Theorem 4).

For convenience of the reader, we recall that an infinite pro-$p$-group $P$ is said to be a Demushkin group, if the continuous cohomology group homomorphism $\varphi_h\colon\ H^1(P,\mathbb{F}_p) \to H^2(P,\mathbb{F}_p)$ mapping each $g \in H^1(P,\mathbb{F}_p)$ into the cup-product $h \cup g$ is surjective, for every $h \in H^1(P,\mathbb{F}_p) \setminus \{0\}$, and the group $H^2(P,\mathbb{F}_p)$ is of order $p$ (throughout this paper, $\mathbb{F}_p$ denotes a field with $p$ elements). The papers referred to in (1.2) contain a classification, up-to a continuous isomorphism, of Demushkin pro-$p$-groups of finite ranks, for each prime $p$. In particular, this classification yields the following:

(1.3) (i) The ranks of finitely-generated Demushkin pro-$p$-groups are even numbers, provided that $p > 2$;

(ii) For each pair $(d,\theta)$ of positive integers with $2 \mid d$, there exists a Demushkin group $P_{d,\theta}$, such that $r(P_{d,\theta}) = d$ and the reduced component of the (continuous) character group $C(P_{d,\theta})$ is cyclic of order $p^{\theta-1}$; when $p > 2$ or $\theta \neq 2$, $P_{d,\theta}$ is uniquely determined, up-to an isomorphism;

(iii) For any integer $d \geq 2$, there are pairwise nonisomorphic Demushkin pro-2-groups $D_n$, $n \in \mathbb{N}$, such that $r(D_n) = d$ and the reduced components of $C(D_n)$ are of order 2, for each index $n$.

As shown by Pop [31], (2.7), statement (1.2) retains validity, if $(F,v)$ is a Henselian real-valued field with a residue field $\widehat{F}$ of characteristic $p$, a $p$-indivisible value group $v(F)$ and a finite quotient group $F^*/F^{*p}$. These results relate the admissibility problem for Demushkin groups of finite ranks with the open question of whether every admissible Demushkin group $\widetilde{P}$ of rank $r(\widetilde{P}) \geq 3$ is standardly admissible, i.e. $\widetilde{P} \cong \mathcal{G}(F(p)/F)$, for some finite extension $F/\mathbb{Q}_p$ (see [14], Proposition 8.2). In view of the irreducibility of the $p^n$-th cyclotomic polynomial over $\mathbb{Q}_p$, for every $n \in \mathbb{N}$ (cf. [20], Ch. 8, Theorem 1), the papers quoted in (1.2) (ii) give the following necessary conditions for standard admissibility of $\widetilde{P}$; in view of (1.1), (1.2) and (1.3), these conditions are sufficient in case $p > 2$ (see also [15], Theorem 7.3):

(1.4) With notations being as in (1.3) (ii), $\widetilde{P} \cong P_{d,\theta}$, where $\theta \geq 2$, $d \geq 3$ and $d - 2$ is divisible by $(p-1)p^{(\theta-2)}$.

These results have been extended by Efrat [13, 14] to the case of $p$-Henselian fields containing a primitive $p$-th root of unity (see [28], for an earlier result of this kind concerning the absolute Galois groups of arbitrary Henselian fields). The purpose of this paper is to extend the scope of (1.2) along the lines drawn by Efrat (see [13], page 216). In order to simplify the description of the obtained results, consider first an arbitrary nontrivially valued field $(K,v)$. In what follows, $O_v(K)$ and $\widehat{K}$ will be the valuation ring and the residue field of $(K, v)$, respectively, and $K_{h(v)}$ will be a fixed Henselization of $K$ in $K_{\mathrm{sep}}$ relative to $v$ (it is known that $K_{h(v)}$ is uniquely determined by $(K, v)$, up-to a $K$-isomorphism, see [15]). Given a prime number $p \neq \mathrm{char}(K)$, we denote by $\varepsilon$ some primitive $p$-th root of unity in $K_{\mathrm{sep}}$, and by $G(K)$ the minimal isolated subgroup of $v(K)$ containing $v(p)$. By definition, $\Delta(v)$ is the following subgroup of $v(K)$: $\Delta(v) = G(K)$ in case $\varepsilon \notin K_{h(v)}$; if $\varepsilon \in K_{h(v)}$, $[K(\varepsilon)\colon K] = m$ and $v'$ is a valuation of $K(\varepsilon)$ extending $v$, then $\Delta(v)$ is the minimal isolated subgroup of $v(K)$ containing the values $v'((\varepsilon - c)^m)\colon\ c \in O_v(K),\ c \neq \varepsilon$. It is easy to see that $G(K) = \{0\}$ unless $\mathrm{char}(\widehat{K}) = p$, and that $\Delta(v)$ does not depend on the choice of $v'$. With these notation, the main results of this paper can be stated as follows:

**Theorem 1.1.** *Let $(K, v)$ be a $p$-Henselian field with* $\mathrm{char}(K) = 0$, $\mathrm{char}(\widehat{K}) = p$ *and $r(p)_K \in \mathbb{N}$. Then $\widehat{K}$ is perfect and the following conditions hold:*

(i) *$\mathcal{G}(K(p)/K)$ is a free pro-$p$-group if and only if $\varepsilon \notin K_{h(v)}$ or $\Delta(v) = p\Delta(v)$;*

(ii) *$\mathcal{G}(K(p)/K)$ is isomorphic to a topological semidirect product $\mathbb{Z}_p^{\kappa} \rtimes \Psi$, for some $\kappa \in \mathbb{N}$ and a free pro-$p$-group $\Psi$, if and only if $G(K) = pG(K)$, $\varepsilon \in K_{h(v)}$ and the group $\Delta(v)/p\Delta(v)$ is of order $p^{\kappa}$.*

**Theorem 1.2.** *Let $(K, v)$ be a $p$-Henselian field, such that* $\mathrm{char}(K) = 0$, $\mathrm{char}(\widehat{K}) = p$ *and $G(K) \neq pG(K)$. Then $r(p)_K \in \mathbb{N}$ if and only if $\widehat{K}$ is finite, $G(K)$ is cyclic and, in case $\varepsilon \in K_{h(v)}$, the group $\Delta(v)/p\Delta(v)$ is finite. When this holds, the following conditions are equivalent:*

(i) *$\mathcal{G}(K(p)/K) \cong \mathbb{Z}_p^{\kappa-1} \rtimes \Psi$, where $\kappa \in \mathbb{N}$ and $\Psi$ is a standardly admissible Demushkin group with $r(\Psi) \geq 3$;*

(ii) *$\varepsilon \in K_{h(v)}$ and $\Delta(v)/p\Delta(v)$ is of order $p^{\kappa}$.*

*In particular, $\mathcal{G}(K(p)/K)$ is a Demushkin group if and only if $\varepsilon \in K_{h(v)}$ and the group $\Delta(v)/G(K)$ is $p$-divisible.*

It is known that if $(E, w)$ is a valued field and $\Omega/E$ is a Galois extension, then the Galois group $\mathcal{G}(\Omega/E)$ acts transitively on the set $w(\Omega/E)$ of valuations of $\Omega$ extending $w$, whose value groups are included in a fixed divisible hull of $w(E)$. Therefore, the decomposition groups of $\mathcal{G}(\Omega/E)$ attached to $w$, i.e. the stabilizers $\mathrm{Stab}(w') = \{\psi \in \mathcal{G}(\Omega/E)\colon\ w' \circ \psi = w'\}$, where $w'$ runs across $w(\Omega/E)$, form a conjugacy class in $\mathcal{G}(\Omega/E)$. Recall that each admissible pro-$p$-group $P$ is isomorphic to $\mathcal{G}(L(p)/L)$, for some Henselian field $(L, \omega)$ (and thereby is realizable as a decomposition group). Indeed, it is known (see, e.g., [18], Ch. 4, Sects. 6 and 7) that for each field $F$ and ordered abelian group $\Gamma$ there exists a Henselian field $(K, v)$ with $\widehat{K} \cong F$ and $v(K) = \Gamma$, so the noted property of $P$ can be obtained from (2.3) (ii) and (2.7). Note also that, by the Endler-Engler-Schmidt theorem, see [16], for any nontrivial valuation $\omega'$ of $L$, which is independent of $\omega$, the decomposition group of $\mathcal{G}(L(p)/L)$ attached to $\omega$ is trivial. Our third main result proves that if $P$ is an admissible Demushkin group and $3 \leq r(P) < \infty$, then its nontrivial proper subgroups are not realizable as decomposition groups.

**Theorem 1.3.** *Let $E$ be a field with a nontrivial Krull valuation $w$. Assume that $v$ is not $p$-Henselian, $\mathcal{G}(E(p)/E)$ is a Demushkin group, $r(p)_E \in \mathbb{N}$ and $r(p)_E \geq 3$. Then $E(p)$ is included in any Henselization $E_{h(v)} \subseteq E_{\rm sep}$.*

The main results of this paper enable one to show (see Remarks 7.3 and 5.3) that admissible Demushkin pro-$p$-groups of rank $\geq 3$ will be standardly admissible, if the considered ground fields contain primitive $p$-th roots of unity, and the following open problem has an affirmative solution:

(1.5) Let $F$ be a field, such that $r(p)_F \geq 1$ and $F(p) \subseteq F_{h(\omega)}$, for each nontrivial Krull valuation $\omega$ of $F$, and suppose that the transcendency degree of $F$ over its prime subfield is finite. Is $\mathcal{G}(F(p)/F)$ a free pro-$p$-group?

It is known (see [36], page 265, and [32], Ch. I, 4.2) that if $F$ is a field with a primitive $p$-th root of unity, then $\mathcal{G}(F(p)/F)$ is a free pro-$p$-group if and only if $r(p)_F \geq 1$ and the $p$-component ${\rm Br}(F)_p$ of the Brauer group ${\rm Br}(F)$ is trivial. When $F(p) = F_{\rm sep}$ and $p \neq {\rm char}(F)$, the fulfillment of (1.5) implies that ${\rm Br}(F) = \{0\}$ in all presently known cases, since then $F$ turns out to be pseudo algebraically closed, i.e. each geometrically irreducible affine variety defined over $F$ has an $F$-rational point (see [19], Theorem 10.17 and Problem 11.5.9, and [33], Ch. II, 3.1).

The basic notation, terminology and conventions kept in this paper are standard and virtually the same as in [6]. Throughout, $\mathbb{P}$ denotes the set of prime numbers, Brauer and value groups are written additively, Galois groups are viewed as profinite with respect to the Krull topology, and by a profinite group homomorphism, we mean a continuous one. For any field $E$, $E^*$ denotes its multiplicative group, $E^{*n} = \{a^n\colon\ a \in E^*\}$, for each $n \in \mathbb{N}$, $\mathcal{G}_E = \mathcal{G}(E_{\rm sep}/E)$ stands for the absolute Galois group of $E$, and for each $p \in \mathbb{P}$, ${}_p{\rm Br}(E) = \{b_p \in {\rm Br}(E)\colon\ pb_p = 0\}$ and $P(E) = \{p \in \mathbb{P}\colon\ E(p) \neq E\}$. We denote by $s(E)$ the class of finite-dimensional simple $E$-algebras, $d(E)$ is the subclass of division algebras from $s(E)$, and for each $A \in s(E)$, $[A]$ is the similarity class of $A$ in ${\rm Br}(E)$. As usual, ${\rm Br}(E'/E)$ denotes the relative Brauer group of an arbitrary field extension $E'/E$. We write $\rho_{E'/E}$ for the scalar extension map of ${\rm Br}(E)$ into ${\rm Br}(E')$, and ${\rm I}(E'/E)$ for the set of intermediate fields of $E'/E$.

The paper is organized as follows: Section 2 includes preliminaries on Krull valuations used in the sequel. Section 3 contains characterizations of free pro-$p$-groups and of Demushkin groups of finite ranks in the class of Galois groups of maximal $p$-extensions. The proof of Theorems 1.1 and 1.2 is divided into three parts presented in Sections 4, 5 and 6. This allows us to determine the structure of $\mathcal{G}(K(p)/K)$ by a reduction to the special case where $K$ contains a primitive $p$-th root of unity (see Remark 6.3). Specifically, it becomes clear (Corollary 6.4) that a pro-$p$-group $P$ of rank 2 is isomorphic to $\mathcal{G}(K(p)/K)$, for some $p$-Henselian field $(K, v)$, if and only if $P$ is a free pro-$p$-group or a Demushkin group. Theorem 1.3 is deduced from Theorems 1.1 and 1.2 in Section 7, where we also present a description of the decomposition groups of Demushkin groups of rank 2.

## 2. **Preliminaries on Henselian $\Omega$-valuations**

Let $K$ be a field with a nontrivial valuation $v$, $O_v(K) = \{a \in K\colon\ v(a) \geq 0\}$ the valuation ring of $(K,v)$, $M_v(K) = \{\mu \in K\colon\ v(\mu) > 0\}$ the maximal ideal of $O_v(K)$, $v(K)$ and $\widehat{K} = O_v(K)/M_v(K)$ the value group and the residue field of $(K,v)$, respectively. For each $\gamma \in v(K)$, $\gamma \geq 0$, we denote by $\nabla_\gamma(K)$ the set $\{\lambda \in K\colon\ v(\lambda - 1) > \gamma\}$. As usual, the completion of $K$ relative to (the topology induced by) $v$ is denoted by $K_v$, and is considered with its valuation $\bar{v}$ continuously extending $v$. Whenever $v(E)$ is Archimedean, i.e. it is embeddable as an ordered subgroup in the additive group $\mathbb{R}$ of real numbers, we identify $v(E)$ with its isomorphic copy in $\mathbb{R}$. In what follows, $\mathrm{Is}_v(K)$ denotes the set of isolated subgroups of $v(K)$ different from $v(K)$. It is well-known (cf. [2], Ch. VI, Sect. 4.3) that each $H \in \mathrm{Is}_v(K)$ is a pure subgroup of $v(K)$, the ordering of $v(K)$ induces canonically on $v(K)/H$ a structure of an ordered group, and one can naturally associate with $v$ and $H$ a valuation $v_H$ of $K$ with $v_H(K) = v(K)/H$. Unless specified otherwise, $K_H$ will denote the residue field of $(K, v_H)$, $\eta_H$ the natural projection $O_{v_H}(K) \to K_H$, and $\hat{v}_H$ the valuation of $K_H$ induced canonically by $v$ and $H$. The valuations $v$, $v_H$ and $\hat{v}_H$ are related as follows:

(2.1) (i) $\hat{v}_H(K_H) = H$, $\widehat{K}_H$ is isomorphic to $\widehat{K}$ and $\eta_H$ induces a surjective homomorphism of $O_v(K)$ upon $O_{\hat{v}_H}(K_H)$ (cf. [15], Proposition 5.2.1).

(ii) For each $H \in \mathrm{Is}_v(K)$, $v_H$ induces on $K$ the same topology as $v$; the mapping of $\mathrm{Is}_v(K)$ on the set $V_v$ of proper subrings of $K$ including $O_v$, by the rule $X \to v_X(K)$, $X \in \mathrm{Is}_v(K)$, is an inclusion-preserving bijection.

(iii) If $v(K)$ properly includes the union $H(K)$ of the groups $H \in \mathrm{Is}_v(K)$, then $v(K)/H(K)$ is Archimedean (cf. [15], Theorem 2.5.2).

We say that the valuation $v$ is $\Omega$-Henselian, for a given normal extension $\Omega/K$, if $v$ is uniquely, up-to an equivalence, extendable to a valuation $v_L$ on each $L \in I(\Omega/K)$. In order that $v$ is $\Omega$-Henselian, it is necessary and sufficient that the Hensel-Rychlik condition holds (cf. [15], Sect. 18.1):

(2.2) Given a polynomial $f(X) \in O_v(K)[X]$, which fully decomposes in $\Omega[X]$, and an element $a \in O_v(K)$, such that $2v(f'(a)) < v(f(a))$, where $f'$ is the formal derivative of $f$, there is a zero $c \in O_v(K)$ of $f$ satisfying the equality $v(c - a) = v(f(a)/f'(a))$.

If $v$ is $\Omega$-Henselian and $L \in I(\Omega/K)$, then $v_L$ is $\Omega$-Henselian. In this case, we denote by $\widehat{L}$ the residue field of $(L, v_L)$, put $v(L) = v_L(L)$, and write $L_v$ for the completion of $L$ with respect to $v_L$. When $v(K)$ is non-Archimedean, the $\Omega$-Henselian property can be also characterized as follows:

**Proposition 2.1.** *Let $(K,v)$ be a valued field, and let $H \in \mathrm{Is}_v(K)$. Then $v$ is $\Omega$-Henselian if and only if $v_H$ is $\Omega$-Henselian and $\hat{v}_H$ is $\widehat{\Omega}$-Henselian.*

*Proof.* Suppose first that $v_H$ is $\Omega$-Henselian and $\hat{v}_H$ is $\widehat{\Omega}$-Henselian. Fix a monic polynomial $f(X) \in O_v(K)[X]$, which fully decomposes over $\Omega$ and has a simple zero $\beta \in O_v(K)$ modulo $M_v(K)$. Denote by $\hat{f}_H$ the reduction of $f$ modulo $M_{v_H}(K)$. Then $\beta \in O_{v_H}(K)$, $\hat{f}_H(X) \in O_{\hat{v}_H}(K_H)[X]$, and the residue class $\hat{\beta}_H \in K_H$ is a simple zero of $\hat{f}_H$ modulo $M_{\hat{v}_H}(K_H)$. Hence, by the $\widehat{\Omega}$-Henselian property of $\hat{v}_H$, $\hat{f}_H$ has a simple zero $\tilde{\alpha}_H \in O_{\hat{v}_H}(K_H)$, such that $\hat{\beta}_H - \tilde{\alpha}_H \in M_{\hat{v}_H}(K_H)$. Now take a preimage $\alpha_H$ of $\tilde{\alpha}_H$ in $O_{v_H}(K)$. The preceding observations indicate that $f(\alpha_H) \in M_{v_H}(K)$ and $f'(\alpha_H) \notin M_{v_H}(K)$. Since $v_H$ is $\Omega$-Henselian, it follows from (2.2) that $O_{v_H}(K)$ contains a simple zero $\alpha$ of $f$ with the property that $\alpha - \alpha_H \in M_{v_H}(K)$. As $O_v(K)$ is an integrally closed ring, it is now easy to see that $\alpha \in O_v(K)$ and $\alpha - \beta \in M_v(K)$, which proves that $v$ is $\Omega$-Henselian.

Conversely, assume that $v$ is $\Omega$-Henselian, fix a finite field extension $L/K$, denote by $O_H(L)$ the integral closure of $O_{v_H}(K)$ in $L$, and let $w_1$ and $w_2$ be valuations of $L$ extending $v_H$. The $\Omega$-Henselian property of $v$ ensures that $O_v(L)$ equals the integral closure of $O_v(K)$ in $L$. At the same time, one concludes that $O_v(L) \subseteq O_H(L) \subseteq O_{w_j}(L)$ and $O_{w_j}(L) = O_{v_L,H_j}(L)$, for some $H_j \in \mathrm{Is}_{v_L}(L)$, $j = 1, 2$. Since the set of valuation subrings of $L$ including $O_v(L)$ is a chain with respect to set-theoretic inclusion, one can assume without loss of generality that $O_{w_1}(L) \subseteq O_{w_2}(L)$, whence $H_1 \subseteq H_2$ (see [2],Ch. VI, Sect. 4, Proposition 4). As $H_j \in \mathrm{Is}_{v_L}(L)$, $j = 1, 2$, this means that $H_2/H_1$ is a torsion-free group, whereas Ostrowski's theorem implies that $H$ is a subgroup of $H_j$ of index dividing $[L\colon K]$, for each index $j$. Therefore, $H_2/H_1$ is a homomorphic image of $H_2/H$, whence its order also divides $[L\colon K]$. The obtained results prove that $H_1 = H_2$ and $v_H$ is $\Omega$-Henselian. It remains to be seen that $\hat{v}_H$ is $\widehat{\Omega}$-Henselian. Let $\tilde{h}(X) = X^n + \sum_{i=0}^{n-1} \tilde{a}_i X^{n-i} \in O_{\hat{v}_H}(K_H)[X]$ have a simple zero $\tilde{\eta} \in O_{\hat{v}_H}(K_H)$ modulo $M_{\hat{v}_H}(K_H)$, and let $a_i$ be a preimage of $\tilde{a}_i$ in $O_{\hat{v}_H}(K_H)$, for $i = 1, \dots, n-1$. Then $h(X) = X^n + \sum_{i=0}^{n-1} a_i X^{n-i}$ lies in $O_v(K)[X]$ and $O_v(K)$ contains any preimage $\eta$ of $\tilde{\eta}$ in $O_{v_H}(K)$. Moreover, by the $\Omega$-Henselity of $v$, the coset $\eta + M_v(K)$ contains a simple zero $\xi$ of $h$. This implies $\tilde{h}(\hat{\xi}_H) = 0$, $\tilde{h}'(\hat{\xi}_H) \neq 0$ and $\hat{\xi}_H - \tilde{\eta} \in M_{\hat{v}_H}(K_H)[X]$, which proves that $\hat{v}_H$ is $\widehat{\Omega}$-Henselian. □

A finite extension $R$ of $K$ in $\Omega$ is said to be inertial, if $R$ has a unique, up-to an equivalence, valuation $v_R$ extending $v$, the residue field $\widehat{R}$ of $(R, v_R)$ is separable over $\widehat{K}$, and $[R\colon K] = [\widehat{R}\colon \widehat{K}]$. When $v$ is $\Omega$-Henselian, these extensions have the following frequently used properties (see [21], page 135 and Theorems 2.8 and 2.9, for the case where $v$ is Henselian):

(2.3) (i) An inertial extension $R$ of $K$ in $\Omega$ is Galois if and only if $\widehat{R}/\widehat{K}$ is Galois. When this holds, $\mathcal{G}(R/K)$ and $\mathcal{G}(\widehat{R}/\widehat{K})$ are canonically isomorphic.

(ii) The set of inertial extensions of $K$ in $\Omega$ is closed under the formation of subextensions and finite compositums. The compositum $\Omega_0$ of these extensions is Galois over $K$ with $\mathcal{G}(\Omega_0/K) \cong \mathcal{G}(\widehat{\Omega}/\widehat{K})$.

**Proposition 2.2.** *Let $(K, v)$ be a nontrivially valued field and $(K_{h(v)}, \sigma)$ a Henselization of $(K, v)$. Then the residue field of $(K_{h(v)}, \sigma_H)$ is isomorphic to $K_H$, for each $H \in \mathrm{Is}_v(K)$. Moreover, if $v(p) \in H$, for some $p \in \mathbb{P}$, then $K_{h(v)}$ contains a primitive $p$-th root of unity if and only if so does $K_H$.*

*Proof.* Fix Henselizations $(K_{h(v_H)}, \omega_H)\colon\ K_{h(v_H)} \subseteq K_{\mathrm{sep}}$, and $(\widetilde{\Phi}, \tilde{v}_H)\colon\ \widetilde{\Phi} \subseteq K_{H,\mathrm{sep}}$, of $(K, v_H)$ and $(K_H, \hat{v}_H)$, respectively, and denote by $\Sigma(H)$ the compositum of the inertial extensions of $K_{h(v_H)}$ in $K_{\mathrm{sep}}$ relative to $\sigma_H$. Also, let

$\Phi$ be the preimage of $\widetilde{\Phi}$ under the bijection $I(\Sigma(H))/K_{h(v_H)}) \to I(\widehat{K}_{\rm sep}/\widehat{K})$, canonically induced by the natural homomorphism of $O_{\omega_H}(\Sigma(H))$ into $\widehat{K}_{\rm sep}$, and let $\varphi_H$ be the valuation of $\Phi$ extending $\omega_H$. It follows from Proposition 2.1 and [15], Theorem 15.3.5, that $(K_{h(v_H)}, \omega_H)$ can be chosen so that $K_{h(v_H)} \subseteq K_{h(v)}$ and $\omega_H$ is induced by $\sigma_H$. It is easily verified that $\widetilde{\Phi}$ is the residue field of $(\Phi, \varphi_H)$ and there exists a valuation $\phi$ of $\Phi$, such that $\phi_H = \varphi_H$ and $\hat{\phi}_H = \tilde{v}_H$. Moreover, it follows from Proposition 2.1, the definition of $\widetilde{\Phi}$ and the observation concerning $(K_{v_H}, \omega_H)$ that $(\Phi, \phi)$ is a Henselization of $(K, v)$. In view of [15], Theorem 15.3.5, this proves the former assertion of Proposition 2.2. The rest of our proof relies on the well-known fact that a field $F$ with a Henselian valuation $f$ contains a primitive $p$-th root of unity, for a given $p \in \mathbb{P}$, $p \neq \mathrm{char}(\widehat{F})$, if and only if $\widehat{F}$ contains such a root. When $v(p) \in H$, this applies to $(\Phi, \varphi_H)$, so the latter assertion of Proposition 2.2 can be viewed as a consequence of the former one. □

The following lemma plays a major role in the study of $\mathcal{G}(K(p)/K)$ when $(K, v)$ is $p$-Henselian (i.e. $K(p)$-Henselian, see also (2.4)). For convenience of the reader, we prove the lemma here (referring to [27], for a much more general result in the case where $K$ is dense in its Henselizations).

**Lemma 2.3.** *Let $(K, v)$ be a valued field and $\widetilde{F}$ an extension of $\widehat{K}$ in $\widehat{K}(p)$ of degree $p \in \mathbb{P}$. Then $\widetilde{F}$ has an inertial lift in $K(p)$ over $K$, i.e. there exists an inertial extension $F$ of $K$ in $K(p)$, such that $\widehat{F} \cong \widetilde{F}$ over $\widehat{K}$.*

*Proof.* If $\mathrm{char}(K) = p$, then our assertion is an easy consequence of the Artin-Schreier theory, so we assume further that $\mathrm{char}(K) = p' \neq p$. Suppose first that $v$ is of height $n \in \mathbb{N}$. When $n = 1$, our assertion is a special case of Grunwald-Wang's theorem (cf. [27]). Proceeding by induction on $n$, we prove the statement of the lemma, under the hypothesis that $n \geq 2$ and it holds for valued fields of heights $< n$. Let $H$ be the maximal group from $\mathrm{Is}_v(K)$. Then the valuation $\hat{v}_H$ of $K_H$ is of height $n-1$ and, by the inductive hypothesis, $\widetilde{F}$ has an inertial lift $\widetilde{F}_H \subseteq K_H(p)$ over $K_H$ relative to $\hat{v}_H$. Note also that if $F \in I(K(p)/K)$ is an inertial lift of $\widetilde{F}_H$ over $K$ relative to $v_H$, then it is an inertial lift of $\widetilde{F}$ over $K$ with respect to $v$ as well.

In order to complete the proof of Lemma 2.3 it remains to be seen that it reduces to the special case in which $v$ is of finite height. Let $\mathbb{F}$ be the prime subfield of $K$. Clearly, it suffices to show that one may consider only the case where $K/\mathbb{F}$ has finite transcendency degree. Fix a Henselization $(K_{h(v)}, \sigma)$ of $(K, v)$ (with $K_{h(v)} \in I(K_{\rm sep}/K)$) and an inertial lift $H(\widetilde{F}) \in I(K_{\rm sep}/K_{h(v)})$ of $\widetilde{F}$ over $K_{h(v)}$. Let $f(X) = X^p + \sum_{i=1}^{p} c_i X^{p-i}$ be the minimal polynomial over $K_{h(v)}$ of some primitive element $\eta_1$ of $H(\widetilde{F})/K_{h(v)}$ lying in $O_\sigma(H(\widetilde{F}))$. Denote by $S$ the set $\{\eta_i\colon\ i = 1, \dots, p\}$ of zeroes of $f(X)$ in $K_{\rm sep}$, and by $T$ the set of $K_{h(v)}$-coordinates of the zeroes $\eta_i\colon\ i = 2, \dots, p$, with respect to the $K_{h(f)}$-basis $\eta_1^{j-1}$, $j = 1, \dots, p$, of $H(\widetilde{F})$. Our choice of $\eta_1$ ensures the inclusion $Y_f = \{c_i\colon\ i = 1, \dots, p\} \subset O_\sigma(K_{h(v)})$. As the valued extension $(K_{h(v)}, \sigma)/(K, v)$ is immediate, $O_v(K)$ contains a system of representatives $Y_f' = \{c_i'\colon\ i = 1, \dots, p\}$ of the elements of $Y_f$ modulo the ideal $M_\sigma(K_{h(v)})$.

Let $S'$ and $T'$ be the sets of coefficients of the minimal (monic) polynomials over $K$ of the elements of $Y_f$ and $T$, respectively, and let $\Lambda_0$ be the extension of $\mathbb{F}$ generated by the union $Y_f \cup Y_f' \cup S \cup S' \cup T \cup T'$. Assume that $\Lambda$ is the algebraic closure of $\Lambda_0$ in $K_{\rm sep}$, $\Phi = K \cap \Lambda$, $\Phi' = K_{h(v)} \cap \Lambda$, and $\psi$ and $\psi'$ are the valuations induced by $\sigma$ on $\Phi$ and $\Phi'$, respectively. It is easily verified that the polynomial $g(X) = X^p + \sum_{i=1}^p c_i' X^{p-i}$ lies in $O_\psi(\Phi)[X]$ and the root field $\widetilde{F}_0$, over $\widehat{\Phi}$, of its reduced polynomial $\hat{g}$ modulo $M_\psi(\Phi)$ is a cyclic extension of $\widehat{\Phi}$ of degree $p$. Observing that $\psi$ is of height $\leq 1+d$, where $d$ is the transcendency degree of $\Phi/\mathbb{F}$, one concludes that $\widetilde{F}_0$ has an inertial lift $F_0 \in I(\Phi(p)/\Phi)$ over $\Phi$. Since $\hat{g}$ remains irreducible over $\widehat{K}$, the compositum $F = F_0K$ is an inertial lift of $\widetilde{F}$ over $K$, so Lemma 2.3 is proved. $\square$

When $(K, v)$ is a $p$-Henselian field, for a given $p \in \mathbb{P}$, (2.3) and Lemma 2.3, combined with Galois theory and the subnormality of proper subgroups of finite $p$-groups (cf. [26], Ch. I, Sect. 6), imply the following assertions:

(2.4) (i) Each finite extension $\widetilde{F}$ of $\widehat{K}$ in $\widehat{K}(p)$, possesses a uniquely determined, up-to a $K$-isomorphism, inertial lift over $K$ relative to $v$;
(ii) The residue field of $(K(p), v_{K(p)})$ is $\widehat{K}$-isomorphic to $\widehat{K}(p)$.

Statements (2.4) and the following assertion reduce the study of a number of algebraic properties of maximal $p$-extensions of $p$-Henselian fields to the special case of Henselian ground fields:

(2.5) Let $(K, v)$ be a $p$-Henselian field, $(K_{h(v)}, \sigma)$ a Henselization of $(K, v)$, and $U$ the compositum of inertial extensions of $K$ in $K(p)$ relative to $v$. Then $UK_{h(v)}$ is $K_{h(v)}$-isomorphic to the tensor product $U \otimes_K K_{h(v)}$, and equals the compositum of inertial extensions of $K_{h(v)}$ in $K_{h(v)}(p)$ relative to $\sigma$.

Statement (2.5) is implied by (2.4) and the fact that $(K_{h(v)}, \sigma)$ is immediate over $(K, v)$. In the sequel, we will also need the following characterization of finite extensions of $K_v$ in $K_v(p)$, in case $v$ is $p$-Henselian with $v(K)$ Archimedean (cf. [2], Ch. VI, Sect. 8.2, and [21], page 135):

(2.6) (i) Every finite extension $L$ of $K_v$ in $K_{v,{\rm sep}}$ is $K_v$-isomorphic to $\widetilde{L} \otimes_K K_v$ and $\widetilde{L}_v$, where $\widetilde{L}$ is the separable closure of $K$ in $L$. The extension $L/K_v$ is Galois if and only if so is $\widetilde{L}/K$; when this holds, $\mathcal{G}(L/K_v)$ and $\mathcal{G}(\widetilde{L}/K)$ are canonically isomorphic.
(ii) $K_{\rm sep} \otimes_K K_v$ is a field and there are canonical isomorphisms $K_{\rm sep} \otimes_K K_v \cong K_{v,{\rm sep}}$ and $\mathcal{G}_K \cong \mathcal{G}_{K_v}$.

For example, when ${\rm char}(K) = 0$, $\widehat{K}$ is finite, ${\rm char}(\widehat{K}) = p$ and the minimal group $G(K) \in {\rm Is}_v(K)$ containing $v(p)$ is cyclic, (2.6) allows us to determine the structure of $\mathcal{G}(K(p)/K)$ in accordance with (1.1) and (1.2). As noted in the Introduction, the concluding result of this Section enables one to prove that admissible pro-$p$-groups are isomorphic to decomposition groups; this result can be deduced from Galois theory and the main result of [28]:

(2.7) For each Henselian field $(K, v)$, there is $R \in I(K_{\rm sep}/K)$, such that $\mathcal{G}_R \cong \mathcal{G}_{\widehat{K}}$, $v(R)$ is divisible and finite extensions of $R$ in $K_{\rm sep}$ are inertial.

## 3. **Free pro-$p$-groups and Demushkin groups in the class of Galois groups of maximal $p$-extensions**

The purpose of this Section is to characterize the groups pointed out in its title. Our argument relies on the following two lemmas.

**Lemma 3.1.** *Let $A$ be an abelian torsion $p$-group, $\mu$ a positive integer dividing $p-1$, $\varphi$ an automorphism of $A$ of order $\mu$, and $\varepsilon_\mu$ a primitive $\mu$-th root of unity in the ring $\mathbb{Z}_p$ of $p$-adic integers. Then $\varphi$ and the mapping $\varphi^u \to \varepsilon_\mu^u$, $u = 0, \dots, \mu-1$, induce canonically on $A$ a structure of a $\mathbb{Z}_p$-module. This module decomposes into a direct sum $A = \oplus_{u=0}^{\mu-1} A_u$, where $A_u = \{a_u \in A\colon\ \varphi(a_u) = \varepsilon^u a_u\}$, for each index $u$.*

*Proof.* The scalar multiplication $\mathbb{Z}_p \times A \to A$ is uniquely defined by the group operation in $A$ and the rule $z.a = 0\colon\ a \in A$, $p^k a = 0$, $z \in p^k\mathbb{Z}_p$. For each $n \in \mathbb{N}$, denote by $s_n$ the integer satisfying the conditions $\varepsilon_\mu - s_n \in p^n\mathbb{Z}_p$ and $0 \le s_n \le p^n - 1$. It is easily seen that $\varepsilon_\mu^u a = s_n a$ whenever $a \in A$, $n \in \mathbb{N}$ and $p^n a = 0$. Note also that the element $a_u = \sum_{u'=0}^{\mu-1} \varepsilon_\mu^{(\mu-u)u'} \varphi^{u'}(a)$ lies in $A_u$, for $u = 0, \dots, \mu-1$. Since the matrix $(z_{ij}) = (\varepsilon_\mu^{(1-i)(j-1)})$, $1 \le i, j \le \mu$, is invertible in the ring $M_\mu(\mathbb{Z}_p)$, this implies that the $\mathbb{Z}_p$-submodule of $A$ generated by the elements $a_u$, $u = 0, \dots, \mu-1$, contains $\varphi^{u'-1}(a)$, for $u' = 0, \dots, \mu-1$, which completes the proof of Lemma 3.1. □

**Lemma 3.2.** *Let $E$ be a field with $r(p)_E \in \mathbb{N}$, for some $p \in P(E)$, $p \neq$* char$(E)$*, and let $L$ be an extension of $E$ in $E(p)$ of degree $p$. Assume that $\varepsilon$ is a primitive $p$-th root of unity in $E_{\rm sep}$, $\varphi$ is a generator of $\mathcal{G}(E(\varepsilon)/E)$, and $E_\varepsilon = \{a \in E(\varepsilon)^*\colon\ \varphi(a)a^{-s} \in E(\varepsilon)^{*p}\}$, where $s$ is an integer satisfying the equality $\varepsilon^s = \varphi(\varepsilon)$. Put $N(L/E)_\varepsilon = E_\varepsilon \cap N(L(\varepsilon)/E(\varepsilon))$ and denote by $p^t$ the index of $E(\varepsilon)^{*p}$ in $N(L/E)_\varepsilon$. Then:*

(i) *Each $\lambda \in N(L/E)_\varepsilon$ is presentable as a product $\lambda = N_{E(\varepsilon)}^{L(\varepsilon)}(\tilde{\lambda})\lambda_0^p$, for some $\tilde{\lambda} \in L_\varepsilon$, $\lambda_0 \in E(\varepsilon)^{*p}$;*

(ii) *$r(p)_L = r(p)_E + (p-1)(t-1)$;*

(iii) *$E_\varepsilon \subseteq N(L(\varepsilon)/E(\varepsilon))$ if and only if $r(p)_L = 1 + p(r(p)_E - 1)$.*

*Proof.* Fix a generator $\psi$ of $\mathcal{G}(L/E)$, denote by $\bar{\psi}$ the $E(\varepsilon)$-automorphism of $L(\varepsilon)$ extending $\psi$, set $[E(\varepsilon)\colon E] = m$, and for each $\lambda \in L(\varepsilon)$, let $\rho(\lambda) = \prod_{i=0}^{m-1} \bar{\varphi}^i(\lambda)^{l^i}$, where $\bar{\varphi}$ is the $L$-automorphism of $L(\varepsilon)$ extending $\varphi$, and $l$ is an integer with $0 < l \le p-1$ and $sl \equiv 1 (\text{mod } p)$. It is easily verified that $\rho(a)a^{-m} \in E(\varepsilon)^{*p}$, for each $a \in E_\varepsilon$. Note also that $L(\varepsilon)/E$ is cyclic, whence $N_{E(\varepsilon)}^{L(\varepsilon)}(\bar{\varphi}(u)) = \varphi(N_{E(\varphi)}^{L(\varepsilon)}(u))$, for each $u \in L(\varepsilon)$. This proves Lemma 3.2 (i).

Lemma 3.2 (iii) is implied by Lemma 3.2 (ii), so we turn to the proof of Lemma 3.2 (ii). It is easily obtained from Kummer theory and [39], Theorem 2, that $t = 0$ if and only if $p = 2$, $E$ is a Pythagorean field (i.e. formally real with $E^{*2}$ closed under addition) and $L = E(\sqrt{-1})$. When this holds, it can be deduced from Hilbert's Theorem 90 (cf. [26], Ch. VIII, Sect. 6) that $L^* = K^*L^{*2}$ and $L^{*2} \cap K^* = K^{*2} \cup -1.K^{*2}$. This implies that $r(2)_L = r(2)_E - 1$, as claimed by Lemma 3.2. Henceforth, we assume that $t > 0$. Suppose first that $r(p)_E = 1$. Then it follows from [39], Theorem 2, that $\mathcal{G}(E(p)/E) \cong \mathbb{Z}_p$ unless $p = 2$ and $E$ is Pythagorean with a unique ordering (i.e. with $E^* = E^{*2} \cup -1.E^{*2}$). This, combined with Albert's theorem (cf. [1], Ch. IX, Sect. 6) or [6], Lemma 3.5, proves our assertion. Henceforth, we assume that $r(p)_E \geq 2$. It follows from Kummer theory and Albert's theorem that $E_\varepsilon/E(\varepsilon)^{*p}$ has dimension $r(p)_E$ as an $\mathbb{F}_p$-vector space. More precisely, it is easily verified that there exist $a_1, \dots, a_{r(p)_E} \in E_\varepsilon$, such that the cosets $a_j E(\varepsilon)^{*p}$, $j = 1, \dots, r(p)_E$, form a basis of $E_\varepsilon/E(\varepsilon)^{*p}$ and the following conditions hold:

(3.1) (i) $L(\varepsilon)$ is generated over $E(\varepsilon)$ by a $p$-th root $\xi_1$ of $a_1$; moreover, $a_1$ can be chosen so that $\xi_1 \in L_\varepsilon$;

(ii) There is an index $\bar{t} \geq 2$, such that $a_i \in N(L(\varepsilon)/E(\varepsilon))$, $i = 2, \dots, \bar{t}$, and $a_i \notin N(L(\varepsilon)/E(\varepsilon))$, $i > t$;

(iii) $a_{t+1} = -a_1$, provided that $p = 2$, $-1 \notin E^{*2}$ and $a_1 \notin N(L/E)$.

In view of Lemma 3.2 (i), $L_\varepsilon$ contains elements $\xi_1, \dots, \xi_t \in L_\varepsilon$, such that $\xi_1^p a_1^{-1} \in E(\varepsilon)^{*p}$ and $N_{E(\varepsilon)}^{L(\varepsilon)}(\xi_i) a_i^{-1} \in E(\varepsilon)^{*p}$, for $i = 2, \dots, \bar{t}$. For each index $i \geq 2$, put $\xi_{i,0} = \xi_i$, and $\xi_{i,j} = \bar{\psi}(\xi_{i,(j-1)})\xi_{i,(j-1)}^{-1}$, for $j = 2, \dots, (p-1)$. Using repeatedly Hilbert's Theorem 90 (as in the proof of implication (cc)→(c) of [6], (5.3)), one concludes that $L_\varepsilon/L(\varepsilon)^{*p}$ contains as an $\mathbb{F}_p$-basis the following set $S$ of cosets:

(3.2) (i) If $p > 2$ or $-1 \notin E^{*2}$, then $S$ consists of $\xi_1 L(\varepsilon)^{*p}$, $\xi_{i,j} L(\varepsilon)^{*p}$, $2 \leq i \leq \bar{t}$, $0 \leq j \leq (p-1)$, and $a_u L(\varepsilon)^{*p}$, $u > t$;

(ii) When $p = 2$ and $a_1 \notin N(L/E)$, $S$ is formed by $\xi_1 L(\varepsilon)^{*2}$, $\xi_{i,j} L(\varepsilon)^{*2}$, $2 \leq i \leq \bar{t} - 1$, $0 \leq j \leq 1$, and $a_u L(\varepsilon)^{*2}$, $u \geq \bar{t}$;

(iii) If $p = 2$, $-1 \notin E^{*2}$ and there is $\xi_1' \in L$ of norm $N_E^L(\xi_1') = a_1$, then $S$ equals $\xi_1' L(\varepsilon)^{*2}$, $\xi_{i,j} L(\varepsilon)^{*2}$, $2 \leq i \leq \bar{t}$, $0 \leq j \leq 1$, and $a_u L(\varepsilon)^{*2}$, $u > \bar{t}$.

Note finally that, by [1], Ch. IX, Theorem 6, and Kummer theory, $r(p)_L$ equals the dimension of $L_\varepsilon/L(\varepsilon)^{*p}$ as an $\mathbb{F}_p$-vector space. This implies that the index $\bar{t}$ in (3.1) is equal to $t$ in cases (i) and (iii) of (3.2), and in case (3.2) (ii), $\bar{t} = t + 1$. Therefore, Lemma 3.2 (ii) can be deduced from (3.2). □

**Corollary 3.3.** *Let $E$ be a field with $r(p)_E \in \mathbb{N}$, for some $p \in P(E)$. Then $\mathcal{G}(E(p)/E)$ is a free pro-$p$-group if and only if $r(p)_L = 1 + [L\colon E]$, for every finite extension $L$ of $E$ in $E(p)$.*

*Proof.* This follows from Lemma 3.2 (iii), Galois theory and the characterization of free pro-$p$-groups of finite rank by the indices of their open subgroups (cf. [32], Ch. I, 4.2). □

Assume that $E$ is a field with $r(p)_E \leq \infty$, for some $p \in P(E)$, $p \neq \mathrm{char}(E)$, take $\varepsilon$, $\varphi$, $s$ and $l$ as in Lemma 3.2, and put $m = [E(\varepsilon)\colon E]$. In view of Lemma 3.1, then the action of $\mathcal{G}(E(\varepsilon)/E)$ on $E(\varepsilon)$ canonically induces on $E(\varepsilon)$, $E(\varepsilon)^*$ and $\mathrm{Br}(E(\varepsilon))_p$ structures of modules over the group ring $\mathbb{Z}[\mathcal{G}(E(\varepsilon)/E)]$. Note further that the $\mathbb{Z}_p$-submodules $\mathrm{Br}(E(\varepsilon))_{p,j}$ $j = 0, \dots, m-1$, of $\mathrm{Br}(E(\varepsilon))_p$ are $\mathbb{Z}[\mathcal{G}(E(\varepsilon)/E)]$-submodules too. Denote by $Y$ any of the groups $E(\varepsilon)^*/E(\varepsilon)^{*p}$, ${}_p\mathrm{Br}(E(\varepsilon))$ and $H_p(E(\varepsilon)) = \mathrm{Br}(E(p)(\varepsilon)/E(\varepsilon)) \cap {}_p\mathrm{Br}(E(\varepsilon))$. The preceding observations show that $Y$ can be viewed in a natural manner as a module over the group ring $\mathbb{F}_p[\mathcal{G}(E(\varepsilon)/E)]$, which satisfies the following:

(3.3) The set $Y_j = \{y_j \in Y\colon \ \varphi(y_j) = s^j y_j\}$ is an $\mathbb{F}_p[\mathcal{G}(E(\varepsilon)/E)]$-submodule of $Y$, for $j = 0, 1, \dots, m-1$; the sum of submodules $Y_0, \dots, Y_{m-1}$, is direct and equal to $Y$.

In view of the Merkur'ev-Suslin theorem [29], (16.1), this ensures that

(3.4) ${}_p\mathrm{Br}(E(\varepsilon))$ is generated by the similarity classes of symbol division $E(\varepsilon)$-algebras $A_\varepsilon(E(\varepsilon); a, b)$ of Schur index $p$, where $a$ and $b$ lie in he union of the sets $E_{\varepsilon,j} = \{a_j \in E(\varepsilon)^\ast\colon \ \varphi(a_j)a_j^{-s^j} \in E(\varepsilon)^{\ast p}\}$, $j = 0, 1, \dots, m-1$.

It is easily obtained from Kummer theory and elementary properties of cyclic $E(\varepsilon)$-algebras (cf. [26], Ch. VIII, Sect. 6, and [30], Sect. 15.1, Corollary a) that (3.4) can be supplemented as follows:

(3.5) If $a \in E_{\varepsilon,j'}$ and $b \in E_{\varepsilon,j''}$, then $[A_\varepsilon(E(\varepsilon); a, b)] \in_p \mathrm{Br}(E(\varepsilon))_{\bar{j}}$, where $\bar{j}$ is the remainder of $j' + j'' - 1$ modulo $m$.

Denote for brevity $H_p(E(\varepsilon))_1$ by $H_{p,1}(E)$. Using (3.4) and (3.5) (see also [30], Sect. 15.1, Proposition b, and for more details, [9], Sect. 3), one concludes that $\mathcal{G}(E(p)/E)$ is a free pro-$p$-group if and only if any of the following three equivalent conditions holds:

(3.6) (i) $H_{p,1}(E) = \{0\}$;
(ii) $E_\varepsilon \subseteq N(L(\varepsilon)/E(\varepsilon))$, for each finite extension $L$ of $E$ in $E(p)$;
(iii) $L_\varepsilon \subseteq N(L'(\varepsilon)/L(\varepsilon))$ whenever $L'$ is a finite extension of $E$ in $E(p)$, $L \in I(L'/E)$ and $L$ is a maximal subfield of $L'$.

It is known that the class of Demushkin groups is closed under taking open subgroups (see, e.g., [32], Ch. I, 4.5). Our next result characterizes Demushkin groups among finitely-generated Galois groups of maximal $p$-extensions (for a proof, see [9]); characterizations of Demushkin groups in the class of finitely generated one-relator pro-$p$-groups can be found in [12].

**Proposition 3.4.** *Let $E$ be a field such that $r(p)_E \in \mathbb{N}$, for some $p \in P(E)$, $p \neq \mathrm{char}(E)$, and let $\varepsilon$ be a primitive $p$-th root of unity in $E_{\mathrm{sep}}$. Then the following conditions are equivalent:*
(i) *$\mathcal{G}(E(p)/E)$ is a Demushkin group;*
(ii) *$H_{p,1}(E)$ is of order $p$ and $H_{p,1}(E) \subseteq \mathrm{Br}(L(\varepsilon)/E(\varepsilon))$, provided $L \in I(E(p)/E)$ and $[L\colon E] = p$;*
(iii) *For each $\alpha \in E_\varepsilon \setminus E(\varepsilon)^{\ast p}$ and $\Delta_p \in d(E(\varepsilon))$ with $[\Delta_p] \in H_{p,1}(E)$, $\Delta_p$ is $E(\varepsilon)$-isomorphic to $A_\varepsilon(E(\varepsilon); \alpha, \beta)$, for some $\beta \in E_\varepsilon$);*
(iv) *$r(p)_R = 2 + [R\colon E](r(p)_E - 2)$ in case $R \in I(E(p)/E)$ and $[R\colon E] \in \mathbb{N}$.*

Note that the implication (i)$\to$(iv) in Proposition 3.4 follows from [22], Proposition 5.4, Galois theory and the fact that every Demushkin group $P$ is of cohomological dimension $\mathrm{cd}(P) = 2$ (cf. [32], Ch. I, 4.5).

*Remark* 3.5. Let $P_1$ and $P_2$ be pro-$p$-groups, for a given $p \in \mathbb{P}$, such that $P_j \cong \mathbb{Z}_p^{m_j} \rtimes \Phi_1$, $j = 1, 2$, where $m_j$ is an integer $\geq 0$ and $\Phi_j$ is a free pro-$p$-group with $r(\Phi_j) \geq 2$ or a Demushkin group with $r(\Phi_j) \geq 3$, for each index $j$. It follows from (1.1), Corollary 3.3 and Proposition 3.4 (iii) that if $R_j$ is a closed proper subgroup of $\Phi_j$ and $r(R_j) = 2$, then the index of $R_j$ in $\Phi_j$ is infinite. Hence, by [23], Theorem 2 (ii), $R_j$ is a free pro-$p$-group. This, combined with Corollary 3.3 and Galois cohomology (see [32], Ch. I, 4.1), implies that if $A_j \leq \Phi_j$, $A_j \neq \{0\}$ and $A_j$ is abelian and closed in $\Phi_j$, then $A_j \cong \mathbb{Z}_p$. Since the set of closed normal subgroups of $\Phi_j$ is closed under taking centralizers, and the automorphism group $\mathrm{Aut}(\mathbb{Z}_p)$ is isomorphic to the direct sum $\mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}_p$, it is also clear that $A_j$ is not normal in $\Phi_j$. These observations indicate that if $P_1 \cong P_2$, then $\Phi_1 \cong \Phi_2$ and $m_1 = m_2$.

## 4. **Proofs of Theorems 1.1 and 1.2 in the case of** $v(K) = G(K)$

The main purpose of this Section is to prove Theorems 1.1 and 1.2 in the special case where $v(K) = G(K) \neq pv(K)$. Let $(K, v)$ be a $p$-Henselian field with $\mathrm{char}(\widehat{K}) = p$. First we show that $\widehat{K}$ is perfect, provided that $r(p)_K \in \mathbb{N}$. This result is presented by the following lemma (proved in [31], (2.7), and [13], Proposition 3.1, under heavier assumptions like the one that the group $K^*/K^{*p}$ is finite). This lemma does not require that $v(K) \neq pv(K)$.

**Lemma 4.1.** *Assume that $(K, v)$ is a $p$-Henselian field, such that $\widehat{K}$ is imperfect and* $\mathrm{char}(\widehat{K}) = p$. *Then $r(p)_K = \infty$. Moreover, if* $\mathrm{char}(K) = p$ *or $v(p) \in pv(K)$, then there exists $\Lambda \in I(K(p)/K)$, such that $[\Lambda\colon K] = [\widehat{\Lambda}\colon \widehat{K}] = p$ and $\widehat{\Lambda}$ is purely inseparable over $\widehat{K}$.*

*Proof.* Let $\widetilde{\mathbb{F}}$ be the prime subfield of $\widehat{K}$, $\widetilde{B}$ a basis of the field $\widehat{K}^p = \{\hat{u}^p\colon\ \hat{u} \in \widehat{K}\}$ as a vector space over $\widetilde{\mathbb{F}}$, and $B$ a (full) system of preimages of the elements of $\widetilde{B}$ in $O_v(K)$. The condition on $\widehat{K}$ guarantees that $\widetilde{B}$ is infinite. Suppose first that $\mathrm{char}(K) = p$, put $\rho(K) = \{\alpha^p - \alpha\colon\ \alpha \in K\}$, denote by $\mathbb{F}$ the prime subfield of $K$, and fix a nonzero element $\pi \in M_v(K)$. Clearly, the natural homomorphism of $O_v(K)$ upon $\widehat{K}$ induces an isomorphism $\mathbb{F} \cong \widetilde{\mathbb{F}}$. Note also that $\rho(K)$ is an additive subgroup of $K$, and by the Artin-Schreier theorem (cf. [26], Ch. VIII, Sect. 6), the group $K/\rho(K)$ can be canonically viewed as an $\mathbb{F}$-vector space of dimension $r(p)_K$. It follows from the $p$-Henselian property of $K$ and the Artin-Schreier theorem that, for each $a \in O_v(K)$ with $v(a) = 0$ and a residue class $\hat{a} \notin K^p$, the root field $\Lambda_a$ of the polynomial $X^p - X - \pi^{-p}a$ is a cyclic extension of $K$, such that $[\Lambda_a\colon K] = [\widehat{\Lambda}_a\colon \widehat{K}] = p$ and $\widehat{\Lambda}_a/\widehat{K}$ is purely inseparable. This implies that the cosets $ab\pi^{-p} + \rho(K)$, $b \in B$, are linearly independent over $\mathbb{F}$, which proves Lemma 4.1 in case $\mathrm{char}(K) = p$.

Assume now that $\mathrm{char}(K) = 0$, $\varepsilon$ is a primitive $p$-th root of unity in $K_{\mathrm{sep}}$, and $[K(\varepsilon)\colon K] = m$. Our first objective is to obtain the following reduction:

(4.1) It suffices for the proof of Lemma 4.1 to consider the special case where $v(K)$ is Archimedean, $v(p) \in pv(K)$ and $v$ is Henselian.

It is well-known that $\prod_{j=1}^{p-1}(1 - \varepsilon^j) = p$ and $\prod_{j'=0}^{p-1}(\varepsilon_1 - \varepsilon^{j'}) = \varepsilon - 1$, where $\varepsilon_1 \in K_{\mathrm{sep}}$ is a $p$-th root of $\varepsilon$. As $\mathrm{char}(\widehat{K}) = p$, this implies that $pv'(\varepsilon_1 - 1) = v'(\varepsilon - 1)$ and $(p-1)v'(\varepsilon - 1) = v(p)$, for every valuation $v'$ of $K(\varepsilon_1)$ extending $v$. Since cyclotomic field extensions are abelian and $m \mid (p-1)$ (cf. [26], Ch. VIII, Sect. 3), these results enable one to deduce from Galois theory and Ostrowski's theorem that $K(p) \cap K(\varepsilon_2)$ possesses a subfield $L$, such that $[L\colon K] = p$ and $v(p) \in pv(L)$. Hence, by Lemma 3.2, one may assume for the proof of Lemma 4.1 that $v(p) \in pv(K)$. Replacing $(K, v)$ by $(K_{G(K)}, \hat{v}_{G(K)})$ and applying (2.1) and Proposition 2.1, one sees that our considerations further reduce to the special case where $G(K) = v(K)$. In this case, it is easily deduced from Zorn's lemma that $\mathrm{Is}_v(E)$ has a maximal element $\Omega$ with respect to set-theoretic inclusion. Observing that $\mathrm{char}(K_\Omega) = p$, one obtains from (2.1) that $\widehat{K}$ is perfect, provided that $K_\Omega$ is of the same kind. Thus it turns out that it is sufficient to prove Lemma 4.1 in the special case where $v(K)$ is Archimedean. Using the Grunwald-Wang theorem, one arrives at the conclusion that every cyclic extension $L$ of $K_v$ of degree $p$ is $K$-isomorphic to $\widetilde{L} \otimes_K K_v$, for some $\widetilde{L} \in I(K(p)/K)$ with $[\widetilde{L} \colon K] = p$. In view of Galois theory, the subnormality of proper subgroups of finite $p$-groups, and the $p$-Henselian property of $v$, this implies that $K_v(p)$ is $K$-isomorphic to $K(p) \otimes_K K_v$, whence $\mathcal{G}(K_v(p)/K_v) \cong \mathcal{G}(K(p)/K)$. Therefore, one may assume for the proof of Lemma 4.1 that $K = K_v$. As $v(K) \leq \mathbb{R}$, this ensures that $v$ is Henselian (see, e.g., [26], Ch. XII), which yields (4.1).

It remains for us to prove Lemma 4.1 in the case pointed out by (4.1). For each $a \in O_k$ with $v(a) = 0$ and $\hat{a} \notin \widehat{K}^p$, put $\rho(a) = \prod_{j=0}^{m-1} \varphi^j (1 + (\varepsilon - 1)^p \pi^{-p} a)^{l^j}$, where $\pi$ is an element of $K^*$ of value $v(\pi) = p^{-1} v(p)$. It is easily verified that $\rho(a) \in K_\varepsilon$. Since $m \mid (p-1)$ and $(p-1)v'(\varepsilon - 1) = v(p)$, one also obtains by direct calculations that $v'(\rho(a) - 1) = v'(\varepsilon - 1)$. Similarly, it is proved that the polynomial $h_a(X) = \pi^p (\varepsilon - 1)^{-p} . g_a((\varepsilon - 1)\pi^{-1} X)$, where $g_a(X) = (X+1)^p - \rho(a)$, lies in $O_{v'}(K(\varepsilon))[X]$ and is congruent to $X^p - ma$ modulo $M_{v'}(K(\varepsilon))[X]$. As $v(m^p - m) \geq v(p)$ and $\tilde{a} \notin \widehat{K}$, these calculations show that $h_a$ and $g_a$ are irreducible over $K(\varepsilon)$, whence $\rho(a) \notin K(\varepsilon)^{*p}$. In view of the definition of $B$, they also lead to the following conclusion:

(4.2) The co-sets $\rho(ab)K(\varepsilon)^{*p}$, $b \in B$, are linearly independent over $\mathbb{F}_p$.

Hence, by Albert's theorem, the extension $L'_a$ of $K(\varepsilon)$ in $K_{\mathrm{sep}}$ obtained by adjunction of a $p$-th root of $\rho(a)$, equals $L_a(\varepsilon)$, for some $L_a \in I(K(p)/K)$ with $[L_a \colon K] = p$ and $\hat{a} \notin \widehat{L}_a^{*p}$. Furthermore, it follows from (4.2) that the fields $L_{ab}$, $b \in B$, are pairwise distinct, so the equality $r(p)_K = \infty$ becomes an immediate consequence of Galois theory. Lemma 4.1 is proved. □

*Remark* 4.2. Suppose that $(K, v)$ is a valued field with $\mathrm{char}(K) = p$ and $v(K) \neq pv(K)$, $\rho(K) = \{\alpha^p - \alpha \colon \ \alpha \in K\}$, and $\pi_p$ is an element of $K^*$, such that $v(\pi_p) > 0$ and $v(\pi_p) \notin pv(K)$. Clearly, the co-sets $\pi_p^{-(1+p\nu)} + \rho(K)$, $\nu \in \mathbb{N}$, are linearly independent over the prime subfield of $K$. Therefore, $K/\rho(K)$ is infinite, so it follows from the Artin-Schreier theorem and Galois theory that $r(p)_K = \infty$ and the polynomials $f_n(X) = X^p - X - \pi_p^{-(1+pn)}$, $n \in \mathbb{N}$, are irreducible over $K$. It also turns out that the root field $L_n \in I(K_{\mathrm{sep}}/K)$ of $f_n$ is a totally ramified extension of $K$ in $K(p)$ of degree $p$, for each index $n$, and $L_{n'} \neq L_{n''}$, $n' \neq n''$.

The main result of this Section is contained in the following lemma.

**Lemma 4.3.** *Let $(K, v)$ be a $p$-Henselian field, such that* $\mathrm{char}(K) = 0$, $\mathrm{char}(\widehat{K}) = p$ *and* $v(K) = G(K) \neq pG(K)$. *Then* $r(p)_K \in \mathbb{N}$ *if and only if* $G(K)$ *is cyclic and* $\widehat{K}$ *is finite. When this holds,* $\mathcal{G}(K(p)/K)$ *is a (standardly* *admissible) Demushkin group or a free pro-p-group depending on whether or not $K_{h(v)}$ contains a primitive p-th root of unity.*

*Proof.* Suppose first that $v(E)$ is Archimedean. Using Grunwald-Wang's theorem as in the proof of (4.1), one obtains that $\mathcal{G}(K(p)/K) \cong \mathcal{G}(K_v(p)/K_v)$, which reduces our considerations to the special case where $v$ is Henselian. Then the latter assertion of the lemma and the sufficiency part of the former one follow from (2.6), (1.1) and (1.2). We show that $r(p)_K = \infty$, provided $v(K)$ is noncyclic or $\widehat{K}$ is infinite. Our argument relies on the fact that, in the former case, $pv(K)$ is a dense subgroup of $v(K)$. Fix a primitive $p$-th root of unity $\varepsilon \in K_{\rm sep}$, and take $m$, $\varphi$, $s$ and $l$ as in Lemma 3.2. Consider the sequence $\tilde{\alpha}_n = \prod_{i=0}^{m-1} \varphi^i(1+(\varepsilon-1)\alpha_n)^{l^i}$, $n \in \mathbb{N}$, satisfying the following:

(4.3) (i) If $\widehat{K}$ is infinite and $v(p) \notin pv(K)$, then $\alpha_n$, $n \in \mathbb{N}$, is a system of representatives in $O_v(K)$ of a subset of $\widehat{K}$, which is linearly independent over the prime subfield of $\widehat{K}$;

(ii) If $v(p) \in pv(K)$ and $\widehat{K}$ is infinite, then $\alpha_n = \pi^{-1}\alpha'_n$, for each $n \in \mathbb{N}$, where $\pi \in K$ is chosen so that $0 < v(\pi) \leq p^{-1}v(p)$ and $v(\pi) \notin pv(K)$, and the sequence $\alpha'_n$, $n \in \mathbb{N}$, is defined as $\alpha_n$, $n \in \mathbb{N}$, in case (i);

(iii) When $v(K)$ is noncyclic, $\alpha_n \in K$, $0 < v(\alpha_n) \leq p^{-1}v(p)$ and $v(\alpha_n) \notin pv(K)$, for every index $n$; also, $v(\alpha_n)$, $n \in \mathbb{N}$, are pairwise distinct.

It follows from (4.3) that $\tilde{\alpha}_n \in K_\varepsilon$, $v_{K(\varepsilon)}(\tilde{\alpha}_n) = 0$ and $v_{K(\varepsilon)}(\tilde{\alpha}_n - 1) \notin pv(K(\varepsilon))$, for each $n \in \mathbb{N}$. Furthermore, (4.3) ensures that the co-sets $\tilde{\alpha}_n K(\varepsilon)^{*p}$, $n \in \mathbb{N}$, are linearly independent over $\mathbb{F}_p$. These observations, combined with Albert's theorem and Ostrowski's theorem, prove that $K$ admits infinitely many totally ramified extensions of degree $p$ (in $K(p)$). Hence, by Galois theory, $r(p)_K = \infty$, as claimed.

It remains to be proved that $v(K)$ is Archimedean, provided $r(p)_K \in \mathbb{N}$. The equality $v(K) = G(K)$ means that $v(p) \notin H$, for any $H \in {\rm Is}_v(K)$. This implies that ${\rm Is}_v(K)$ satisfies the conditions of Zorn's lemma, whence it contains a minimal element, say, $\overline{H}$, with respect to inclusion. We prove that $v_{\overline{H}}(K) \neq pv_{\overline{H}}(K)$ by assuming the opposite. As $v_{\overline{H}}(K) = v(K)/\overline{H}$ and $v(K) \neq pv(K)$, this requires that $\overline{H} \neq p\overline{H}$. Observing also that ${\rm char}(K_{\overline{H}}) = p$, one obtains from Proposition 2.1 and Remark 4.2 that ${\rm I}(K_{\overline{H}}(p)/K_{\overline{H}})$ has a subset $\{\widetilde{K}_n \colon\ n \in \mathbb{N}\}$ of totally ramified extensions of $K_{\overline{H}}$ (relative to $\hat{v}_{\overline{H}}$) of degree $p$. By (2.4) (i), the inertial lifts $K_n$ of $\widetilde{K}_n$, $n \in \mathbb{N}$, over $K$ relative to $v_{\overline{H}}$, form an infinite subset of $I(K(p)/K)$. In view of Galois theory, however, our conclusion contradicts the assumption that $r(p)_K \in \mathbb{N}$, so it follows that $\overline{H} = p\overline{H}$ and $v_{\overline{H}}(K) \neq pv_{\overline{H}}(K)$. It remains to be seen that $\overline{H} = \{0\}$. Suppose that $\overline{H} \neq \{0\}$. Then $\hat{v}_{\overline{H}}$ must be nontrivial, which implies that $K_H$ is infinite. Since $v_{\overline{H}}$ is $p$-Henselian, ${\rm char}(K_{\overline{H}}) = p$ and $v_{\overline{H}}(K) \leq \mathbb{R}$, this leads, by the already proved special case of Lemma 4.3, to the conclusion that $r(p)_K = \infty$. The obtained results shows that $\overline{H} = \{0\}$, i.e. $v(K)$ is Archimedean, which completes our proof. □

## 5. $p$-divisible value groups

In this Section we prove Theorem 1.1 (i) in the case where $v(K) = pv(K)$. The corresponding result can be stated as follows:

**Proposition 5.1.** *Let $(K, v)$ be a $p$-Henselian field, such that* $\mathrm{char}(\widehat{K}) = p$ *and $v(K) = pv(K)$. Suppose further that $p \in P(K)$ and $r(p)_K \in \mathbb{N}$. Then $\widehat{K}$ is perfect and $\mathcal{G}(K(p)/K)$ is a free pro-$p$-group.*

Proposition 5.1 generalizes [13], Proposition 3.4, which covers the case where $K$ contains a primitive $p$-th root of unity. Note that the assumption on $r(p)_K$ is essential. Indeed, it follows from [37], Theorem 4.1, and Ostrowski's theorem that there exists a Henselian field $(F, w)$, such that $\mathrm{char}(\widehat{F}) = p$, $\widehat{F}$ is algebraically closed, $F$ contains a primitive $p$-th root of unity, and $\mathrm{Br}(F)_p \neq \{0\}$. Since ${}_p\mathrm{Br}(F) \cong H^2(\mathcal{G}(F(p)/F), \mathbb{F}_p)$ [36], page 265, this means that $\mathcal{G}(F(p)/F)$ is not a free pro-$p$-group (see [33], Ch. I, 4.2).

*Proof of Proposition 5.1.* As noted in the Introduction, it is known that $\mathcal{G}(E(p)/E)$ is a free pro-$p$-group, for every field $E$ of characteristic $p$. Therefore, one may assume for the proof that $\mathrm{char}(K) = 0$, whence the prime subfield of $K$ may be identified with the field $\mathbb{Q}$ of rational numbers. First we show that our proof reduces to the special case where $v(K)$ is Archimedean. Observe that $H = pH$ and $v_H(K) = pv_H(K)$, for each $H \in \mathrm{Is}_v(K)$. This follows from the equality $v(K) = pv(K)$ and the fact that $H$ is a pure subgroup of $v(K)$. Hence, by Ostrowski's theorem, finite extensions of $K$ in $K(p)$ are inertial relative to $G(K)$. It is therefore clear from (2.3) (ii) that $\mathcal{G}(K(p)/K) \cong \mathcal{G}(K_{G(K)}(p)/K_{G(K)})$. Thus the proof of Proposition 5.1 reduces to the special case of $v(K) = G(K)$. This implies that $v(K) \neq H(K)$, where $H(K)$ is defined as in (2.1) (iii), so the preceding observations indicate that it suffices for our proof to consider the special case in which $v(K)$ is Archimedean. Applying now the Grunwald-Wang theorem (repeatedly, as in the proof of Lemma 4.3), one obtains that $\mathcal{G}(K(p)/K) \cong \mathcal{G}(K_{h(v)}(p)/K_{h(v)})$, which allows us to assume further that $v$ is Henselian and $v(K) \leq \mathbb{R}$.

For the rest of the proof, fix $\varepsilon$, $\varphi$, $s$ and $K_\varepsilon$ as in Lemma 3.2, take $m$ and $l$ as in its proof, and put $v' = v_{K(\varepsilon)}$. The following statement is easily deduced from Albert's theorem, (2.6) and the $p$-Henselian property of $v$:

(5.1) An element $\theta \in K_\varepsilon$ lies in $K(\varepsilon)^{*p}$ if and only if $\theta \in K(\varepsilon)_{v'}^{*p}$. In particular, this holds when $v'(\theta - 1) > r$ and $r \in v(K)$ is sufficiently large.

Since $\widehat{K}$ is perfect, $v(K)$ is Archimedean and $v(K) = pv(K)$, one deduces the following statement from the density of $K(\varepsilon)$ in $K(\varepsilon)_{v'}$:

(5.2) For each $\alpha \in K_\varepsilon$, there exist elements $\alpha_1 \in K_\varepsilon$ and $\tilde{\alpha} \in K(\varepsilon)^*$, such that $\alpha_1 \tilde{\alpha}^p = \alpha$ and $v'(\alpha_1 - 1) > 0$.

Our objective is to specify (5.2) as follows:

(5.3) (i) For each $\alpha \in K_\varepsilon \setminus K(\varepsilon)^{*p}$, there exists a sequence $\alpha_n \in K_\varepsilon$, $n \in \mathbb{N}$, such that $\alpha_n \alpha^{-1} \in K(\varepsilon)^p$ and $v_1(\alpha_n - 1) > v(p) - n^{-1}$.

(ii) $K_\varepsilon \subseteq N(L(\varepsilon)/K(\varepsilon))$, for every extension $L$ of $K$ in $K(p)$ of degree $p$.

First we show that (5.3) implies $\mathcal{G}(K(p)/K)$ is a free pro-$p$-group. In view of Corollary 3.3, it is sufficient to establish that $r(p)_M = 1 + p^k(r(p) - 1)$ whenever $k \in \mathbb{N}$, $M \in I(K(p)/K)$ and $[M\colon K] = p^k$. Given such $k$ and $M$, there exists $M_1 \in I(M/K)$ with $[M_1\colon K] = p$. Using the fact that $M_1(p) = K(p)$, applying Lemma 3.2 to $M_1/K$, and (5.3) (i) to $M_\varepsilon$ and $v_M$, and proceeding by induction on $k$, one obtains that $r(p)_M = 1 + p^k(r(p)_K - 1)$, as required. To prove that (5.3) (i)→(5.3) (ii) we need the following fact:

(5.4) An element $z \in K(\varepsilon)$ lies in $K(\varepsilon)^{*p}_{v'}$ whenever $v'(z-1) > pv'(\varepsilon - 1)$.

Statement (5.4) is implied by (2.2), applied to the polynomial $\tilde{h}(X) = h((\varepsilon - 1)^{-1}X)$, where $h(X) = (X+1)^p - z$. Fix an element $\delta \in v(K)$, $\delta > 0$, and consider the polynomials $f_\delta(X) = X^p - 1 - (\varepsilon-1)^p\pi_\delta^{-p}t_\delta$, $h_\delta(X) = f_\delta(X+1)$, and $\tilde{h}_\delta(X) = h_\delta(\pi_\delta(\varepsilon-1)^{-1}X)$, where $\pi_\delta \in K(\varepsilon)^*$, $t_\delta \in K_\varepsilon \in \nabla_0(K(\varepsilon))$ and $0 < v'(\pi_\delta) < (1/p)v'(\varepsilon - 1) + \delta/p$. Clearly, $f_\delta$, $h_\delta$ and $\tilde{h}_\delta$ share a common root field $Y_\delta$ over $K(\varepsilon)$, which equals $\widetilde{Y}_\delta K(\varepsilon)$, for some $\widetilde{Y}_\delta \in I(K(p)/K)$ with $[\widetilde{Y}\colon K] = p$. In addition, it is verified by direct calculations that if $\tau_\delta \in K_{\rm sep}$ is a zero of $\tilde{h}$, then $v'(\tilde{h}'(\tau_\delta)) = v'(\pi_\delta^{p-1})$. This, combined with (2.2), (5.1) and (5.4), shows that $N(Y_\delta/K(\varepsilon))$ includes the set $K(\varepsilon) \cap \nabla_{\delta'}(K(\varepsilon))$, where $\delta' = (2p-2)p^{-1}(v'(\varepsilon - 1) + \delta)$. In view of Albert's theorem, the obtained result, applied to any sufficiently small $\delta$, yields (5.3) (i)→(5.3) (ii).

It remains for us to prove (5.3) (i). First we consider the special case in which $\widehat{K}$ contains more than $1 + \sum_{j=0}^{m-1} l^j :\ = \bar{l}$ elements. Fix a sequence $\hat{\alpha}_\nu$, $\nu = 1, \dots \bar{l}$, of pairwise distinct elements of $\widehat{K}^*$, and let $\alpha_\nu$ be a preimage of $\hat{\alpha}_\nu$ in $O_v(K)$, for each index $\nu$. Assume that (5.3) (i) is false, i.e. there exists $d \in K_\varepsilon$, for which the supremum $c(d)$ of values $v'(d'-1)$, $d' \in dK(\varepsilon)^{*p}$, is less than $v(p)$. Take $d$ so that $c(d)$ is maximal with respect to this property, and put $\bar{\delta} = p^{-1-\bar{l}}(v(p) - c(d))$, and take $d' \in K_\varepsilon$ so that $v'(d'-1) > c(d) - \bar{\delta}$. Denote by $p_{d'}$ the polynomial $p_{d'}(X) = \prod_{i=0}^{m-1}(1 + \varphi^{s^i}(\pi')X)^{l^i}$, where $\pi' = d' - 1$, and put $p_{d'}(X) = 1 + \sum_{\nu=1}^{\bar{l}} a_\nu X^\nu$, $s_{d'} = \{a_\nu\colon\ 1 \le \nu \le \bar{l}, v'(a_\nu) < v(p)\}$. It is easily verified that $f(\lambda) \in K_\varepsilon$, for every $\lambda \in M_v(K)$. Now fix an element $\pi \in M_v(K)$ so that $c(d) < v(\pi'\pi^p)$ and $v(\pi^p) < \bar{\delta}$. It follows from the choice of $d$ and $\pi$ that there exist $b_1, \dots, b_{\bar{l}} \in K(\varepsilon)$ satisfying the following conditions, for every index $\nu$:

(5.5) $b_\nu f((\alpha_\nu\pi)^p)^{-1} \in K(\varepsilon)^{*p}$ and $v'(b_\nu - 1) \ge v(p) - \bar{\delta}$.

More precisely, one can find elements $\tilde{b}_1, \dots, \tilde{b}_{\bar{l}} \in \nabla_0(K(\varepsilon))$ so that $\tilde{b}_\nu^p = b_\nu f((\alpha_\nu\pi)^p)^{-1}$ and $b_\nu$ satisfies (5.5), for $\nu = 1, \dots, \bar{l}$. This means that $K(\varepsilon)$ contains elements $\pi_1, \dots, \pi_{\bar{l}}$, such that $v'(f((\alpha_\nu\pi)^p) - 1 - \pi_\nu^p) \ge v(p) - \bar{\delta}$, $\nu = 1, \dots, \bar{l}$. As $f((\alpha_\nu\pi)^p) - 1 = \sum_{\mu=1}^{\bar{l}} \alpha_\nu^{p\mu}(\pi^p a_\mu)^\mu$, for each index $\nu$, the obtained result and the choice of the sequence $a_\nu$, $\nu = 1, \dots, \bar{l}$, enables one to deduce from basic linear algebra that there exist $\tilde{\pi}_1, \dots, \tilde{\pi}_{\bar{l}} \in K(\varepsilon)$, for which $v'(a_\mu\pi^{p\mu} - \tilde{\pi}_\mu^p) \ge v(p) - \bar{\delta}$, $\mu = 1, \dots, \bar{l}$. Thus it turns out that $v'(a_\mu - (\tilde{\pi}_\mu.\pi^{-\mu})^p) \ge v(p) - \bar{\delta} - p\mu v(\pi)$, for every index $\mu$. Hence, there exists $\tilde{\pi} \in K(\varepsilon)$, such that $v'(f(1) - 1 - \tilde{\pi}^p) = v'(-1 + f(1)(1+\tilde{\pi})^{-p}) \ge v(p) - \bar{\delta} - p\bar{l}v(\pi)$. Moreover, it follows from the choice of $\pi$ that $v(p) - \bar{\delta} - p\bar{l}v(\pi) > c(d)$. Since, however, $f(1)d^{-m} \in K(\varepsilon)^{*p}$, the assumption on $c(d)$ and our calculations require that $c(d) \geq v(p) - \bar{\delta} - p\bar{l}v(\pi)$. The obtained contradiction proves (5.3) (i) when $\widehat{K}$ contains more than $\bar{l}$ elements.

Suppose finally that $\widehat{K}$ is of order $\leq \bar{l}$. Then $K$ has an inertial extension $K_n$ in $K(p)$ of degree $p^n$, for each $n \in \mathbb{N}$. As $\widehat{K}$ is perfect and $v(K) = pv(K)$, $K^* = K^{*p^n}\nabla_0(K)$, which implies $N(K_n/K) = K^*$. When $n$ is sufficiently large, $\widehat{K}_n$ contains more than $\bar{l}$ elements, so one can apply (5.3) (i) to $K_n(\varepsilon)$ and the prolongation of $v_{K_n}$ on $K_n(\varepsilon)$. Since $\mathrm{char}(\widehat{K}) = p$, $K$ is a nonreal field, by [25], Theorem 3.16, so it follows from Galois theory and [39], Theorem 2, that $G(K(p)/K)$ is a torsion-free group. In view of Galois cohomology (see [34] and [33], Ch. I, 4.2), these observations show that (5.3) (i) holds in general, which completes the proof of Proposition 5.1.

**Corollary 5.2.** *Let $(K, v)$ be a $p$-Henselian field, for a given $p \in \mathbb{P}$, and suppose that $v(K) = pv(K)$, $\mathcal{G}(K(p)/K)$ is a Demushkin group and $r(p)_K \geq 3$. Then $p \neq \mathrm{char}(\widehat{K})$.*

*Proof.* As $\mathrm{cd}(\mathcal{G}(K(p)/K)) = 2$, $\mathcal{G}(K(p)/K)$ is not a free pro-$p$-group (cf. [33], Ch. I, 4.2 and 4.5), our conclusion follows from Proposition 5.1. □

*Remark* 5.3. Let $(K, v)$ be a $p$-Henselian field, for some $p \in \mathbb{P}$, and $V(K)$ the set of valuation subrings of $K$ included in $O_v(K)$ and corresponding to $p$-Henselian valuations of $K$. Then it can be deduced from Zorn's lemma that $K$ has a valuation $w$, such that $O_w(K)$ is a minimal element of $V(K)$ with respect to inclusion. Hence, by Proposition 2.1, the residue field $\widetilde{K}_{[w]}$ of $(K, w)$ does not possess $p$-Henselian valuations. Note also that, in the setting of Corollary 5.2, $\mathcal{G}(K(p)/K) \cong \mathcal{G}(\widetilde{K}_{[w]}(p)/\widetilde{K}_{[w]})$.

Theorem 1.2 and [37], Proposition 2.2 and Theorem 3.1, ensure that if $(K, v)$ is $p$-Henselian with $G(K) \neq pG(K)$, $\mathrm{char}(\widehat{K}) = p$ and $r(p)_K \in \mathbb{N}$, then finite extensions of $K$ in $K(p)$ are defectless. As shown in [4], Sect. 6, this is not necessarily true without the assumption on $r(p)_K$ even when $\mathcal{G}(K(p)/K)$ is a Demushkin group. The proof relies on a lemma, which is essentially equivalent to the concluding result of this Section.

**Proposition 5.4.** *In the setting of Proposition 5.1, suppose that $K$ contains a primitive $p$-th root of unity $\varepsilon$, $v(K) \leq \mathbb{R}$, $F$ is an extension of $K$ in $K(p)$ of degree $p$, and $\psi$ is a generator of $\mathcal{G}(F/K)$. Then there exist $\lambda_n \in F$, $n \in \mathbb{N}$, such that $0 < v_F(\lambda_n) < v_L(\psi(\lambda_n) - \lambda_n) < 1/n$, for each index $n$.*

*Proof.* It is clear from the $p$-Henselity of $v$ that if $F/K$ is inertial, then $F/K$ has a primitive element $\xi$, such that $v(\xi) = v(\psi(\xi) - \xi) = 0$. Since $\widehat{K}$ is perfect and $v(K) = pv(K)$, this allows us to assume further that $F/K$ is immediate. Then our assertion is deduced by the method of proving [31], (2.7), and [9], (3.1) (see also [13], Lemma 3.3). □

## 6. $p$-Henselian valuations with $p$-indivisible value groups

The purpose of this Section is to complete the proofs of Theorems 1.1 and 1.2. As a major step in this direction, we prove the following lemma.

**Lemma 6.1.** *Let $(K,v)$ be a $p$-Henselian field with* $\mathrm{char}(\widehat{K}) \neq p$ *and* $v(K) \neq pv(K)$, *for a given $p \in \mathbb{P}$, and let $\varepsilon \in K_{\mathrm{sep}}$ be a primitive $p$-th root of unity. Then:*

(i) $\mathcal{G}(K(p)/K) \cong \mathcal{G}(\widehat{K}(p)/\widehat{K})$, *provided that* $\varepsilon \notin K_{h(v)}$;

(ii) $\mathcal{G}(K(p)/K) \cong \mathcal{G}(K_{\Delta(v)}(p)/K_{\Delta(v)})$, *if* $\varepsilon \in K_{h(v)}$ *and* $v(K) \neq \Delta(v)$;

(iii) *If* $\varepsilon \in K_{h(v)}$, *then* $\mathcal{G}(K(p)/K) \cong \mathbb{Z}_p^{\tau(p)} \rtimes \mathcal{G}(\widehat{K}(p)/\widehat{K})$, *where $\tau(p)$ is the dimension of $\Delta(v)/p\Delta(v)$ as an $\mathbb{F}_p$-vector space and $\mathbb{Z}_p^{\tau(p)}$ is a topological group product of isomorphic copies of $\mathbb{Z}_p$, indexed by a set of cardinality $\tau(p)$; in particular, if $\Delta(v) = p\Delta(v)$, then $\mathcal{G}(K(p)/K) \cong \mathcal{G}(\widehat{K}(p)/\widehat{K})$.*

*Proof.* Suppose that $[K(\varepsilon)\colon K] = m$, take $\sigma$ as in (2.5) and $\varphi$, $s$, $l$ as in Lemma 3.2, and denote by $U$ the compositum of the inertial extensions of $K$ in $K(p)$ relative to $v$. As $(K_{h(v)}, \sigma)/(K, v_{G(K)})$ is immediate, it follows from the $p$-Henselian property of $v$ that $K_{h(v)} \cap K(p) = K$. At the same time, by (2.5), $U.K_{h(v)}$ equals the compositum of the inertial extensions of $K_{h(v)}$ in $K_{h(v)}(p)$ relative to $\sigma$. It is therefore clear from [5], Lemma 1.1 (a), that if $\varepsilon \notin K_{h(v)}$, then $K_{h(v)}(p) = U.K_{h(v)} = K(p)K_{h(v)}$ and $\mathcal{G}(K(p)/K) \cong \mathcal{G}(K_{h(v)}(p)/K_{h(v)}) \cong \mathcal{G}(\widehat{K}(p)/\widehat{K})$. Thus Lemma 6.1 (i) is proved.

In the rest of the proof, we assume that $\varepsilon \in K_{h(v)}$. Suppose first that $K(\varepsilon)$ embeds in $K_v$ over $K$. Fix a prolongation $v'$ of $v$ on $K(\varepsilon)$, and put $v_j = v' \circ \varphi^{j-1}$, for $j = 1, \dots, m$. Then the valuations $v_1, \dots, v_m$ are independent, so it follows from the Approximation Theorem (cf. [2], Ch. VI, Sect. 7.2) that, for each $\gamma \in v(K) \setminus pv(K)$, there exists $\alpha_\gamma \in K(\varepsilon)$ of values $v_1(\alpha_\gamma) = \gamma$ and $v_j(\alpha_\gamma) = 0$, $1 < j \leq m$. Put $\tilde{\alpha}_\gamma = \prod_{i=0}^{m-1} \varphi^i(\alpha_\gamma)^{l^i}$ and denote by $\widetilde{K}_{\tilde{\alpha}}$ the extension of $K(\varepsilon)$ generated by the $p$-th roots of $\tilde{\alpha}$ in $K_{\mathrm{sep}}$. It is easily verified that $\tilde{\alpha}_\gamma \in K_\varepsilon$ and $v_1(\tilde{\alpha}_\gamma) = \gamma$. Hence, by applying to $\widetilde{K}_{\tilde{\alpha}}$ Ostrowski's theorem and Albert's theorem, one obtains the following result:

(6.1) There exists $K_\gamma \in I(K(p)/K)$ with $[K_\gamma\colon K] = p$ and $\gamma \in pv(K_\gamma)$.

As $\mathrm{char}(\widehat{K}) \neq p$, it is clear from (2.4), (6.1) and Ostrowski's theorem that every extension of $K_{h(v)}$ in $K_{h(v)}(p)$ of degree $p$ is included in $K(p)K_{h(v)}$. Proceeding by induction on $n$, using (6.1), and arguing as in the proof of (2.4), one proves that $K(p)K_{h(v)}$ includes every extension of $K_{h(v)}$ in $K_{h(v)}(p)$ of degree $p^n$. Thus the equality $K_{h(v)}(p) = K_{h(v)}K(p)$ becomes obvious as well as the fact that $\mathcal{G}(K_{h(v)}(p)/K_{h(v)}) \cong \mathcal{G}(K(p)/K)$. Note further that, by (2.5), $U$ does not admit inertial proper extensions in $K_{h(v)}(p)$ and there are canonical isomorphisms $\mathcal{G}(UK_{h(v)}/K_{h(v)}) \cong \mathcal{G}(U/K) \cong \mathcal{G}(\widehat{K}(p)/\widehat{K})$. Using the fact that $\mathrm{char}(\widehat{K}) \neq p$, one also obtains that $\nabla_0(K_{h(v)}) \subseteq K_{h(v)}^{*p^n}$, for every $n \in \mathbb{N}$. As $\varepsilon \in K_{h(v)}$ and $(K_{h(v)}, \sigma)/(K, v)$ is immediate, one also sees that $\widehat{U}^* = \widehat{U}^{*p^n}$, $n \in \mathbb{N}$. These observations indicate that $[(K_\gamma UK_{h(v)})\colon UK_{h(v)}] = p$ and the field $U_\gamma = K_\gamma UK_{h(v)}$ depends only on the subgroup of $v(K)/pv(K)$ generated by the coset of $\gamma$. Fix a minimal system of generators $V_p$ of $v(K)/pv(K)$ and a full system $W_p$ of representatives of the elements of $V_p$ in $v(K)$. The preceding observations show that every extension of $UK_{h(v)}$ in $K_{h(v)}(p)$ of degree $p$ is included in the compositum of the fields $U_\gamma$, $\gamma \in W_p$. Note further that, for each $\gamma \in W_p$, $U_\gamma$ is generated over $UK_{h(v)}$ by a $p$-th root of an element $u_\gamma \in UK_{h(v)}$ of value $\gamma$. Since $\mathrm{char}(\widehat{K}) \neq p$ and $\varepsilon \in K_{h(v)}$, it also follows that $UK_{h(v)}$ contains a primitive $p^n$-th root of unity, for each $n \in \mathbb{N}$. In view of Kummer theory, this leads to the conclusion that there exists an abelian extension $Z$ of $UK_{h(v)}$ in $K_{h(v)}(p)$ with $\sigma(Z) = p\sigma(Z)$. Since $Z$ does not admit inertial proper extensions in $K_{h(v)}(p)$, the obtained result, the inequality $\mathrm{char}(\widehat{K}) \neq p$ and Ostrowski's theorem imply that $Z = K_{h(v)}(p)$ and so prove the following:

(6.2) $K_{h(v)}(p)$ is abelian over $U.K_{h(v)}$ with $\mathcal{G}(K_{h(v)}(p)/UK_{h(v)}) \cong \mathbb{Z}_p^{\tau(p)}$.

Note further that the set $\Theta(K_{h(v)}) = \{\Theta \in \mathrm{I}(K_{h(v)}(p)/K_{h(v)})\colon\ UK_{h(v)} \cap \Theta = K_{h(v)}\}$, partially ordered by inclusion, satisfies the conditions of Zorn's lemma, whence it possesses a maximal element $T$. In view of (6.1), $\sigma(T) = p\sigma(T)$, so it follows from Ostrowski's theorem and the inequality $\mathrm{char}(\widehat{K}) \neq p$ that $UT = K_{h(v)}(p)$. Hence, by Galois theory and the equality $UK_{h(v)} \cap T = K_{h(v)}$, $\mathcal{G}(K_{h(v)}(p)/K_{h(v)}) \cong \mathcal{G}(K_{h(v)}(p)/UK_{h(v)}) \rtimes \mathcal{G}(UK_{h(v)}/K_{h(v)})$. This, combined with (6.2) and the isomorphism $\mathcal{G}(UK_{h(v)}/K_{h(v)}) \cong \mathcal{G}(\widehat{K}(p)/\widehat{K})$, proves the assertion of Lemma 6.1 (ii) in case $\Delta(v) = v(K)$.

Assume finally that $\varepsilon \in K_{h(v)}$ and $\Delta(v) \neq v(K)$, put $\delta = \hat{v}_{\Delta(v)}$, and denote for brevity by $\widetilde{K}$ the Henselization of $K_{\Delta(v)}$ relative to $\delta_{G(K)}$. It is clear from the definition of $\Delta(v)$ that $\varepsilon \notin K_{h(v_{\Delta(v)})}$. In view of (2.5) with its proof, and of [5], Lemma 1.1 (a), this ensures that $K_{h(v_{\Delta(v)})}(p) = K(p).K_{h(v_{\Delta(v)})}$ and $\mathcal{G}(K(p)/K) \cong \mathcal{G}(K_{\Delta(v)}(p)/K_{\Delta(v)})$. At the same time, it follows from the definition of $\Delta(v)$ that each Henselization of $K_{\Delta(v)}$ relative to $\hat{v}_{\Delta(v)}$ contains a primitive $p$-th root of unity. Hence, by Proposition 2.2, $\widetilde{K}$ contains such a root as well. Note also that, by (2.1) (i), $\widehat{K}$ is isomorphic to the residue field of $(K_{\Delta(v)}, \hat{v}_{\Delta(v)})$. These observations, combined with (6.2), indicate that $\widetilde{K}(p) = K_{\Delta(v)}(p).\widetilde{K}$ and $\mathcal{G}(\widetilde{K}(p)/\widetilde{K}) \cong \mathcal{G}(K_{\Delta(v)}(p)/K_{\Delta(v)}) \cong \mathbb{Z}_p^{\tau(p)} \times \mathcal{G}(\widehat{K}(p)/\widehat{K})$, which completes the proof of Lemma 6.1. □

Lemma 6.1, Proposition 2.2 and our next lemma, enable one to deduce Theorems 1.1 and 1.2 from Lemma 4.3 and Proposition 5.1.

**Lemma 6.2.** *Let $(K, v)$ be a $p$-Henselian field with* $\mathrm{char}(K) = 0$, $\mathrm{char}(\widehat{K}) = p$, *$v(K) \neq pv(K)$ and $v(K) \neq G(K)$. Take $r(p)_K$, $\varepsilon$, $K_{h(v)}$ and $G(K)$ as in Theorems 1.1 and 1.2, and put $r(p) = r(p)_K$, $r(p)' = r(p)_{K_{G(K)}}$. Then:*

(i) *$\mathcal{G}(K(p)/K) \cong \mathcal{G}(K_{G(K)}(p)/K_{G(K)})$, provided that $\varepsilon \notin K_{h(v)}$;*

(ii) *If $\varepsilon \in K_{h(v)}$ and $\Delta(v)$ is defined as in Theorems 1.1 and 1.2, then $r(p) \in \mathbb{N}$ if and only if $r(p)' \in \mathbb{N}$ and $\Delta(v)/p\Delta(v)$ is a finite group; when this holds, $\Delta(v)/p\Delta(v)$ is of order $p^{r(p)-r(p)'}$;*

(iii) *When $r(p)' \in \mathbb{N}$ and $G(K) = pG(K)$, $\mathcal{G}(K_{G(K)}(p)/K_{G(K)})$ is a free pro-$p$-group.*

*Proof.* Proposition 2.1 and our assumptions show that $v_{G(K)}$ is $p$-Henselian and $\mathrm{char}(K_{G(K)}) = 0$. In addition, it is not difficult to see that $\Delta(v)/G(K) = \Delta(v_{G(K)})$. This, combined with Lemma 6.1, proves Lemma 6.2 (i) and (ii). Since, by Proposition 2.1, $\hat{v}_{G(K)}$ is $p$-Henselian, Lemma 6.2 (iii) is proved by applying Proposition 5.1 to $(K_{G(K)}, \hat{v}_{G(K)})$. □

*Remark* 6.3. Let $(K, v)$ be a $p$-Henselian field with $\mathrm{char}(\widehat{K}) = p$, $r(p)_K \in \mathbb{N}$ and $\mathrm{cd}(\mathcal{G}(K(p)/K) \geq 2$. Then (6.1), Lemma 6.1 and the proof of Lemma 4.3 imply the existence of a $p$-Henselian field $(\Lambda, z)$, such that $\mathcal{G}(\Lambda(p)/\Lambda) \cong \mathcal{G}(K(p)/K)$, $\widehat{\Lambda} \cong \widehat{K}$, $z(\Lambda) = \Delta(v)$, and $\Lambda$ contains a primitive $p$-th root of unity. More precisely, one may put $\Lambda = K_{h(v)}$ or take as $\Lambda$ the Henselization of $K_{\Delta(v)}$ relative to $\hat{v}_{\Delta(v)}$, depending on whether or not $\Delta(v) = v(K)$. In view of [13], Theorems 3.7 and 3.8, this enables one to describe the isomorphism classes of $\mathcal{G}(L(p)/L)$ when $(L, \lambda)$ runs across the class of $p$-Henselian fields singled out by Theorems 1.1 and 1.2.

Our next result extends the scope of [38], Lemma 7, as follows:

**Corollary 6.4.** *For a pro-p-group $P$ of rank* 2*, the following conditions are equivalent:*

(i) *$P$ is a free pro-p-group or a Demushkin group;*

(ii) *There exists a p-Henselian field $(K, v)$ with* $\mathrm{char}(\widehat{K}) = p$ *and* $\mathcal{G}(K(p)/K) \cong P$.

*Proof.* Suppose first that $P$ satisfies (ii). Then, by Remark 6.3, $K$ can be chosen so as to contain a primitive $p$-th root of unity. Hence, by [38], Lemma 7, $P$ satisfies (i) in case $p > 2$, so we assume further that $p = 2$ and $P$ is not a free pro-2-group. In view of Galois cohomology, this means that $\mathrm{Br}(K)_2 \neq \{0\}$, and by Proposition 3.4, it suffices to show that, for each quadratic extension $L/K$, $N(L/K)$ is of index 2 in $K^*$. As $r(P) = 2$ and $K^{*2} \subseteq N(L/K)$, this amounts to proving that $N(L/K)$ contains an element $a_L \in K^* \setminus K^{*2}$. When $\sqrt{-1} \in K$, the assertion follows from Kummer theory. Assume now that $-1 \notin K^{*2}$ and $M = K(\sqrt{-1})$. Observing that, by [25], Theorem 3.16, and the equality $\mathrm{char}(\widehat{K}) = 2$, $K$ is nonreal, one obtains from [39], Theorem 2, and Galois theory that $\mathcal{G}(K(p)/K)$ is torsion-free. Hence, by Galois cohomology [33], $\mathcal{G}(K(p)/M)$ is not a free pro-2-group, so our argument proves that $\mathcal{G}(K(2)/M)$ is Demushkin. It is therefore clear from [32], Ch. I, 4.5, that $\mathcal{G}(K(2)/K)$ is also a Demushkin group, so (ii)→(i).

We prove that (i)→(ii). In view of (1.1) and (1.2), applied to $F = \mathbb{Q}_p$, $p > 2$, one may consider only the case where $P$ is a Demushkin group. Let $\omega$ be the canonical discrete valuation of $\mathbb{Q}_p$, $I_p$ the compositum of the inertial extensions of $\mathbb{Q}_p$ in $\mathbb{Q}_p(p)$ relative to $\omega$, $\Gamma'_p$ the extension of $I_p$ generated by the primitive roots of unity in $\mathbb{Q}_{p,\mathrm{sep}}$ of $p$-primary degrees, and $\Gamma_p$ the $\mathbb{Z}_p$-extension of $I_p$ in $\Gamma'_p$. Clearly, $\Gamma'_p/I_p$ is abelian, and it follows from (1.1) and Galois theory that $r(p)_{I_p} = \infty$. Note also that $\omega_{I_p}$ is discrete and finite extensions of $I_p$ in $\Gamma'_p$ are totally ramified relative to $\omega_{I_p}$. Fix a field $R \in I(\Gamma'_p/I_p)$ so that $\mathcal{G}(\Gamma'_p/R)$ is a procyclic pro-$p$-group and put $\Delta_R = \{R' \in I(\mathbb{Q}_{p,\mathrm{sep}}/R)\colon\ R' \cap \Gamma'_p = R\}$. It is clear from the definition of $R$ that it contains a primitive $p$-th root of unity $\varepsilon_p$, and it follows from Galois theory that $r(p)_R = \infty$ and $\mathcal{G}(\Gamma'_p/R) \cong \mathcal{G}(\Gamma'_p R'/R')$, for each $R' \in \Delta_R$. Since $R$ is nonreal, this enables one to deduce from Zorn's lemma, Galois theory and [39], Theorem 2, that there exists $R_p \in \Delta_R$, such that $\mathcal{G}(\mathbb{Q}_{p,\mathrm{sep}}/R_p) \cong \mathbb{Z}_p$. As $r(p)_R = \infty$, this implies that $R_p$ contains as a subfield an infinite extension of $I_p(\varepsilon)$. Hence, by the noted properties of $\omega_{I_p}$, $\mathbb{Q}_{p,\mathrm{sep}}/R_p$ is immediate relative to $\omega_{R_p}$. Let now $\omega(R_p) = H$ and $K$ be a Laurent formal power series field in one indeterminate over $R_p$. It is easy to see that then $K$ has a Henselian valuation $v$ extending $\omega_{R_p}$, such that $H \in \mathrm{Is}_v(K)$, $v(K)/H \cong \mathbb{Z}$ and $K_H \cong R_p$. This, combined with Lemma 6.1 and the fact that $\varepsilon_p \in R_p$, shows that $\mathcal{G}(K(p)/K)$ is a Demushkin group and $r(p)_K = 2$. Observing finally that $R$ can be chosen so that $\mathcal{G}(K(p)/K) \cong P$ (cf. [24]), one obtains that (i)→(ii), which completes our proof. □

The method of proving Theorems 1.1 and 1.2 has the following application to the study of ramification properties of $p$-extensions of $p$-Henselian fields.

**Corollary 6.5.** *Let $(K, v)$ be a $p$-Henselian field such that $\mathrm{char}(\widehat{K}) = p$ and $v(K) \neq pv(K)$. Then $K$ has no totally ramified extension in $K(p)$ of degree $p$ if and only if $\mathrm{char}(K) = 0$ and one of the following conditions holds:*
(i) *$G(K) = pG(K)$ and $K_{h(v)}$ contains no primitive $p$-th roots of unity;*
(ii) *$K_{h(v)}$ contains a primitive $p$-th root of unity and $\Delta(v) = p\Delta(v)$.*

*Proof.* In view of Remark 4.2, one may consider only the case of $\mathrm{char}(K) = 0$. Statement (4.3) and the proof of Lemma 4.3 indicate that if $v(K) = G(K)$, then $K$ possesses infinitely many totally ramified extensions in $K(p)$ of degree $p$. By (6.1), the existence of a totally ramified cyclic extension of $K$ of degree $p$ is also guaranteed when $v(K) = \Delta(v)$. Note further that, for each $H \in \mathrm{Is}_v(K)$, an inertial extension $L$ of $K$ in $K(p)$ relative to $v_H$ is totally ramified relative to $v$ if and only if $L_H/K_H$ is totally ramified relative to $\hat{v}_H$. Since $v_H$ is $p$-Henselian and, by the proof of Lemma 6.1, finite extensions of $K$ in $K(p)$ are inertial relative to $v_H$, provided that $H$ equals $\Delta(v)$ or $G(K)$ depending on whether or not $K_{h(v)}$ contains a primitive $p$-th root of unity, these observations imply together with (2.4) the necessity of conditions (i) and (ii) of Corollary 6.5. They also show that, for the proof of their sufficiency, it remains to be seen that, in case $H = pH$, finite extensions of $K_H$ in $K_H(p)$ are inertial relative to $\hat{v}_H$. As $\mathrm{char}(K_H) = 0$, this follows at once from Ostrowski's theorem, so Corollary 6.5 is proved. □

The concluding result of this Section shows that each standardly admissible pro-$p$-group $P$, where $p > 2$, is isomorphic to $\mathcal{G}(E_P(p)/E_P)$, for some field $E_P$ without a primitive $p$-th root of unity.

**Proposition 6.6.** *Let $P$ be a standardly admissible Demushkin pro-$p$-group, for some $p \in \mathbb{P} \setminus \{2\}$, and let $m \in \mathbb{N}$ be a divisor of $p-1$. Then there exists a field $E$, such that $\mathcal{G}(E(p)/E) \cong P$ and $[E(\varepsilon) \colon E] = m$, where $\varepsilon$ is a primitive $p$-th root of unity in $E_{\mathrm{sep}}$.*

*Proof.* Let $\mathbb{Q}$ be the field of rational numbers, $\Gamma$ the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$ in $\mathbb{Q}_{\mathrm{sep}}$, and for each $n \in \mathbb{N}$, let $\Gamma_n$ be the subextension of $\mathbb{Q}$ in $\Gamma$ of degree $p^{n-1}$. Fix a primitive $p$-th root of unity $\varepsilon \in \mathbb{Q}_{\mathrm{sep}}$, denote by $R_m$ the extension of $\mathbb{Q}$ in $\mathbb{Q}(\varepsilon)$ of degree $(p-1)/m$, suppose that the reduced component of $C(P)$ is of order $p^{\nu}$ (see (1.4)), put $\Phi = R_m\Gamma_{\nu}$, and let $\omega$ be a valuation of $\Phi$ extending the normalized $p$-adic valuation of $\mathbb{Q}$. It follows from the Grunwald-Wang theorem that there is a cyclic extension $F$ of $\Phi$ in $\mathbb{Q}_{\rm sep}$, such that $[F\colon \Phi] = m$, $F \cap \mathbb{Q}(\varepsilon) = \Phi$ and $\Phi(\varepsilon)$ is embeddable over $\Phi$ in $F_f$, where $f$ is a valuation of $F$ extending $\omega$. Using the same theorem, one proves the existence of a field $F' \in I(\mathbb{Q}_{\rm sep}/F)$, such that $F' \cap F(\varepsilon) = F$, $F'/F$ is inertial relative to $f$ and $[F'\colon F] = r$, where $r = (r(P)-2)/(p^{\nu}-p^{\nu-1})$. This implies that $F'$ has a unique, up-to an equivalence, valuation $f'$ extending $f$. Consider now some $p$-Henselization $E \in I(F'(p)/F')$ of $F$ relative to $f'$. It follows from Galois theory and the definition of $E$ that $[E(\varepsilon)\colon E] = m$. Observing that $\varepsilon \in E_{h(f)}$, $[E_f\colon \mathbb{Q}_p] = r(P) - 2$ and $\mathcal{G}(E_f(p)/E_f) \cong \mathcal{G}(E(p)/E)$, one obtains from (1.1) and (1.2) that $\mathcal{G}(E(p)/E)$ is a Demushkin group and $r(p)_E = r(P)$. Taking also into account that $\nu$ is the greatest integer for which $E(\varepsilon)$ contains a primitive $p^{\nu}$-th root of unity, one deduces from [10], Theorem 1 (see also [24], Sect. 5), that the reduced component of $C(\mathcal{G}(E(p)/E))$ is of order $p^{\nu}$. Since $p > 2$ and by (1.3) (ii), $P$ is uniquely determined by $(r(P), \nu)$, up-to an isomorphism, these results indicate that $\mathcal{G}(E(p)/E) \cong P$, which proves Proposition 6.6. □

## 7. The decomposition groups of admissible Demushkin groups

The purpose of this Section is to prove Theorem 1.3 and to describe the decomposition groups of Demushkin pro-$p$-groups of finite rank. The assumptions of Theorem 1.3 guarantee that the field $E' = E(p) \cap E_{h(w)}$ is a proper extension of $E$, where $E_{h(w)}$ is a Henselization of $E$ in $E_{\rm sep}$ relative to $w$. Put $\Sigma(R) = R(\varepsilon) \cap E'(\varepsilon)^{*p}$, for each $R \in {\rm I}(E(p)/E)$, and denote by $w'$ the $p$-Henselian valuation of $E'$ extending $w$. Suppose first that $w(E)$ is Archimedean. We show that $E'/E$ is an infinite extension. Assuming the opposite, one obtains the existence of a field $\Phi \in I(E(p)/E')$, such that $\Phi/E$ is Galois, $[\Phi\colon E] \in \mathbb{N}$, and $w$ has at least 2 nonequivalent prolongations $w_1$ and $w_2$ on $\Phi$. Since $w_2 = w_1 \circ \theta$, for some $\theta \in \mathcal{G}(\Phi/E)$, and one can choose $w_1 = w'_{\Phi}$, $w_1$ and $w_2$ must be $p$-Henselian valuations. This contradicts the Grunwald-Wang theorem and thereby proves that $[E'\colon E] = \infty$. Hence, by Remark 3.5, $\mathcal{G}(E(p)/E')$ is a free pro-$p$-group. Our argument also relies on the fact that $E'_{h(w')}$ is separably closed in $E'_{w'}$. In view of (3.6), this ensures that $E''_{\varepsilon} \subseteq N(L'/E'')$ whenever $L'$ is a finite extension of $E'$ in $E(p)$ and $E'' \in I(L'/E')$. Therefore, it can be easily deduced from the Approximation Theorem (e.g., [26], Ch. XII, Sect. 1) and norm transitivity in towers of finite separable extensions, that $E_{\varepsilon} \subseteq N(L(\varepsilon)/E(\varepsilon)).\Sigma(E)$, for every finite extension $L$ of $E$ in $E(p)$. Consider the fields $E_n \in I(E(p)/E)$, $n \in \mathbb{N}$, defined inductively as follows:

(7.1) $E_1 = E$, and for each $n \in \mathbb{N}$, $E_{n+1}$ is the compositum of the extensions of $E_n$ in $E(p)$ of degree $p$.

It is clear from (7.1), Lemma 3.2 and Galois theory that $E_n/E$ is a finite Galois extension, and by Proposition 3.4, $\mathcal{G}(E(p)/E_n)$ is a Demushkin group of rank $2 + [E_n\colon E](r(p)_E - 2)$, for each $n \in \mathbb{N}$. Note also that Galois theory and the subnormality of proper subgroups of finite $p$-groups imply that $E(p) = \cup_{n=1}^{\infty} E_n$. Observing that the symbol $E(\varepsilon)$-algebras $A_\varepsilon(E(\varepsilon); a_1, a_2)$ and $A_\varepsilon(E(\varepsilon); a_2, a_1)$ are inversely isomorphic whenever $a_1, a_2 \in E(\varepsilon)^*$, one deduces from Corollary 3.3, statement (3.5) and Albert's theorem that $N(E_{n+1}(\varepsilon)/E_n(\varepsilon)) \cap E_{n,\varepsilon} \subseteq E_n(\varepsilon)^{*p}$. Denote by $w_n$ the valuation of $E_n$ induced by $w'$, for each index $n$. The preceding observations indicate that $\Sigma(E_n) = E_{n,\varepsilon}$, so it follows from Albert's theorem and the $p$-Henselity of $w'$ that $E_{n+1} \subset E'$, $n \in \mathbb{N}$. This yields $E(p) \subseteq E'$ when $w(E) \leq \mathbb{R}$.

In order to deduce Theorem 1.3 in general, it suffices to prove the following statements, assuming that $E' \neq E(p)$ and $w(E)$ is non-Archimedean:

(7.2) (i) $w_{G(E)}$ is $p$-Henselian and finite extensions of $E$ in $E(p)$ are inertial relative to $w_{G(E)}$; in particular, $\mathcal{G}(E_{G(E)}(p)/E_{G(E)}) \cong \mathcal{G}(E(p)/E)$;

(ii) The valuation $\hat{w}_{G(E)}$ of $E_{G(E)}$ is Archimedean; equivalently, $G(E) \subseteq H$, for every $H \in \mathrm{Is}_w(E)$, $H \neq \{0\}$.

The rest of this Section is devoted to the proof of (7.2). Let $H'$ be an arbitrary group from $\mathrm{Is}_{w'}(E')$. By (2.1) (ii), the topologies on $E'$ induced by $w'$ and by $w'_{H'}$ are equivalent, whence the completions $E'_{w'}$ and $E'_{w'_{H'}}$ are $E$-isomorphic. Note also that $H'$ is a maximal element of $\mathrm{Is}_{w'}(E')$ if and only if $H' \cap w(E)$ is maximal in $\mathrm{Is}_w(E)$ (with respect to the orderings by inclusion). As a first step towards the proof of (7.2), we prove the following:

(7.3) With notation being as above, suppose that the group $H = H' \cap w(E)$ is maximal in $\mathrm{Is}_w(E)$. Then:

(i) $w_H$ is $p$-Henselian with $\mathrm{char}(E_H) \neq p$;

(ii) Finite extensions of $E$ in $E(p)$ are inertial relative to $w_H$; in particular, $\mathcal{G}(E_H(p)/E_H) \cong \mathcal{G}(E(p)/E)$;

(iii) $E'_{H'}$ is a $p$-Henselization of $E_H$ relative to $\hat{w}_H$, and $\hat{w}'_{H'}$ is the $p$-Henselian valuation of $E'_{H'}$ extending $\hat{w}_H$.

Statement (2.1) (i) and the choice of $H$ ensure that $w'_H(E')$ and $w_H(E)$ are Archimedean. Since, by Proposition 2.1, $w'_{H'}$ is $p$-Henselian, these observations enable one to deduce from the inequality $E' \neq E(p)$ that $w_H$ is $p$-Henselian. As $w(E)$ is non-Archimedean, we have $H \neq \{0\}$, which implies that $\hat{w}_H$ is a nontrivial valuation of $E_H$. Therefore, $E_H$ is infinite, so it follows from Proposition 5.1 and Lemma 4.3 that $\mathrm{char}(E_H) \neq p$. This completes the proof of (7.3) (i). The latter conclusion of (7.3) (ii) follows from (2.3) (ii) and the former one, and (7.3) (iii) is implied by (7.3) (i) and Proposition 2.1. It remains for us to prove former assertion of (7.3) (ii). Denote for brevity by $(\Sigma, \sigma)$ some Henselization of $(E, w_H)$. Clearly, $(\Sigma, \sigma)/(E, w_H)$ is immediate. Moreover, by (2.1) (iii) and the maximality of $H$ in $\mathrm{Is}_w(E)$, $w_H(E)$ is Archimedean, which implies that $E$ is dense in $\Sigma$ with respect to the topology of $\sigma$. Observing also that $w_H$ is $p$-Henselian and arguing as in the concluding part of the proof of (4.1), one obtains that $\Sigma(p) = E(p)\Sigma$, $E(p) \cap \Sigma = E$ and $\mathcal{G}(E(p)/E) \cong \mathcal{G}(\Sigma_\sigma(p)/\Sigma_\sigma) \cong \mathcal{G}(\Sigma(p)/\Sigma)$. This implies the former statement of (7.3) (ii) is equivalent to the one that finite extensions of $\Sigma$ in $\Sigma(p)$ are inertial relative to $\sigma$. Thus the proof of our assertion reduces to the special case in which $w_H$ is Henselian. In this case, when $\varepsilon \notin E$, the former part of (7.3) (ii) is contained in [5], Lemma 1.1 (a). Suppose finally that $w_H$ is Henselian and $\varepsilon \in E$. By [6], Lemma 3.8, and the assumption that $\mathcal{G}(E(p)/E)$ is a Demushkin group, then $E$ is a $p$-quasilocal field, in the sense of [6]. Since $r(p)_E \geq 3$ and $\mathrm{char}(E_H) \neq p$, this ensures that $w_H(E) = pw_H(E)$ (apply [8], (1.4)). The obtained result, combined with Ostrowski's theorem, implies that finite extensions of $E$ in $E(p)$ are inertial relative to $w_H$, so (7.3) is proved.

*Remark* 7.1. In the setting of (7.2), let $w$ be of finite height $d \geq 2$, and let $H$ and $H'$ be as in (7.3). Then $\hat{w}_H$ is of height $d-1$, so (7.2) and Theorem 1.3 can be proved by induction on $d$ (taking the inductive step via (7.3)).

The second step towards the proof of (7.2) and Theorem 1.3 is contained in the following lemma.

**Lemma 7.2.** *Let $(E, w)$ be a field with $\mathcal{G}(E(p)/E)$ Demushkin, $r(p)_E \in \mathbb{N}$, and $w_H$ non-$p$-Henselian, for any $H \in \mathrm{Is}_w(E)$. Then $E(p) \subseteq E_{h(w)}$.*

*Proof.* Put $E' = E(p) \cap E_{h(w)}$, denote by $w'$ the $p$-Henselian valuation of $E'$ extending $w$, and let $E_n$, $n \in \mathbb{N}$, be the fields defined in (7.1). We prove Lemma 7.2 by showing that $E_n \subseteq E'$, for every $n \in \mathbb{N}$. It is clear from Galois theory and the subnormality of proper subgroups of finite $p$-groups that $(E, w_G)$ will be $p$-Henselian, if $w_G$ is uniquely extendable on each finite extension of $E$ in $E(p)$ of degree $p$. At the same time, (7.3) and our assumptions indicate that $w(E)$ equals the union $H(E)$ of the groups $H \in \mathrm{Is}_w(E)$. Since $E_{h(v)}$ contains as an $E$-subalgebra a Henselization of $(E, w_H)$, for each $H \in \mathrm{Is}_w(E)$, this allows us, for the proof of Lemma 7.2, to consider only the special case where $\mathrm{char}(\widehat{E}) \neq p$. Also, it follows from the equality $w(E) = H(E)$ that if $R$ is a finite extension of $E$ in $E(p)$, and $f(X) \in O_w(E)[X]$ is the minimal (monic) polynomial of some primitive element of $R/E$, then the value of the discriminant of $f(X)$ is contained in some $H_f \in \mathrm{Is}_w(E)$. When $H \in \mathrm{Is}_w(E)$, $H_f \subseteq H$ and the reduction $f_H[X] \in E_H[X]$ modulo $M_{w_H}(E)$ is irreducible over $E_H$, this implies that $w_H$ is uniquely extendable to a valuation of $R$. Therefore, the assumptions that $r(p)_E \in \mathbb{N}$ and $w_H$ is not $p$-Henselian, for any $H \in \mathrm{Is}_w(E)$ indicate that $R$ can be chosen so that $f_H$ is reducible over $E_H$ whenever $H \in \mathrm{Is}_w(E)$ and $H_f \leq H$. It follows from the choice of $R$ that it is embeddable in $E_w$ over $E$. Since the valuation $w'$ of $E'$ is $p$-Henselian, whence $E'$ is separably closed in $E'_{w'}$, this implies that $R \subseteq E'$. The choice of $R$ also ensures that $(R, w_R)$ is immediate over $(E, w)$, where $w_R$ is the valuation of $R$ induced by $w'$. Let $\chi$ be a generator of $\mathcal{G}(R/E)$. It follows from the immediacy of $(R, w_R)/(E, w)$ and the equality $[R \colon E] = p$ that the compositions $w_R \circ \chi^{u-1}$, $u = 0, \dots, p-1$, are pairwise independent valuations of $R$ extending $w$ (see [2], Ch. VI, Sect. 8.2, and [26], Ch. IX, Proposition 11). As $\mathcal{G}(E(p)/R)$ is a Demushkin group and $r(p)_R \in \mathbb{N}$, this enables one to deduce from Grunwald-Wang's theorem that $(R, w_R)$ satisfies the conditions of Lemma 7.2. The obtained result allows us to define inductively a tower of fields $R_n \in I(E'/E)$, $n \in \mathbb{N}$, whose union $\Phi$ is an infinite extension of $E$ and embeds in $E_w$ over $E$. By [23], Theorem 2 (ii), $\mathcal{G}(E(p)/\Phi)$ is a free pro-$p$-group, so it follows from (3.6), Lemma 3.2 (i), the density of $E$ in $\Phi$ and the Approximation Theorem that if $L \in I(E(p)/E)$, $[L\colon E] \in \mathbb{N}$ and $\alpha \in E_{\varepsilon}$, then there is $\theta \in L_{\varepsilon}$, such that $\bar{w}(-1 + N_{E(\varepsilon)}^{L(\varepsilon)}(\theta)\alpha^{-1}) > 0$, for each prolongation $\bar{w}$ of $w$ on $E(\varepsilon)$. In view of the $p$-Henselity of $w'$, the equality $\mathrm{char}(\widehat{E}) = 0$ and Ostrowski's theorem, this ensures that $N_{E(\varepsilon)}^{L(\varepsilon)}(\theta)\alpha^{-1} \in E'(\varepsilon)^{*p}$. These observations, combined with the fact that $N(E_{n+1}(\varepsilon)/E_n(\varepsilon)) \cap E_{n,\varepsilon} = E_n(\varepsilon)^{*p}$, for every $n \in \mathbb{N}$, enable one to prove by induction on $n$ that $E_{n,\varepsilon} \subseteq E'(\varepsilon)^{*p}$, whence $E_n \subseteq E'$, for every index $n$. As $E(p) = \cup_{n=1}^{\infty} E_n$, this means that $E' = E(p)$, as claimed. □

We are now in a position to prove (7.2) and Theorem 1.3. Denote by $\mathcal{H}(E)$ the set of those $H \in \mathrm{Is}_w(E)$, $H \supseteq G(E)$, for which $w_H$ is $p$-Henselian, and for each $H \in \mathcal{H}(E)$, let $H'$ be the preimage in $w'(E')$ of the maximal torsion subgroup of $w'(E')/H$. It is easily verified that $H' \in \mathrm{Is}_{w'}(E')$ and $H' \cap w(E) = H$. The assumption that $E' \neq E(p)$ and Lemma 7.2 indicate that $\mathcal{H}(E)$ is nonempty. Note also that finite extensions of $E$ in $E(p)$ are inertial relative to $w_H$ (and $\mathcal{G}(E(p)/E) \cong \mathcal{G}(E_H(p)/E_H)$), for each $H \in \mathcal{G}(E)$. Since $\mathrm{char}(E_H) \neq p$, this is obtained from [5], Lemma 1.1 (a), and [8], (1.4), by the method of proving (7.3) (ii). Taking further into account that $\mathcal{H}(E)$ is closed under the formation of intersections, and applying Zorn's lemma, one concludes that $\mathcal{H}(E)$ contains a minimal element, say $G$, with respect to inclusion. We show that $G = G(E)$. As $G' \in \mathrm{Is}_{w'}(E')$ and $G' \cap w(E) = G$, it follows from Proposition 2.1 and the $p$-Henselian property of $w_G$ that $(E'_{G'}, \hat{w}_{G'})$ is a $p$-Henselization of $(E_G, \hat{w}_G)$. Considering now $(E_G, \hat{w}_G)$ instead of $(E, w)$, and applying Proposition 2.1, one reduces the proof of (7.2) and Theorem 1.3 to the special case in which $w(E) = G$. Using Lemma 7.2, one also concludes that if $G \neq G(E)$, then there exists a group $\widetilde{G} \in \mathcal{H}(E)$ which is properly included in $G$. This contradicts the minimality of $G$ in $\mathcal{H}(E)$ and so proves that $G = G(E)$. In view of the preceding observations, the obtained result completes the proof of (7.2) (i) (and of Theorem 1.3 in the case where $\mathrm{char}(\widehat{E}) \neq p$). The equality $w(E) = G(E)$ means that $w(p) \notin H$, for any $H \in \mathrm{Is}_w(E)$. This ensures that $\mathrm{char}(E_H) = p$, $H \in \mathrm{Is}_w(E)$, and $\mathrm{Is}_w(E)$ satisfies the conditions of Zorn's lemma with respect to the ordering by inclusion. Taking a maximal element $\overline{H}$ in $\mathrm{Is}_w(E)$, one obtains from (7.3) (i) that $\overline{H} = 0$, which completes the proof of (7.2). As $w$ is not $p$-Henselian, the obtained result and Proposition 2.1 imply that $\hat{w}_{G(E)}$ is not $p$-Henselian and $(E'_{G(E)'}, \hat{w}_{G(E)'})$ is a $p$-Henselization of $(E_{G(E)}, \hat{w}_{G(E)})$. Since $\mathcal{G}(E(p)/E) \cong \mathcal{G}(E_{G(E)}(p)/E_{G(E)})$ and $\hat{w}_{G(E)}$ is Archimedean, this rules out the possibility that $E' \neq E(p)$, so Theorem 1.3 is proved.

*Remark* 7.3. Let $E$ be a field with $r(p)_E \in \mathbb{N}$, for some $p \in P(E)$, and let $\mathbb{F}$ be the prime subfield of $E$. Suppose that $\mathcal{G}(E(p)/E)$ is a Demushkin group and, in case $r(p)_E \geq 3$, $E$ contains a primitive $p$-th root of unity. As shown in [9], then it follows from Proposition 3.4, [39], Theorem 2, and (when $r(p) \geq 3$) from [29], (16.1), and the isomorphism $H^2(\mathcal{G}(E(p)/E), \mathbb{F}_p) \cong {}_p\mathrm{Br}(E)$, that $E$ possesses a subfield $\widetilde{E}$, such that $\mathcal{G}(\widetilde{E}(p)/\widetilde{E}) \cong \mathcal{G}(E(p)/E)$, $\widetilde{E}$ is algebraically closed in $E$ and $\widetilde{E}/\mathbb{F}$ is of finite transcendency degree $d$. This ensures that nontrivial valuations of $\widetilde{E}$ are of heights $\leq d + 1$. Note also that, under the hypotheses of Theorem 1.3, $\widetilde{E}$ can be chosen so that its valuation $\tilde{w}$ induced by $w$ is nontrivial and non-$p$-Henselian. In view of Remark 7.1, these observations simplify the proof of Theorem 1.3 and relate (1.5) to the problem of classifying admissible Demushkin groups.

Theorem 1.3 allows one to view Theorem 1.1 (ii) as a generalization of [14], Theorem 6.3 (ii). Observe now that the proof of Theorem 1.3 in case $w(E) \leq \mathbb{R}$ and the one of Lemma 7.2 do not require that $r(p)_E \geq 3$. Since, by Proposition 3.4, the class of Demushkin groups of rank 2 is closed under the formation of open subgroups, this enables one to obtain the following result by adapting the proof of Theorem 1.3:

**Proposition 7.4.** *Let $(E, w)$ be a nontrivially valued field with $r(p)_E = 2$, for some $p \in P(E)$, and suppose that $\mathcal{G}(E(p)/E)$ is a Demushkin group and the field $E' = E_{h(w)} \cap E(p)$ is different from $E$ and $E(p)$. Then:*

(i) *$E_{h(w)}$ contains a primitive $p$-th root of unity, $E'/E$ is a $\mathbb{Z}_p$-extension and $p \notin P(\widehat{E})$; in addition, if $\mathrm{char}(\widehat{E}) = p$, then $\widehat{E}$ is perfect;*

(ii) *$\Delta(w) \neq p\Delta(w)$ and $w_H$ is $p$-Henselian, for some $H \in \mathrm{Is}_w(E)$; in particular, $w(E)$ is non-Archimedean.*

It is not difficult to see that, for each Demushkin pro-$p$-group $P$ of rank 2, there exists $(E, w)$ satisfying the conditions of Proposition 7.4 with $\mathcal{G}(E(p)/E) \cong P$. Note also that $\mathcal{G}(E(p)/E')$ is a characteristic subgroup of $\mathcal{G}(E(p)/E)$ unless $P \cong \mathbb{Z}_p^2$. This follows from Galois theory and the fact that $E'$ is the unique $\mathbb{Z}_p$-extension of $E$ in $E(p)$. Observe finally that the (continuous) automorphism group of $\mathbb{Z}_p^2$ acts transitively upon the set $\Omega_p$ of those closed subgroups $\Gamma \leq \mathbb{Z}_p^2$, for which $\mathbb{Z}_p^2/\Gamma \cong \mathbb{Z}_p$. This implies that if $P \cong \mathbb{Z}_p^2$ and $\Gamma \in \Omega_p$, then $\Gamma$ is a direct summand in $\mathbb{Z}_p^2$, $\Gamma \cong \mathbb{Z}_p$ and there is an isomorphism $P \cong \mathcal{G}(E(p)/E)$ which maps $\Gamma$ upon $\mathcal{G}(E(p)/E')$. Thus Corollary 6.4 and Proposition 7.4, combined with Theorems 1.1, 1.2 and 1.3, completely describe the decomposition groups of admissible Demushkin pro-$p$-groups of finite rank. The question of whether a field $R$, such that $\mathcal{G}(R(p)/R)$ is a Demushkin group with $r(p)_R \in \mathbb{N}$, possesses a $p$-Henselian valuation remains open. By [14], Proposition 9.4, the answer is affirmative, if $r(p)_R = 2$ and $R$ contains a primitive $p$-th root of unity.

## References


[1] A.A. Albert, *Modern Higher Algebra*, Univ. of Chicago Press, XIV, Chicago, Ill., 1937.

[2] N. Bourbaki, *Elements de Mathematique. Algebre Commutative*, Chaps. V, VI, VII, Hermann, Paris, 1964.

[3] C. Chevalley, *Sur la theorie du corps de classes dans les corps finis et les corps locaux*, J. Fac. Sci. Univ. Tokio, II, **9** (1933), 365-476.

[4] I.D. Chipchakov, *Henselian valued quasi-local fields with totally indivisible value groups*, I, Comm. Algebra **27** (1999), 3093-3108; Preprint, arXiv:1011.2611v3 [math.Ra].

[5] I.D. Chipchakov, *On the Galois cohomological dimensions of stable fields with Henselian valuations*, Comm. Algebra **30** (2002), 1549-1574.

[6] I.D. Chipchakov, *On the residue fields of Henselian valued stable fields*, I, J. Algebra **319** (2008), 16-49.

[7] I.D. Chipchakov, *Primarily quasilocal fields and* 1*-dimensional abstract local class field theory*, Preprint, arXiv:math/0506515v7 [math.RA].

[8] I.D. Chipchakov, *On Henselian valuations and Brauer groups of primarily quasilocal fields*, Preprint.

[9] I.D. Chipchakov, *Characterization of Demushkin groups among Galois groups of maximal $p$-extensions*, Preprint.

[10] S.P. Demushkin, *The group of a maximal $p$-extension of a local field*, Izv. Akad. Nauk SSSR Math. Ser. **25** (1961), 329-346 (in Russian).

[11] S.P. Demushkin, *On* 2*-extensions of a local field*, Sibirsk. Mat. Zh. **4** (1963), 951-955 (in Russian: English transl. in Amer. Math. Soc. Transl., Ser. 2, **50** (1966), 178-182).

[12] D. Dummit and J. Labute, *On a new characterization of Demushkin groups*, Invent. Math. **73** (1983), 413-418.

[13] I. Efrat, *Finitely generated pro-$p$ Galois groups of $p$-Henselian fields*, J. Pure Appl. Algebra **138** (1999), 215-228.

[14] I. Efrat, *Demuskin fields with valuations*, Math. Z. **243** (2003), 333-353.

[15] I. Efrat, *Valuations, Orderings, and Milnor $K$-Theory,* Math. Surveys and Monographs 124, Amer. Math. Soc., Providence, RI, 2006.

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

[17] A.J. Engler and T.M. Viswanathan, *Digging holes in algebraic closures a la Artin*, I, Math. Ann. **265** (1983), 263-271; II, Contemp. Math. **8** (1982), 351-360.

[18] Yu.L. Ershov, *Decision Problems and Constructivizable Models*, Mat. Logika I Osnovaniya Matematiki, Nauka, Moscow, 1980 (in Russian).

[19] M.D. Fried and M. Jarden, *Field Arithmetic*, 3rd revised ed., Ergebnisse der Math. und ihrer Grenzgebiete, 3, Fol. 11, Berlin-Heidelberg-New York, Springer, 2008.

[20] K. Iwasawa, *Local Class Field Theory*, transl. from Japanese into Russian by A.A. Bel'skii, transl. edited by B.B. Venkov, Mir, Moscow, 1983.

[21] B. Jacob and A.R. Wadsworth, *Division algebras over Henselian fields*, J. Algebra **128** (1990), 126-179.

[22] H. Koch, *Die Galoische Theorie der $p$-Erweiterungen*, Math. Monogr. 10, VEB Deutscher Verlag der Wissenschaften, Berlin; Springer-Verlag X, Berlin-Heidelberg-New York, 1970.

[23] J.P. Labute, *Demushkin groups of rank $\aleph_0$*, Bull. Soc. Math. France **94** (1966), 211-244.

[24] J.P. Labute, *Classification of Demushkin groups*, Canad. J. Math. **19** (1967), 106-132.

[25] T.Y. Lam, *Orderings, valuations and quadratic forms*, Conf. Board Math. Sci. Regional Conf. Ser. Math. No 52, Amer. Math. Soc., Providence, RI, 1983.

[26] S. Lang, *Algebra*, Reading, Mass., Addison-Wesley, Inc., XVIII, 1965.

[27] F. Lorenz and P. Roquette, *The theorem of Grunwald-Wang in the setting of valuation theory*, F.-V. Kuhlmann (ed.) et. al., Valuation theory and its applications, Vol. II (Saskatoon, SK, 1999), 175-212, Fields Inst. Commun., **33**, Amer. Math. Soc., Providence, RI, 2003.

[28] O.V. Mel'nikov and O.I. Tavgen', *The absolute Galois group of a Henselian field*, Dokl. Akad. Nauk BSSR **29** (1985), 581-583 (in Russian).

[29] A.S. Merkur'ev and A.A. Suslin, *$K$-cohomology of Brauer-Severi varieties and the norm residue homomorphism*, Izv. Akad. Nauk SSSR **46** (1982), 1011-1046 (Russian: English transl. In Math. USSR Izv. **21** (1983), 307-340).

[30] R. Pierce, *Associative Algebras*, Graduate Texts in Math., vol. 88, Springer-Verlag, New York-Heidelberg-Berlin, 1982.

[31] F. Pop, *Galoissche Kennzeichnung $p$-adisch abgeschlossener Körper*, J. Reine Angew. Math. **392** (1988), 145-175.

[32] J.-P. Serre, *Structure de certains pro-$p$-groupes (après Demushkin)*, Semin. Bourbaki **15** 1962/1963 (1964), No 252.

[33] J.-P. Serre, *Cohomologie Galoisienne*, Cours au College de France, 1962/1963, 2nd ed., Springer-Verlag, Berlin-Göttingen-Heidelberg-New York, 1964.

[34] J.-P. Serre, *Sur la dimension cohomologique des groupes profinis*, Topology **3** (1965), 413-420.

[35] I.R. Shafarevich, *On p-extensions*, Mat. Sb., N. Ser., bf 20 (**62**) (1947), 351-363 (in Russian).

[36] J. Tate, *Relations between $K_2$ and Galois cohomology*, Invent. Math. **36** (1976), 257-274.

[37] I.L. Tomchin and V.I. Yanchevskij, *On defects of valued division algebras*, Algebra i Analiz **3** (1991), 147-164 (in Russian: English transl. in St. Petersburg Math. J. **3** (1992), 631-647).

[38] R. Ware, *Galois groups of maximal p-extensions*, Trans. Amer. Math. Soc. **333** (1992), 721-728.

[39] G. Whaples, *Algebraic extensions of arbitrary fields*, Duke Math. J. **24** (1957), 201-204.

Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Acad. G. Bonchev Str., bl. 8, 1113, Sofia, Bulgaria; email: chipchak@math.bas.bg