PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY, SERIES B
Volume 10, Pages 326–340 (September 27, 2023)
https://doi.org/10.1090/bproc/192

A CONVERSE TO THE HASSE–ARF THEOREM

G. GRIFFITH ELDER AND KEVIN KEATING

(Communicated by David Savitt)

Abstract. Let K be a local field with perfect residue field and let L/K be a finite Galois extension. The Hasse-Arf theorem says that if $\mathrm{Gal}(L/K)$ is abelian then the upper ramification breaks of L/K must be integers. We prove the following converse to the Hasse-Arf theorem: Let G be a nonabelian group which is isomorphic to the Galois group of some totally ramified extension E/F of local fields with residue characteristic $p > 2$. Then there is a totally ramified extension L/K of local fields with residue characteristic p such that $\mathrm{Gal}(L/K) \cong G$ and L/K has at least one nonintegral upper ramification break.

1. Introduction

Let K be a local field, that is, a complete discrete valuation field with perfect residue field of characteristic $p > 0$. Let L/K be a finite Galois extension. Associated to L/K are rational numbers $u_1 \le u_2 \le \cdots \le u_n$ known as the upper ramification breaks of L/K. The upper ramification breaks provide arithmetic information about the extension L/K. For instance, L/K is a nontrivial unramified extension if and only if -1 is the only upper ramification break of L/K, and L/K is at most tamely ramified if and only if the set of upper ramification breaks of L/K is contained in $\{-1, 0\}$. It is a classical problem to determine the possibilities for sequences of upper breaks. The Hasse-Arf theorem [2,9] says that if $G = \mathrm{Gal}(L/K)$ is abelian then every upper break of L/K is an integer. The Hasse-Arf theorem plays an important role in several areas of number theory. For instance, it is used in the construction of the Artin representation [3] and in Lubin's proof of the local Kronecker-Weber theorem [11].

The purpose of this paper is to prove a converse to the Hasse-Arf theorem. A full converse to the Hasse-Arf theorem would state that if G is a finite nonabelian group then there exists a G-extension of local fields which has a nonintegral upper ramification break. In fact the converse to Hasse-Arf does not hold in such generality. For instance, if G is a nonabelian simple group and L/K is a G-extension then K has infinite residue field and L/K is unramified, so the only upper ramification break of L/K is -1. In addition, if G is a nonabelian group of order prime to p then every G-extension L/K of local fields with residue characteristic p is at most tamely ramified, and hence has upper ramification breaks contained in $\{-1, 0\}$. To rule out examples like these we restrict our attention to totally ramified extensions. Furthermore, to avoid vacuous cases we only consider those nonabelian groups G which can actually occur as the Galois group of a totally ramified extension of local

Received by the editors February 17, 2023, and, in revised form, July 26, 2023, and August 19, 2023.

2020 *Mathematics Subject Classification.* Primary 11S15, 11S20, 20D15.

fields with residue characteristic $p > 2$. In Theorem 6.3 we prove that if G is a such a group then there exists a local field K with residue characteristic p and a totally ramified G-extension L/K which has a nonintegral upper ramification break.

In Section 2 we outline higher ramification theory for Galois extensions of local fields. Our approach to proving the converse to Hasse-Arf is based on constructing Galois extensions of local fields in characteristic p which have nonintegral upper ramification breaks. A benefit of working in characteristic p is that one can solve embedding problems for p-extensions, as explained in Section 3. This means that it's enough to construct extensions whose Galois groups are minimal in a certain sense. Therefore in Section 4 we classify minimal p-groups. In Section 5 we use the results of Sections 3 and 4 to prove the converse to the Hasse-Arf theorem for totally ramified p-extensions. In Section 6 we extend the proof to cover arbitrary totally ramified extensions.

Throughout the paper we let K be a field which is complete with respect to a discrete valuation, with perfect residue field of characteristic $p > 2$. Let K^{sep} be a separable closure of K, and for each finite subextension L/K of K^{sep}/K let v_L be the valuation on K^{sep} normalized so that $v_L(L^\times) = \mathbb{Z}$. Let $\mathcal{O}_L$ denote the ring of integers of L, let $\mathcal{M}_L$ denote the maximal ideal of $\mathcal{O}_L$, and let π_L be a uniformizer for L.

2. Ramification in extensions of local fields

Let L/K be a finite totally ramified Galois extension. In this section we define the lower and upper ramification breaks of L/K, and the ramification subgroups of $\mathrm{Gal}(L/K)$. For more information on these topics see Chapter IV of [12].

Let L/K be a totally ramified Galois extension of degree mp^n, with $p \nmid m$. Set $G = \mathrm{Gal}(L/K)$. For $\sigma \in G$ with $\sigma \neq \mathrm{id}_L$ define the ramification number of σ to be $i(\sigma) = v_L(\sigma(\pi_L) - \pi_L) - 1$; also define $i(\mathrm{id}_L) = \infty$. (Beware that $i(\sigma)$ is related to $i_G(\sigma)$ as defined in [12, IV] by $i_G(\sigma) = i(\sigma) + 1$.) One easily sees that if $\sigma, \tau \in G \smallsetminus \{\mathrm{id}_L\}$ with $i(\sigma) > 0$ then

$$i(\sigma^p) > i(\sigma), \;\; i([\sigma, \tau]) > i(\tau). \tag{2.1}$$

For real $x \geq 0$ set $G_x = \{\sigma \in G : i(\sigma) \geq x\}$. Then G_x is a normal subgroup of G, known as the xth lower ramification subgroup of G. Say $b \geq 0$ is a lower ramification break of L/K (or simply a lower break) if $G_{b+\epsilon} \subsetneqq G_b$ for all $\epsilon > 0$. Thus b is a lower break of L/K if and only if $b = i(\sigma)$ for some $\sigma \in G$ with $\sigma \neq \mathrm{id}_L$. It follows that every lower break of L/K is a nonnegative integer. Furthermore, a nonnegative integer b is a lower ramification break if and only if $G_{b+1} \subsetneqq G_b$.

We have $i(\sigma) = 0$ if and only if $|\sigma|$ is not a power of p. Hence $b_0 = 0$ is a lower ramification break of L/K if and only if $m > 1$. If b is a positive lower break of L/K then $|G_b : G_{b+1}| = p^d$ for some $d \geq 1$. In this case we say that b is a lower break with multiplicity d. The positive lower ramification breaks of L/K, counted with multiplicities, form a multiset with cardinality n. We denote the positive lower breaks of L/K by $b_1 \leq b_2 \leq \cdots \leq b_n$.

Let M/K be a subextension of L/K and set $H = \mathrm{Gal}(L/M)$. It follows from the definitions that $H_x = H \cap G_x$ for all $x \geq 0$. Therefore the multiset of lower ramification breaks of L/M is contained in the multiset of lower ramification breaks of L/K. In other words, the ramification groups G_x and the lower ramification breaks are compatible with passage to subgroups of Galois groups.

There is a different numbering system for the ramification groups of $G = \mathrm{Gal}(L/K)$ which is compatible with passage to quotients G/H of G by a normal subgroup H. The upper ramification breaks (or upper breaks) of L/K are defined in terms of the lower breaks as follows: First, $u_0 = 0$ is an upper break of L/K if and only if $b_0 = 0$ is a lower break. The positive upper breaks $u_1 \le u_2 \le \cdots \le u_n$ of L/K are then defined recursively by $u_1 = b_1/m$ and $u_{i+1} - u_i = (b_{i+1} - b_i)/mp^i$ for $1 \le i \le n-1$. We may view u_i as the upper ramification break of L/K which corresponds to b_i. The upper ramification breaks of L/K, counted with multiplicities, form a multiset, which we denote by $\mathcal{U}_{L/K}$. Note that if L/K is a ramified C_p-extension then L/K has a single upper and lower ramification break $u_1 = b_1$. Thus we may refer simply to the ramification break of L/K.

The upper ramification subgroups of G are defined for real $x \ge 0$ by $G^0 = G_0 = G$, $G^x = G_{b_1}$ for $0 < x \le u_1$, $G^x = G_{b_i}$ for $u_{i-1} < x \le u_i$, and $G^x = \{\mathrm{id}_L\}$ for $x > u_n$. Thus $u \ge 0$ is an upper ramification break of L/K if and only if $G^{u+\epsilon} \lneq G^u$ for all $\epsilon > 0$. Theorem 2.1 shows that the groups G^x and the upper ramification breaks are compatible with passage to quotients of Galois groups:

Theorem 2.1 (Herbrand)**.** *Let L/K be a finite totally ramified Galois extension and let M/K be a Galois subextension of L/K. Set $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/M)$.*

(a) *For $x \ge 0$ we have $(G/H)^x = G^x H/H$.*
(b) *$\mathcal{U}_{M/K} \subset \mathcal{U}_{L/K}$.*

Proof. Statement (a) is proved as Proposition 14 in [12, IV]. Statement (b) follows easily from (a). □

Corollary 2.2. *Let $x \ge 0$. Then $x \notin \mathcal{U}_{M/K}$ if and only if $G^x \le G^{x+\epsilon}H$ for all sufficiently small $\epsilon > 0$.*

Proof. This follows from (a) since $G^x H = G^{x+\epsilon}H$ if and only if $G^x \le G^{x+\epsilon}H$. □

We will make frequent use of the following (presumably well-known) fact:

Lemma 2.3. *Let N/K be a finite totally ramified Galois extension and set $G = \mathrm{Gal}(N/K)$. Assume that $Z(G)$ contains a subgroup H such that $H \cong C_p^2$, and let $M = N^H$ be the fixed field of H. Suppose there are $u < v$ such that $u, v \notin \mathcal{U}_{M/K}$ and $\mathcal{U}_{N/K} = \mathcal{U}_{M/K} \cup \{u, v\}$. Let $b < c$ be the lower ramification breaks of N/K that correspond to u, v and let $\mathcal{S}$ denote the set of fields L such that $M \subset L \subset N$ and $[L : M] = p$. Then there is $L_0 \in \mathcal{S}$ with the following properties:*

(a) *$\mathcal{U}_{L_0/K} = \mathcal{U}_{M/K} \cup \{u\}$ and N/L_0 has ramification break c.*
(b) *For all $L \in \mathcal{S}$ such that $L \ne L_0$ we have $\mathcal{U}_{L/K} = \mathcal{U}_{M/K} \cup \{v\}$ and N/L has ramification break b.*

Proof. First we prove that the lower ramification breaks of N/M are b, c. Since b is a lower ramification break of L/K there exists $g \in G_b \smallsetminus G_{b+1}$. Since $u \notin \mathcal{U}_{M/K}$, it follows from Corollary 2.2 that $G^u \le G^{u+\epsilon}H$ for sufficiently small $\epsilon > 0$. Since $G^u = G_b$ and $G^{u+\epsilon} = G_{b+1}$ we get $G_b \le G_{b+1}H$. Hence there are $g' \in G_{b+1}$ and $h \in H$ such that $g = g'h$. It follows that $h = (g')^{-1}g \in G_b \smallsetminus G_{b+1}$, so we have $i(h) = b$. Thus b is a lower ramification break of N/M. A similar argument shows that c is a lower ramification break of N/M. Now since the lower ramification breaks of N/M are b, c, for each $L \in \mathcal{S}$ the ramification break of N/L is either b or c. Let $L_0 = N^{H_c}$ be the fixed field of $H_c = H_{b+\epsilon}$. Since the ramification break of

N/L is $\geq c$ if and only if $\mathrm{Gal}(N/L) \leq H_c$ we see that N/L_0 has ramification break c, and N/L has ramification break b for all $L \in \mathcal{S}$ with $L \neq L_0$.

To complete the proof let $L \in \mathcal{S}$ and set $A = \mathrm{Gal}(N/L) \leq H$. Since c is the largest lower break of N/M, for sufficiently small $\epsilon > 0$ we have

$$G^{v+\epsilon} \cap H = G_{c+1} \cap H = H_{c+1} = \{\mathrm{id}_L\}.$$

It follows that $G^{v+\epsilon} \cap A = \{\mathrm{id}_L\}$, so we get $|G^{v+\epsilon}A : G^{v+\epsilon}| = |A| = p$. Since v is an upper break of N/K with multiplicity 1 we have $|G^v : G^{v+\epsilon}| = p$. Hence the statements $G^{v+\epsilon}A = G^v$, $G^{v+\epsilon}A \leq G^v$, and $G^v \leq G^{v+\epsilon}A$ are equivalent. It follows that $G^v \leq G^{v+\epsilon}A$ if and only if $A \leq G^v$. By Corollary 2.2 we deduce that $v \notin \mathcal{U}_{L/K}$ if and only if $A \leq G^v = G_c$. Hence $v \notin \mathcal{U}_{L/K}$ if and only if $A \leq G_c \cap H = H_c$. Since $\mathcal{U}_{L/K}$ is equal to either $\mathcal{U}_{M/K} \cup \{u\}$ or $\mathcal{U}_{M/K} \cup \{v\}$, we conclude that $\mathcal{U}_{L/K} = \mathcal{U}_{M/K} \cup \{u\}$ if $L = L_0$ and $\mathcal{U}_{L/K} = \mathcal{U}_{M/K} \cup \{v\}$ if $L \neq L_0$. □

3. Embedding problems in characteristic p

Let K be a field, let L/K be a finite Galois extension, and set $G = \mathrm{Gal}(L/K)$. Let $\widetilde{G}$ be a finite group and let $\phi : \widetilde{G} \to G$ be an onto homomorphism. A solution to the embedding problem associated to $(L/K, \widetilde{G}, \phi)$ is a finite extension M/L such that M is Galois over K and there is an isomorphism of exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(M/L) & \longrightarrow & \mathrm{Gal}(M/K) & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \ker\phi & \longrightarrow & \widetilde{G} & \xrightarrow{\phi} & G & \longrightarrow & 1. \end{array}$$

In this section we use a theorem of Witt to show that certain embedding problems for local fields of characteristic p always admit totally ramified solutions.

Recall that the rank of a finite p-group G is the minimum size of a generating set for G. Let $\Phi(G)$ denote the Frattini subgroup of G. It follows from the Burnside basis theorem that the Frattini quotient $G/\Phi(G)$ is an elementary abelian p-group such that $\mathrm{rank}(G)$ is equal to $\mathrm{rank}(G/\Phi(G))$. In [14, III], Witt proved the following:

Theorem 3.1. *Let K be a field of characteristic p and let L/K be a finite Galois extension such that $G = \mathrm{Gal}(L/K)$ is a p-group. Let $\widetilde{G}$ be a finite p-group such that $\mathrm{rank}(\widetilde{G}) = \mathrm{rank}(G)$ and let $\phi : \widetilde{G} \to G$ be an onto homomorphism. Then there is an extension M/L which solves the embedding problem associated to $(L/K, \widetilde{G}, \phi)$.*

We will use the following applications of Witt's theorem:

Corollary 3.2. *Let K be a local field of characteristic p with perfect residue field and let L/K be a finite totally ramified Galois extension whose Galois group $G = \mathrm{Gal}(L/K)$ is a p-group. Let $\widetilde{G}$ be a finite p-group and let $\phi : \widetilde{G} \to G$ be an onto group homomorphism. Then there is a totally ramified field extension M/L which solves the embedding problem associated to $(L/K, \widetilde{G}, \phi)$.*

Proof. Let $N = \ker\phi$. It suffices to consider the case where $N \cong C_p$, and hence $N \leq Z(G)$. If the extension $\widetilde{G}$ of G by N is split then $\widetilde{G} \cong C_p \times G$. In this case choose a ramified C_p-extension F/K whose ramification break is greater than all the upper breaks of L/K. Then L and F are linearly disjoint over K, so $M = LF$ is a totally ramified Galois extension of K with $\mathrm{Gal}(M/K) \cong C_p \times G \cong \widetilde{G}$. Hence

M solves the given embedding problem. If the extension $\widetilde{G}$ of G by N is not split we claim that $\operatorname{rank}(\widetilde{G}) = \operatorname{rank}(G)$. We clearly have $\operatorname{rank}(\widetilde{G}) \geq \operatorname{rank}(G)$. Let A be a generating set for G such that $|A| = \operatorname{rank}(G)$ and let $\widetilde{A} \subset \widetilde{G}$ satisfy $|\widetilde{A}| = |A|$ and $\phi(\widetilde{A}) = A$. If $\langle \widetilde{A} \rangle \neq \widetilde{G}$ then since $C_p \cong N \leq Z(G)$ we get $\langle \widetilde{A} \rangle \cong G$ and $\widetilde{G} = N \times \langle \widetilde{A} \rangle$. This contradicts the assumption that our extension is not split, so we must have $\langle \widetilde{A} \rangle = \widetilde{G}$. Hence $\operatorname{rank}(\widetilde{G}) = \operatorname{rank}(G)$. It follows by Theorem 3.1 that there is a field extension M/L which solves the given embedding problem. If M/L is unramified then there is an unramified C_p-extension F/K such that $M = LF$. It follows that $\operatorname{Gal}(M/K) \cong C_p \times G$, which is a contradiction. Therefore M/L is a totally ramified extension. □

Corollary 3.3. *Let K be a local field of characteristic p with perfect residue field and let $\widetilde{G}$ be a p-group. Then there is a totally ramified $\widetilde{G}$-extension L/K.*

Proof. Take $G = \{1\}$ in Corollary 3.3. □

4. Minimal nonabelian p-groups

We put a partial order on finite p-groups by $H \preccurlyeq G$ if H is isomorphic to a quotient of G. We are interested in the groups which are $\preccurlyeq$-minimal among nonabelian p-groups. We call such a group a minimal nonabelian p-group.

Proposition 4.1. *Let $p > 2$ and let G be a p-group. Then G is a minimal nonabelian p-group if and only if G satisfies the following conditions:*

(i) *G is nilpotent of class 2.*
(ii) *$Z(G)$ is cyclic of order p^d for some $d \geq 1$.*
(iii) *$[G,G]$ is the subgroup of $Z(G)$ of order p.*
(iv) *$\overline{G} := G/Z(G)$ is an elementary abelian p-group of rank $2n$ for some $n \geq 1$, and $[\ ,\ ]$ induces a nondegenerate skew-symmetric $\mathbb{F}_p$-bilinear form $(\ ,\ )_{\overline{G}}$ on $\overline{G}$ with values in $[G,G]$.*

Proof. Suppose G is a minimal nonabelian p-group. Since $Z(G)$ is nontrivial, $\overline{G}$ is abelian by the minimality of G. Hence G is nilpotent of class 2, which gives (i). Let N be a nontrivial normal subgroup of G. Then G/N is abelian by the minimality of G, so $[G,G] \leq N$. Hence $[G,G]$ is contained in all nontrivial subgroups of $Z(G)$, so $Z(G)$ is cyclic and $[G,G]$ is the unique subgroup of $Z(G)$ of order p. This proves (ii) and (iii).

Let z be a generator for $Z(G) \cong C_{p^d}$ and set $w = z^{p^{d-1}}$. Then $[G,G] = \langle w \rangle$. For $x, y \in G$ we have $xyx^{-1} = yw^a$ for some $a \in \mathbb{Z}$. Hence $xy^px^{-1} = y^pw^{pa} = y^p$, so $y^p \in Z(G)$. It follows that $\overline{G}$ is an elementary abelian p-group. Let $x, y_1, y_2 \in G$. Then there are $a_j \in \mathbb{Z}$ such that $xy_jx^{-1} = y_jw^{a_j}$ for $j = 1, 2$. It follows that $xy_1y_2x^{-1} = y_1y_2w^{a_1+a_2}$, and hence that $[x, y_1y_2] = [x,y_1][x,y_2]$. Since $[y,x] = [x,y]^{-1}$, we deduce that $[\ ,\ ]$ induces a skew-symmetric $\mathbb{F}_p$-bilinear pairing $(\ ,\ )_{\overline{G}}$ on $\overline{G}$. If $[x,y] = 1$ for all $y \in G$ then $x \in Z(G)$, so the pairing is nondegenerate. Therefore $\overline{G}$ has even $\mathbb{F}_p$-rank. This proves (iv).

Conversely, suppose (i)–(iv) hold. Then G is nonabelian by (i) or (iii). Let N be a nontrivial normal subgroup of G. Then $N \cap Z(G)$ is nontrivial, so $[G,G] \leq N$ by (ii) and (iii). Hence G/N is abelian, so G is a minimal nonabelian p-group. □

The minimal nonabelian p-groups can be described more explicitly. For $n, d \geq 1$ we define a group $H(n,d)$ of order p^{2n+d} generated by $x_1, \ldots, x_n, y_1, \ldots, y_n, z$, with

$|x_i| = |y_i| = p$ and $|z| = p^d$. All these generators commute with each other, except for x_i and y_i, which satisfy $[x_i, y_i] = z^{p^{d-1}}$ for $1 \le i \le n$. Thus $H(1,1)$ is the Heisenberg p-group, and $H(n,1)$ is an extraspecial p-group.

For $n, d \ge 1$ we also define a group $A(n,d)$, which has order p^{2n+d} and generators $x_1, \dots, x_n, y_1, \dots, y_n, z$. In $A(n,d)$ we have $|x_i| = p$ for $2 \le i \le n$, $|y_i| = p$ for $1 \le i \le n$, and $x_1^p = z$ with $|z| = p^d$. As with $H(n,d)$, all generators commute with each other except for x_i and y_i, which satisfy $[x_i, y_i] = z^{p^{d-1}}$ for $1 \le i \le n$. Thus $A(1,1)$ is the metacyclic group of order p^3, and $A(n,1)$ is an extraspecial p-group.

It is clear from the constructions that the groups $H(n,d)$ and $A(n,d)$ satisfy conditions (i)–(iv) of Proposition 4.1. We now prove the converse, which states that every minimal nonabelian p-group is isomorphic to one of these groups.

Proposition 4.2. *Let $p > 2$ and let G be a minimal nonabelian p-group. Then either $G \cong H(n,d)$ or $G \cong A(n,d)$ for some $n, d \ge 1$.*

Proof. Since G is a minimal nonabelian p-group, G satisfies conditions (i)–(iv) of Proposition 4.1. Let z be a generator for $Z(G)$; then $|z| = p^d$ for some $d \ge 1$. Set $w = z^{p^{d-1}}$, so that $\langle w \rangle = [G, G]$. It follows from (iv) that $x^p \in Z(G)$ for all $x \in G$. For $x \in G$ set $\overline{x} = xZ(G) \in \overline{G}$.

Suppose that $x^p \in Z(G)^p$ for all $x \in G$. Since $[\ ,\ ]$ induces a nondegenerate $\mathbb{F}_p$-linear pairing $(\ ,\ )_{\overline{G}}$ on $\overline{G}$, there is an $\mathbb{F}_p$-basis $\{\overline{x}_1, \dots, \overline{x}_n, \overline{y}_1, \dots, \overline{y}_n\}$ for $\overline{G}$ such that $(\overline{x}_i, \overline{x}_j)_{\overline{G}} = (\overline{y}_i, \overline{y}_j)_{\overline{G}} = w^0$ and $(\overline{x}_i, \overline{y}_j)_{\overline{G}} = w^{\delta_{ij}}$ for all $1 \le i, j \le n$. Let $x_i' \in G$ be such that $\overline{x}_i = x_i' Z(G)$. Then there is $a_i \in \mathbb{Z}$ such that $(x_i')^p = z^{pa_i}$. Therefore $x_i = x_i' z^{-a_i}$ satisfies $x_i Z(G) = \overline{x}_i$ and $|x_i| = p$. Similarly, there are $y_i \in G$ with $y_i Z(G) = \overline{y}_i$ and $|y_i| = p$. It follows that $G \cong H(n,d)$.

Now assume that there exists $y \in G$ such that $y^p \notin Z(G)^p$. Define $\phi : \overline{G} \to Z(G)/Z(G)^p$ by $\phi(xZ(G)) = x^p Z(G)^p$. Then ϕ is clearly well-defined. We claim that ϕ is a group homomorphism, and hence an $\mathbb{F}_p$-linear map. Let $x, y \in G$; then $[x,y] = z^a$ for some integer a. Thus $yx = xyz^{-a}$, so we get $(xy)^p = x^p y^p z^{pb}$ with $b = -\frac{1}{2}(p-1)a$. Hence $\phi(xy) = \phi(x)\phi(y)$. By our assumption, ϕ is nontrivial, so $\phi(\overline{G}) = Z(G)/Z(G)^p$ is cyclic of order p. Set $V = \ker \phi$ and let $V^\perp$ be the orthogonal complement of V with respect to the pairing $(\ ,\ )_{\overline{G}}$. Then V and $V^\perp$ are $\mathbb{F}_p$-subspaces of $\overline{G}$, with $\dim_{\mathbb{F}_p}(V) = 2n-1$ and $\dim_{\mathbb{F}_p}(V^\perp) = 1$. Let $y_1' \in G$ be such that $\overline{y}_1' = y_1' Z(G)$ generates $V^\perp$. Since $[y_1', y_1'] = w^0$ we have $\overline{y}_1' \in (V^\perp)^\perp = V = \ker \phi$. Hence there is $a \in \mathbb{Z}$ such that $(y_1')^p = z^{ap}$. Then $y_1 = y_1' z^{-a}$ satisfies $\overline{y}_1 = \overline{y}_1'$ and $|y_1| = p$. Now let $x_1 \in G$ be such that $(\overline{x}_1, \overline{y}_1)_{\overline{G}} = w^1$. Then $\overline{x}_1 \notin V$, so x_1^p is a generator for $Z(G)$. Therefore we may assume that $x_1^p = z$. Let W denote the span of $\{\overline{x}_1, \overline{y}_1\}$ in $\overline{G}$. Then the restriction of $(\ ,\ )_{\overline{G}}$ to W is nondegenerate, so $V = W \oplus W^\perp$ and the restriction of $(\ ,\ )_{\overline{G}}$ to $W^\perp$ is a nondegenerate skew-symmetric $\mathbb{F}_p$-bilinear form. Hence there is a basis $\{\overline{x}_2, \dots, \overline{x}_n, \overline{y}_2, \dots, \overline{y}_n\}$ for $W^\perp$ such that $(\overline{x}_i, \overline{x}_j)_{\overline{G}} = (\overline{y}_i, \overline{y}_j)_{\overline{G}} = w^0$ and $(\overline{x}_i, \overline{y}_j)_{\overline{G}} = w^{\delta_{ij}}$ for $2 \le i, j \le n$. Let $x_i' \in G$ be such that $\overline{x}_i = x_i' Z(G)$, and let $a_i \in \mathbb{Z}$ satisfy $(x_i')^p = z^{a_i}$. Since $\overline{x}_i \in W^\perp \subset V$ we have $a_i = pb_i$ for some $b_i \in \mathbb{Z}$. Hence $x_i = x_i' z^{-b_i}$ satisfies $x_i Z(G) = \overline{x}_i$ and $|x_i| = p$. Similarly for $2 \le i \le n$ there are $y_i \in G$ such that $y_i Z(G) = \overline{y}_i$ and $|y_i| = p$. Therefore $G \cong A(n,d)$. □

Remark 4.3. A p-group G is said to be of symplectic type if every abelian characteristic subgroup of G is cyclic. Philip Hall, in unpublished notes, showed that for $p > 2$ the nonabelian p-groups of symplectic type are precisely the groups $H(n,d)$

and $A(n,d)$ for $n,d \geq 1$. Therefore for $p > 2$ the minimal nonabelian p-groups are the same as the nonabelian p-groups of symplectic type. A proof of Hall's result can be found in [8, 5.4.9]. We thank Peter Sin for pointing us to this reference.

Let G be a group and let N_1, N_2 be subgroups of G. Say that G is a central product of N_1 and N_2 if $N_1 \cup N_2$ generates G and every element of N_1 commutes with every element of N_2. In that case there is a subgroup A of $Z(N_1) \times Z(N_2)$ such that $G \cong (N_1 \times N_2)/A$.

We wish to express minimal nonabelian p-groups as central products, with $H(1,1)$ as one of the factors. For convenience we extend the definition of $H(n,d)$ by setting $H(0,d) = C_{p^d}$.

Proposition 4.4.

(a) *Let $n,d \geq 1$. Then $H(n,d)$ is a central product of subgroups N_1 and N_2, with $N_1 \cong H(n-1,d)$ and $N_2 \cong H(1,1)$. More precisely,*

$$H(n,d) \cong (H(n-1,d) \times H(1,1))/B \tag{4.1}$$

for some subgroup B of $Z(H(n-1,d)) \times Z(H(1,1))$ of order p.

(b) *Let $n \geq 2$ and $d \geq 1$. Then $A(n,d)$ is a central product of subgroups N_1 and N_2, with $N_1 \cong A(n-1,d)$ and $N_2 \cong H(1,1)$. More precisely,*

$$A(n,d) \cong (A(n-1,d) \times H(1,1))/B \tag{4.2}$$

for some subgroup B of $Z(A(n-1,d)) \times Z(H(1,1))$ of order p.

Proof.

(a) Let $N_1 \leq H(n,d)$ be generated by $x_1, \ldots, x_{n-1}, y_1, \ldots, y_{n-1}, z$ and let $N_2 \leq H(n,d)$ be generated by $x_n, y_n, z^{p^{d-1}}$. Then $N_1 \cong H(n-1,d)$, $N_2 \cong H(1,1)$, and N_1, N_2 satisfy the conditions for a central product. Therefore there is a subgroup B of $Z(H(n-1,d)) \times Z(H(1,1))$ satisfying (4.1). Since $|H(n,d)| = p^{2n+d}$, $|H(n-1,d)| = p^{2n+d-2}$, and $|H(1,1)| = p^3$, we must have $|B| = p$.

(b) Let N_1 be the subgroup of $A(n,d)$ generated by $x_1, \ldots, x_{n-1}, y_1, \ldots, y_{n-1}, z$ and let N_2 be the subgroup of $A(n,d)$ generated by $x_n, y_n, z^{p^{d-1}}$. Then $N_1 \cong A(n-1,d)$, $N_2 \cong H(1,1)$, and N_1, N_2 satisfy the conditions for a central product. Therefore there is a subgroup B of $Z(A(n-1,d)) \times Z(H(1,1))$ satisfying (4.2). Since $|A(n,d)| = p^{2n+d}$, $|A(n-1,d)| = p^{2n+d-2}$, and $|H(1,1)| = p^3$, we must have $|B| = p$. □

Proposition 4.4(b) does not apply to groups of the form $A(1,d)$. Instead, we use the following description:

Proposition 4.5. *Let $d \geq 1$, and write $H(1,1) = \langle x_1, y_1, z\rangle$, $C_{p^{d+1}} = \langle w\rangle$. Define a subgroup G_d of $H(1,1) \times C_{p^{d+1}}$ by $G_d = \langle x_1 w, y_1, z\rangle$, and set*

$$\overline{G}_d = G_d/\langle (x_1 w)^{p^d} z^{-1}\rangle = G_d/\langle w^{p^d} z^{-1}\rangle.$$

Then $\overline{G}_d \cong A(1,d)$.

Proof. We have $[x_1 w, y_1] = [x_1, y_1] = z$ and $(x_1 w)^p = w^p$. Let $\overline{x}_1, \overline{y}_1, \overline{z}$ denote the images in $\overline{G}_d$ of $x_1 w, y_1, z$. Then $|\overline{x}_1| = p^{d+1}$, $|\overline{y}_1| = p$, and $[\overline{x}_1, \overline{y}_1] = \overline{z} = \overline{x}_1^{p^d}$. Hence $\overline{G}_d \cong A(1,d)$. □

5. p-EXTENSIONS WITH A NONINTEGRAL UPPER BREAK

Let $p > 2$, let G be a nonabelian p-group, and let K be a local field of characteristic p with perfect residue field k. In this section we prove that there exists a totally ramified Galois extension L/K with Galois group G such that L/K has an upper ramification break which is not an integer. It follows from Theorem 3.1 that every embedding problem over K which only involves p-groups can be solved with a totally ramified extension. Therefore we only need to give an example of a G-extension with a nonintegral upper break for each G which is $\preccurlyeq$-minimal among nonabelian p-groups. These groups are classified in Proposition 4.2.

Our proof uses a bootstrap argument, based on constructing $H(1,1)$-extensions with a nonintegral upper ramification break. As a first step, we give an easy method for building $H(1,1)$-extensions using Artin-Schreier extensions. Recall that if $\beta \in K$ satisfies $v_K(\beta) = -b$ with $b \geq 1$ and $p \nmid b$ then the roots of $X^p - X - \beta$ generate a C_p-extension of K with ramification break b (see [6, III, Proposition 2.5]).

Lemma 5.1. *Let a, b be positive integers with $a > b$, $p \nmid a$, and $p \nmid b$. Let $\alpha, \beta \in K$ satisfy $v_K(\alpha) = -a$ and $v_K(\beta) = -b$ and let $x, y \in K^{sep}$ satisfy $x^p - x = \alpha$ and $y^p - y = \beta$. Set $M = K(x, y)$ and let $\gamma \in K$. Let $z \in K^{sep}$ satisfy $z^p - z = \alpha y + \gamma$ and set $L = M(z)$. Then L/K is a totally ramified $H(1,1)$-extension.*

Proof. By construction M/K is a totally ramified C_p^2-extension. Let $\sigma, \tau \in \mathrm{Gal}(M/K)$ satisfy $\sigma(x) = x + 1$, $\sigma(y) = y$, $\tau(x) = x$, and $\tau(y) = y + 1$. Then

$$(\sigma - 1)(\alpha y + \gamma) = 0,$$
$$(\tau - 1)(\alpha y + \gamma) = \alpha = \wp(x).$$

Since $x \in M$ it follows that L/K is Galois. Furthermore, we may extend σ, τ to $\widetilde{\sigma}, \widetilde{\tau} \in \mathrm{Gal}(L/K)$ by setting $\widetilde{\sigma}(z) = z$ and $\widetilde{\tau}(z) = z + x$. We easily find that $|\widetilde{\sigma}| = |\widetilde{\tau}| = p$, $[\widetilde{\sigma}, \widetilde{\tau}] \in \mathrm{Gal}(L/M)$, and $[\widetilde{\sigma}, \widetilde{\tau}](z) = z + 1$. The last formula implies that $[\widetilde{\sigma}, \widetilde{\tau}]$ generates $\mathrm{Gal}(L/M)$. Therefore $\mathrm{Gal}(L/K) \cong H(1,1)$. □

Proposition 5.2. *Let K be local field of characteristic $p > 2$ with perfect residue field and let F/K be a ramified C_p-extension. Let b be the ramification break of F/K, and let a be an integer such that $a > b$ and $a \not\equiv 0, -b \pmod{p}$. Then there is a totally ramified extension L/F such that L/K is an $H(1,1)$-extension with $\mathcal{U}_{L/K} = \{b, a, a + p^{-1}b\}$. In particular, L/K has an upper ramification break which is not an integer.*

Proof. It follows from Proposition 2.4 in [6, III] that there is $y \in F$ such that $F = K(y)$, $v_F(y) = -b$, and $\beta := y^p - y \in K$. Since $p \nmid b$ we can write $a = bt + ps$ with $0 \leq t < p$; by our assumptions on a we get $1 \leq t \leq p - 2$. Set $\alpha = \pi_K^{-ps}\beta^t$; then $v_K(\alpha) = -a$. Let $x \in K^{sep}$ satisfy $x^p - x = \alpha$. Then $M := F(x) = K(x, y)$ is a C_p^2-extension of K with upper ramification breaks b, a. Let r be the inverse of $t + 1$ in $\mathbb{F}_p^\times$, let $z \in K^{sep}$ satisfy $z^p - z = \alpha y + r\alpha\beta$, and set $L = M(z)$. Then L/K is an $H(1,1)$-extension by Lemma 5.1. Furthermore, $\mathrm{Gal}(L/M) \cong C_p$ is the commutator subgroup of $\mathrm{Gal}(L/K)$. Hence by (2.1), $\mathrm{Gal}(L/M)$ is the smallest nontrivial ramification subgroup of $\mathrm{Gal}(L/K)$. Therefore by the corollary to Proposition 3 in [12, IV], the lower ramification breaks of M/K are also lower ramification breaks of L/K.

Let $E = F(z)$. We can't directly compute the ramification break of the C_p-extension E/F, since $v_F(\alpha y + r\alpha\beta) = v_F(r\alpha\beta)$ is divisible by p. So instead we

consider the Artin-Schreier equation

$$X^p - X = \alpha y + r\alpha\beta - \wp(r\pi_K^{-s} y^{t+1}).$$

Since $r\pi_K^{-s} y^{t+1} \in F$, the roots of this equation generate E over F. Furthermore, we have

$$\begin{aligned}\alpha y + r\alpha\beta - \wp(r\pi_K^{-s} y^{t+1}) &= \alpha y + r\alpha\beta + r\pi_K^{-s} y^{t+1} - (r\pi_K^{-s} y^{t+1})^p \\ &= \alpha y + r\alpha\beta + r\pi_K^{-s} y^{t+1} - r\pi_K^{-ps}(y+\beta)^{t+1} \\ &= \alpha y + r\alpha\beta + r\pi_K^{-s} y^{t+1} - r\pi_K^{-ps} \sum_{i=0}^{t+1} \binom{t+1}{i} \beta^{t+1-i} y^i.\end{aligned}$$

Since $\alpha = \pi_K^{-ps}\beta^t$, the $i = 0$ term in the sum is $-r\alpha\beta$ and the $i = 1$ term is $-\alpha y$. It follows that

$$\alpha y + r\alpha\beta - \wp(r\pi_K^{-s} y^{t+1}) = r\pi_K^{-s} y^{t+1} - r\pi_K^{-ps} \sum_{i=2}^{t+1} \binom{t+1}{i} \beta^{t+1-i} y^i.$$

Since $1 \le t \le p-2$ we get

$$\begin{aligned} v_F\left(r\pi_K^{-ps}\binom{t+1}{2}\beta^{t-1}y^2\right) &= -p^2 s - (t-1)pb - 2b \\ &= -pa + pb - 2b.\end{aligned}$$

Since $a > b$ we have

$$v_F(r\pi_K^{-s} y^{t+1}) = -ps - (t+1)b = -a - b > -pa + pb - 2b.$$

Therefore

$$\begin{aligned} v_F(\alpha y + r\alpha\beta - \wp(r\pi_K^{-s} y^{t+1})) &= v_F\left(r\pi_K^{-ps}\binom{t+1}{2}\beta^{t-1}y^2\right) \\ &= -pa + pb - 2b,\end{aligned}$$

which is not divisible by p. Hence the ramification break of E/F is $2b + p(a-b)$.

Since the upper breaks of the C_p^2-extension M/K are b, a, with $b < a$, the lower breaks of this extension are $b, b + p(a-b)$. By assumption, b is the ramification break of the C_p-subextension F/K of M/K. Hence by Lemma 2.3 the ramification break of M/F is $b + p(a-b)$. Therefore the upper breaks of the C_p^2-extension L/F are $b + p(a-b), 2b + p(a-b)$, and the lower breaks are $b + p(a-b), b + pa$. As noted above, the lower breaks $b, b + p(a-b)$ of M/K are also lower breaks of L/K. Hence the lower breaks of L/K are $b, b + p(a-b), b + pa$. We conclude that the upper ramification breaks of L/K are b, a, and

$$a + p^{-2}((b + pa) - (b + p(a-b))) = a + p^{-1}b. \qquad \square$$

Lemma 5.3. *Let N/K be a totally ramified Galois extension such that $\mathrm{Gal}(N/K)$ is isomorphic to either $H(n,d)$ (with $n \ge 0$ and $d \ge 1$) or $A(n,d)$ (with $n, d \ge 1$). Let $G = \mathrm{Gal}(N/K)$, let H be the unique subgroup of $Z(G)$ of order p, and let $M \subset N$ be the fixed field of H. Then $\mathcal{U}_{N/K} = \mathcal{U}_{M/K} \cup \{v\}$ for some $v \in \mathbb{Q}$ such that $v > w$ for all $w \in \mathcal{U}_{M/K}$. Furthermore, $H = G^v$ is the smallest nontrivial ramification subgroup of G.*

Proof. Let $\sigma \in G$ with $\sigma \notin Z(G)$. Then there is $\tau \in G$ such that $[\sigma,\tau]$ generates $H \cong C_p$. Hence by (2.1), for $\rho \in H$ we have $i(\rho) > i(\sigma)$. Suppose $\sigma \in Z(G)$ but $\sigma \notin H$. Then there is $1 \le i \le d-1$ such that σ^{p^i} generates H. Once again by (2.1) we get $i(\rho) > i(\sigma)$ for all $\rho \in H$. It follows that H is the smallest nontrivial ramification subgroup of G. Therefore $H = G^v$, with v the largest upper ramification break of N/K. Using Theorem 2.1(b) we deduce that $\mathcal{U}_{N/K} = \mathcal{U}_{M/K} \cup \{v\}$. □

We now construct $H(n,d)$-extensions and $A(n,d)$-extensions which have at least one nonintegral upper break.

Proposition 5.4. *Let K be a local field of characteristic $p > 2$ and let $n, d \ge 1$.*

(a) *There is a totally ramified Galois extension L/K such that $\mathrm{Gal}(L/K) \cong H(n,d)$ and the largest upper ramification break of L/K is not an integer.*

(b) *There is a totally ramified Galois extension L/K such that $\mathrm{Gal}(L/K) \cong A(n,d)$ and the largest upper ramification break of L/K is not an integer.*

Proof.

(a) Recall that $H(0,d)$ is the cyclic group of order p^d. By Corollary 3.3 there exists a totally ramified $H(n-1,d)$-extension N_1/K. Let v be the largest upper ramification break of N_1/K and let a, b be integers such that $a > b > v$, $p \nmid b$, and $a \not\equiv 0, -b \pmod p$. Then by Proposition 5.2 there is an $H(1,1)$-extension N_2/K such that $\mathcal{U}_{N_2/K} = \{b, a, a + p^{-1}b\}$. Set $N = N_1N_2$. Since $\mathcal{U}_{N_1/K}$ and $\mathcal{U}_{N_2/K}$ are disjoint we have $\mathcal{U}_{N/K} = \mathcal{U}_{N_1/K} \cup \mathcal{U}_{N_2/K}$, and $N_1 \cap N_2 = K$. It follows that

$$\begin{aligned}\mathrm{Gal}(N/K) &\cong \mathrm{Gal}(N_1/K) \times \mathrm{Gal}(N_2/K)\\ &\cong H(n-1,d) \times H(1,1).\end{aligned}$$

For i=1, 2 let M_i be the subfield of N_i fixed by the unique subgroup of $Z(\mathrm{Gal}(N_i/K))$ with order p. Set $M = M_1M_2$; then $\mathrm{Gal}(N/M) \cong C_p^2$. It follows from Lemma 5.3 that $\mathcal{U}_{N_1/K} = \mathcal{U}_{M_1/K} \cup \{v\}$ and $\mathcal{U}_{N_2/K} = \mathcal{U}_{M_2/K} \cup \{a + p^{-1}b\}$. Since $\mathcal{U}_{M/K} = \mathcal{U}_{M_1/K} \cup \mathcal{U}_{M_2/K}$ this implies $\mathcal{U}_{N/K} = \mathcal{U}_{M/K} \cup \{v, a + p^{-1}b\}$. By Proposition 4.4(a) there is a subgroup $B \le \mathrm{Gal}(N/M)$ such that $\mathrm{Gal}(N/M)/B \cong H(n,d)$. Let $L = N^B$ be the fixed field of B; then L/K is a totally ramified $H(n,d)$-extension. Since

$$\mathrm{Gal}(N_1M_2/K) \cong H(n-1,d) \times C_p^2 \ncong H(n,d),$$

we have $L \ne N_1M_2$. Since $a + p^{-1}b > v$ and v is the largest upper ramification break of N_1M_2/K it follows from Lemma 2.3 that $a + p^{-1}b \notin \mathbb{Z}$ is an upper ramification break of L/K.

(b) If $n \ge 2$ then we proceed as in case (a): Let N_1/K be a totally ramified $A(n-1,d)$-extension whose largest upper ramification break is v. By Proposition 5.2 there is an $H(1,1)$-extension N_2/K such that $\mathcal{U}_{N_2/K} = \{b, a, a+p^{-1}b\}$, with $a > b > v$, $p \nmid b$, and $a \not\equiv 0, -b \pmod p$. Setting $N = N_1N_2$, we get $\mathcal{U}_{N/K} = \mathcal{U}_{N_1/K} \cup \mathcal{U}_{N_2/K}$, $N_1 \cap N_2 = K$, and

$$\begin{aligned}\mathrm{Gal}(N/K) &\cong \mathrm{Gal}(N_1/K) \times \mathrm{Gal}(N_2/K)\\ &\cong A(n-1,d) \times H(1,1).\end{aligned}$$

Defining M_i and M as in the proof of (a) we get $\mathrm{Gal}(N/M) \cong C_p^2$ and $\mathcal{U}_{N/K} = \mathcal{U}_{M/K} \cup \{v, a+p^{-1}b\}$. Hence by Proposition 4.4(b) there is $B \le \mathrm{Gal}(N/M)$ such that $\mathrm{Gal}(N/K)/B \cong A(n,d)$. Setting $L = N^B$ we get $\mathrm{Gal}(L/K) \cong A(n,d)$. Since N_1M_2

is a C_p-extension of M such that v is an upper ramification break of N_1M_2/K, using Lemma 2.3 we deduce that $a + p^{-1}b$ is an upper ramification break of L/K.

It remains to construct an $A(1, d)$-extension with a nonintegral upper ramification break for each $d \geq 1$. By Corollary 3.3 there exists a totally ramified $C_{p^{d+1}}$-extension N_1/K. Let v be the largest upper ramification break of N_1/K and let F/K be the C_p-subextension of N_1/K. Let b be the ramification break of F/K and let a be an integer such that $a > v$ and $a \not\equiv 0, -b \pmod{p}$. Then by Proposition 5.2 there is a totally ramified $H(1, 1)$-extension N_2/K such that $N_1 \cap N_2 = F$ and $\mathcal{U}_{N_2/K} = \{b, a, a + p^{-1}b\}$. Set $N = N_1N_2$. Then

$$\mathrm{Gal}(N/K) \cong \{(\sigma_1, \sigma_2) \in \mathrm{Gal}(N_1/K) \times \mathrm{Gal}(N_2/K) : \sigma_1|_F = \sigma_2|_F\}$$

is isomorphic to the group G_d defined in Proposition 4.5. Let M_1/K be the C_{p^d}-subextension of N_1/K and let M_2/K be the C_p^2-subextension of N_2/K. Then $M_1 \cap M_2 = F$. Set $M = M_1M_2$; then N/M is a C_p^2-extension. By Proposition 4.5 there is a C_p-subextension L/M of N/M such that L/K is a totally ramified $A(1, d)$-extension. On the other hand, N_1M_2/M is a C_p-subextension of N/M such that N_1M_2/K has v as an upper ramification break. Since

$$\mathrm{Gal}(N_1M_2/K) \cong C_{p^{d+1}} \times C_p \ncong A(1, d),$$

we have $L \neq N_1M_2$. Hence by Lemma 2.3 we see that $a + p^{-1}b$ is an upper ramification break of L/K. This completes the proof. □

We now prove the converse of the Hasse-Arf theorem for totally ramified p-extensions.

Theorem 5.5. *Let K be a local field of characteristic $p > 2$ with perfect residue field and let G be a finite nonabelian p-group. Then there is a totally ramified G-extension L/K which has an upper ramification break which is not an integer.*

Proof. By Proposition 4.2 there is a quotient $\overline{G} = G/H$ of G which is isomorphic to either $H(n, d)$ or $A(n, d)$ for some $n, d \geq 1$. By Proposition 5.4 there is a totally ramified $\overline{G}$-extension M/K which has a nonintegral upper ramification break. By Corollary 3.2 there is an extension L/M such that L/K is a totally ramified G-extension. Since $\mathcal{U}_{M/K} \subset \mathcal{U}_{L/K}$ it follows that L/K has a nonintegral upper ramification break. □

6. G-extensions with a nonintegral upper break

Let G be a nonabelian group which is the Galois group of some totally ramified extension of local fields with residue characteristic $p > 2$. In this section we prove the converse to the Hasse-Arf theorem for totally ramified extensions by showing that there exists a totally ramified G-extension of local fields with residue characteristic p which has a nonintegral upper ramification break.

Let K be a local field with perfect residue field of characteristic p and let L/K be a totally ramified Galois extension of degree mp^n, with $p \nmid m$. Set $G = \mathrm{Gal}(L/K)$ and let P be the wild ramification subgroup of G. Then $P \trianglelefteq G$ and $G/P \cong C_m$, so $G \cong P \rtimes_\psi C_m$ for some homomorphism $\psi : C_m \to \mathrm{Aut}(P)$. The following result gives a large class of groups G such that every totally ramified G-extension has a nonintegral upper ramification break.

Proposition 6.1. *Let K be a local field with perfect residue field of characteristic p and let L/K be a totally ramified Galois extension of degree mp^n, with $p \nmid m$. Set $G = \mathrm{Gal}(L/K)$ and write $G \cong P \rtimes_\psi C_m$ as above. If the action of C_m on P is nontrivial then L/K has a nonintegral upper ramification break.*

Proof. Let $\Phi(P)$ be the Frattini subgroup of P and let $M = L^{\Phi(P)}$ be the fixed field of $\Phi(P)$. Then $\Phi(P) \trianglelefteq G$, so M/K is a Galois extension. Set $\overline{P} = P/\Phi(P)$ and let $\overline{\psi} : C_m \to \mathrm{Aut}(\overline{P})$ be the homomorphism induced by ψ. Then $\overline{\psi}$ is nontrivial by a theorem of Burnside (see Theorem 1.4 in Chapter 5 of [8]). Hence

$$\mathrm{Gal}(M/K) \cong G/\Phi(P) \cong \overline{P} \rtimes_{\overline{\psi}} C_m$$

is nonabelian. Since $p \nmid m$, $\overline{P}$ is a direct sum of $\mathbb{F}_p[C_m]$-submodules. Hence there is a simple $\mathbb{F}_p[C_m]$-submodule $W \subset \overline{P}$ on which C_m acts nontrivially. Since W is a direct summand of $\overline{P}$ there is a Galois subextension E/K of M/K such that $\mathrm{Gal}(E/K) \cong W \rtimes C_m$. Let T/K be the maximal tamely ramified subextension of L/K; then $T \subset E$. Since W is a simple $\mathbb{F}_p[C_m]$-module, and the ramification subgroups of $\mathrm{Gal}(E/T)$ are normal in $\mathrm{Gal}(E/K)$, E/T has a unique upper and lower ramification break b.

Let F/T be a C_p-subextension of E/T. Then F/T has upper and lower ramification break b. Hence there is $\alpha \in T$ such that $v_T(\alpha) = -b$ and F is generated over T by the roots of $X^p - X - \alpha$ (see Proposition 2.4 in [6, III]). Let σ be a generator of $\mathrm{Gal}(T/K) \cong C_m$. Since E/K is Galois, the splitting field over T of $X^p - X - \sigma(\alpha)$ is a C_p-subextension of E/T. Hence $X^p - X - (\sigma(\alpha) - \alpha)$ splits over E.

Suppose $m \mid b$. There is a uniformizer π_T of T and a primitive mth root of unity $\zeta \in K$ such that $\sigma(\pi_T) = \zeta\pi_T$. Since $v_T(\alpha) = -b$ there is $c \in \mathcal{O}_K^\times$ such that $\alpha \equiv c\pi_T^{-b} \pmod{\mathcal{M}_T^{-b+1}}$. Hence $v_T(\sigma(\alpha)-\alpha) > -b$. If $X^p-X-(\sigma(\alpha)-\alpha)$ is irreducible over T then the splitting field of this polynomial is a C_p-subextension of E/T whose unique upper ramification break is less than b. Since b is the only upper ramification break of E/T, this is a contradiction. Hence $X^p - X - (\sigma(\alpha) - \alpha)$ splits over T. Extending σ to $\widetilde{\sigma} \in \mathrm{Gal}(E/K)$, we get $\widetilde{\sigma}(F) = F$. It follows by the simplicity of W that $E = F$. Let $\chi_\alpha : \mathrm{Gal}(T^{sep}/T) \to \mathbb{F}_p$ and $\chi_{\sigma(\alpha)} : \mathrm{Gal}(T^{sep}/T) \to \mathbb{F}_p$ be the Galois characters associated to α and $\sigma(\alpha)$ by Artin-Schreier theory. Since $X^p - X - (\sigma(\alpha) - \alpha)$ splits over T we get $\chi_\alpha = \chi_{\sigma(\alpha)}$. It follows that $\widetilde{\sigma}\tau\widetilde{\sigma}^{-1} = \tau$ for every $\tau \in \mathrm{Gal}(E/T)$. This contradicts the nontriviality of the action of C_m on W, so we must have $m \nmid b$.

Since b is a lower ramification break of E/T, it is also a lower ramification break of E/K. Therefore b/m is an upper ramification break of E/K. Hence by Theorem 2.1(b), b/m is a nonintegral upper ramification break of L/K. □

Remark 6.2. Proposition 6.1 could also be proved using Remark 1 in [7].

We now prove our converse of the Hasse-Arf theorem:

Theorem 6.3. *Let k be a perfect field of characteristic $p > 2$. Let E/F be a totally ramified Galois extension of local fields with residue field k and set $G = \mathrm{Gal}(E/F)$. Then there is a local field K with residue field k and a totally ramified G-extension L/K which has a nonintegral upper ramification break.*

Proof. Since E/F is totally ramified, the wild ramification subgroup P of $G = \mathrm{Gal}(E/F)$ is a normal Sylow p-subgroup of G. Furthermore, we have $G \cong P \rtimes_\psi C_m$ for some m with $p \nmid m$ and some $\psi : C_m \to \mathrm{Aut}(P)$. If $\psi(C_m)$ is nontrivial then

it follows from Proposition 6.1 that the totally ramified G-extension E/F has a nonintegral upper ramification break. On the other hand, if $\psi(C_m)$ is trivial then $G \cong P \times C_m$, so P is nonabelian. Set $K = k((t))$. Then by Theorem 5.5 there is a totally ramified P-extension L_1/K which has a nonintegral upper ramification break. Since F has a totally ramified C_m-extension, k contains a primitive mth root of unity ζ_m. Hence there is a totally ramified C_m-extension L_2/K. Set $L = L_1L_2$. Then L/K is a totally ramified G-extension with a nonintegral upper ramification break. □

In many cases the G-extension L/K supplied by Theorem 6.3 is an extension of fields of characteristic p, even when E/F is an extension of fields of characteristic 0. In these cases we can use Deligne's theory of extensions of truncated local rings [4] to get a G-extension of fields of characteristic 0 which satisfies the conclusion of Theorem 6.3. A truncated local ring is defined to be a triple (A, M, ϵ) such that

(i) A is an Artin local ring whose maximal ideal $\mathcal{P}_A$ is principal,
(ii) $A/\mathcal{P}_A$ is a perfect field with positive characteristic,
(iii) M is a free A-module of rank 1,
(iv) $\epsilon : M \to A$ is an A-module homomorphism such that $\epsilon(M) = \mathcal{P}_A$.

One can define morphisms between these objects to get a category $\mathcal{T}$. Let K be a local field and let $d \geq 1$. Define

$$\mathrm{Tr}_d(K) = (\mathcal{O}_K/\mathcal{M}_K^d, \mathcal{M}_K/\mathcal{M}_K^{d+1}, \epsilon),$$

where $\epsilon : \mathcal{M}_K/\mathcal{M}_K^{e+1} \to \mathcal{O}_K/\mathcal{M}_K^e$ is induced by the inclusion $\mathcal{M}_K \hookrightarrow \mathcal{O}_K$. We say that $\mathrm{Tr}_e(K) \in \mathcal{T}$ is the truncation of K to level d.

An extension of truncated local rings is a special type of $\mathcal{T}$-morphism; one can associate upper and lower ramification breaks to these extensions. For $S \in \mathcal{T}$ and $d \geq 1$ there is a category $\mathrm{ext}(S)^d$ whose objects are extensions of S whose largest upper ramification break is less than d. Let $\mathrm{ext}(K)^d$ denote the category of finite separable extensions of K whose largest upper ramification break is less than d.

Theorem 6.4. *Let K be a local field of characteristic 0 with absolute ramification index e. Let k be the residue field of K and set $F = k((t))$. Then there is an equivalence of categories between $\mathrm{ext}(K)^e$ and $\mathrm{ext}(F)^e$. Furthermore, if L/K corresponds to E/F under this equivalence, then L/K and E/F have the same upper and lower ramification breaks.*

Sketch of proof. Let $L/K \in \mathrm{ext}(K)^e$ and let r be the ramification index of L/K. Then the inclusion $K \hookrightarrow L$ induces a $\mathcal{T}$-morphism $f_{L/K} : \mathrm{Tr}_e(K) \to \mathrm{Tr}_{re}(L)$ which is an object in $\mathrm{ext}(\mathrm{Tr}_e(K))^e$. In Théorème 2.8 of [4] it is shown that this construction gives an equivalence of categories from $\mathrm{ext}(K)^e$ to $\mathrm{ext}(\mathrm{Tr}_e(K))^e$. Similarly, there is an equivalence of categories from $\mathrm{ext}(F)^e$ to $\mathrm{ext}(\mathrm{Tr}_e(F))^e$. Both of these equivalences preserve the ramification breaks of extensions. Since $\mathrm{Tr}_e(K) \cong \mathrm{Tr}_e(F)$ it follows that there is an equivalence of categories between $\mathrm{ext}(K)^e$ and $\mathrm{ext}(F)^e$ which preserves ramification breaks. □

Corollary 6.5. *Let k be a perfect field of characteristic $p > 2$. Let G be a finite nonabelian group which is the Galois group of some totally ramified Galois extension of local fields with residue field k. Then there is a local field K of characteristic 0 with residue field k and a totally ramified G-extension L/K which has an upper ramification break which is not an integer.*

Proof. By Theorem 6.3 there is a local field F with residue field k and a totally ramified G-extension E/F which has a nonintegral upper ramification break. If $\mathrm{char}(F) = 0$ there is nothing to prove. If $\mathrm{char}(F) = p$ let $u_{E/F}$ be the largest upper ramification break of E/F. Let K be a local field of characteristic 0 with residue field k whose absolute ramification index $e_K = v_K(p)$ satisfies $e_K > u_{E/F}$. Then it follows from Theorem 6.4 that there is a totally ramified G-extension L/K with the same ramification breaks as E/F. □

Remark 6.6. Let L/K be a totally ramified Galois extension of local fields such that for every totally ramified abelian extension E/K, the upper ramification breaks of LE/K are all integers. In [7] Fesenko proved that $\mathrm{Gal}(L/K)$ must be abelian in this case. This gives a converse to the Hasse-Arf theorem of a different sort than the one presented here.

Remark 6.7. Let K be a local field of characteristic 2 and let L/K be a totally ramified Galois extension whose Galois group is the dihedral group D_4 of order 8. It is shown in [5, 13] that the upper ramification breaks of L/K must be integers. Hence the approach that we use here to prove the converse to the Hasse-Arf theorem by constructing extensions of local fields in characteristic p cannot be extended to the case $p = 2$. When we pass to characteristic 0, however, we find that there are several totally ramified D_4-extensions of $\mathbb{Q}_2$ which have nonintegral upper ramification breaks. For instance, the extension of $\mathbb{Q}_2$ generated by a root of the polynomial $X^8 + 4X^7 + 2X^4 + 4X^2 + 14$ is a D_4-extension whose upper breaks are 1, 2, 5/2 (this is the 2-adic field 2.8.22.83 in [10]). It remains an open question whether the converse to Hasse-Arf holds for totally ramified extensions of local fields with residue characteristic 2.

Remark 6.8. It would be interesting to know for which local fields K the following stronger converse to the Hasse-Arf theorem holds: For every nonabelian group G such that K admits a totally ramified G-extension, there is a totally ramified G-extension L/K which has a nonintegral upper ramification break. It follows from the proof of Theorem 6.3 that this converse to Hasse-Arf holds for local fields of characteristic $p > 2$. On the other hand, Remark 6.7 shows that this converse to Hasse-Arf does not hold for local fields of characteristic 2. Let Q_8 be the quaternion group of order 8. There are four totally ramified Q_8-extensions of the 2-adic field $\mathbb{Q}_2$, each of which has upper ramification breaks $1, 2, 3$ (see [10]). Therefore this converse to Hasse-Arf does not hold for $\mathbb{Q}_2$. As far as we know it is an open question whether this stronger converse to the Hasse-Arf theorem holds for local fields K of characteristic 0 with residue characteristic $p > 2$.

Note: Edit in proof

While this article was in press the authors learned from Victor Abrashkin that some of the results presented here could be proved more easily in the finite residue field case using his paper "A ramification filtration of the Galois group of a local field" [1]. The results in that paper and its sequels should allow one to say much more about the possibilities for upper ramification sequences.

References

[1] Victor A. Abrashkin, *A ramification filtration of the Galois group of a local field*, Proceedings of the St. Petersburg Mathematical Society, Vol. III, Amer. Math. Soc. Transl. Ser. 2, vol. 166, Amer. Math. Soc., Providence, RI, 1995, pp. 35–100, DOI 10.1090/trans2/166/02. MR1363291

[2] Cahit Arf, *Untersuchungen über reinverzweigte Erweiterungen diskret bewerteter perfekter Körper* (German), J. Reine Angew. Math. **181** (1939), 1–44, DOI 10.1515/crll.1940.181.1. MR018

[3] Emil Artin, *Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper* (German), J. Reine Angew. Math. **164** (1931), 1–11, DOI 10.1515/crll.1931.164.1. MR1581245

[4] Pierre Deligne, *Les corps locaux de caractéristique p, limites de corps locaux de caractéristique* 0 (French), Representations of reductive groups over a local field, Travaux en Cours, Hermann, Paris, 1984, pp. 119–157. MR771673

[5] Gove Griffith Elder, *Upper ramification sequences of nonabelian extensions of degree p^3 in characteristic p*, Preprint, `arXiv:2303.01984`, 2023.

[6] Ivan B. Fesenko and Sergeĭ V. Vostokov, *Local fields and their extensions*, 2nd ed., Translations of Mathematical Monographs, vol. 121, American Mathematical Society, Providence, RI, 2002. With a foreword by I. R. Shafarevich, DOI 10.1090/mmono/121. MR1915966

[7] Ivan B. Fesenko, *Hasse-Arf property and abelian extensions*, Math. Nachr. **174** (1995), 81–87, DOI 10.1002/mana.19951740108. MR1349039

[8] Daniel Gorenstein, *Finite groups*, 2nd ed., Chelsea Publishing Co., New York, 1980. MR569209

[9] Helmut Hasse, *Führer, Diskriminante und Verzweigungskörper relativ-Abelscher Zahlkörper* (German), J. Reine Angew. Math. **162** (1930), 169–184, DOI 10.1515/crll.1930.162.169. MR1581221

[10] The LMFDB Collaboration, *The L-functions and modular forms database*, `https://www.lmfdb.org`, 2023 [Online; accessed 10 July 2023].

[11] Jonathan Lubin, *The local Kronecker-Weber theorem*, Trans. Amer. Math. Soc. **267** (1981), no. 1, 133–138, DOI 10.2307/1998574. MR621978

[12] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. MR554237

[13] Bradley Weaver, *The local lifting problem for D_4*, Israel J. Math. **228** (2018), no. 2, 587–626, DOI 10.1007/s11856-018-1782-1. MR3874854

[14] Ernst Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f* (German), J. Reine Angew. Math. **174** (1936), 237–245, DOI 10.1515/crll.1936.174.237. MR1581489

Department of Mathematics, University of Nebraska Omaha, Omaha, Nebraska 68182
Email address: `elder@unomaha.edu`

Department of Mathematics, University of Florida, Gainesville, Florida 32611
Email address: `keating@ufl.edu`