A Converse to the Hasse-Arf Theorem

Kevin Keating
Department of Mathematics
University of Florida

June 1, 2022

This is joint work with

G. Griffith Elder — University of Nebraska Omaha

Notation for local fields

Let K be a local field. Then K is complete with respect to a discrete valuation $v_K : K \to \mathbb{Z} \cup \{\infty\}$.

Associated to K we have the following:

$$\begin{aligned}\mathcal{O}_K &= \{x \in K : v_K(x) \geq 0\} = \text{ring of integers of } K \\ \mathcal{M}_K &= \{x \in K : v_K(x) \geq 1\} = \text{maximal ideal of } \mathcal{O}_K \\ \overline{K} &= \mathcal{O}_K/\mathcal{M}_K = \text{residue field of } K.\end{aligned}$$

Say that $\pi_K \in K$ is a uniformizer for K if $v_K(\pi_K) = 1$.

We will be considering finite Galois extensions L/K of local fields of degree n.

We will often assume that L/K is totally ramified. This means that $\overline{L} = \overline{K}$, or equivalently that $|\mathbb{Z} : v_L(K^\times)| = n$.

Higher ramification theory

Let L/K be a finite Galois extension, and set $G = \mathrm{Gal}(L/K)$. For $x \in \mathbb{R}$ with $x \geq -1$ define

$$G_x = \{\sigma \in G : v_L(\sigma(\alpha) - \alpha) \geq x + 1 \text{ for all } \alpha \in \mathcal{O}_L\}.$$

Then G_x is a subgroup of G. In fact $G_x \trianglelefteq G$.

Let $b \in \mathbb{R}$, $b \geq -1$. Say b is a lower ramification break of L/K if $G_b \neq G_{b+\epsilon}$ for all $\epsilon > 0$. We have $b \in \mathbb{Z}$ in this case.

If b is a positive lower ramification break of L/K then we can identify G_b/G_{b+1} with a subgroup of $\mathcal{M}_L^b/\mathcal{M}_L^{b+1}$. Hence G_b/G_{b+1} is an elementary abelian p-group.

We define the multiplicity of the lower break b to be the $\mathbb{F}_p$-dimension of G_b/G_{b+1}.

Suppose L/K is a totally ramified Galois extension of degree $n = ap^\nu$, with $p \nmid a$. Then the positive lower breaks of L/K, counted with multiplicity, form a nondecreasing sequence $b_1 \leq b_2 \leq \cdots \leq b_\nu$ of integers.

Ramification subgroups with the upper numbering

Let $G = \mathrm{Gal}(L/K)$ and $H \leq G$. Then for $x \geq -1$ we have $H_x = H \cap G_x$.

Suppose $H \trianglelefteq G$. How to determine $(G/H)_x$?

Define a function $\phi_{L/K} : \mathbb{R}_{\geq -1} \to \mathbb{R}_{\geq -1}$ by

$$\phi_{L/K}(x) = \int_0^x \frac{dt}{|G_0 : G_t|}.$$

Then $\phi_{L/K}$ is one-to-one and onto, so we may define $\psi_{L/K} : \mathbb{R}_{\geq -1} \to \mathbb{R}_{\geq -1}$ by $\psi_{L/K} = \phi_{L/K}^{-1}$.

Define the upper numbering on the higher ramification groups of L/K by $G^x = G_{\psi_{L/K}(x)}$ for $x \geq -1$. Then

$$\psi_{L/K}(x) = \int_0^x |G^0 : G^t| \, dt.$$

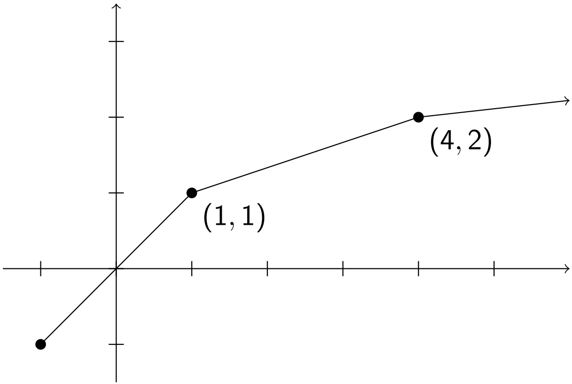
Say that $u \geq -1$ is an upper ramification break of L/K if $G^u \neq G^{u+\epsilon}$ for all $\epsilon > 0$. This is equivalent to $\psi_{L/K}(u)$ being a lower ramification break.

An example

Let L be the extension of $\mathbb{Q}_3$ generated by a root of

$$X^9 + 9X^7 + 3X^6 + 18X^5 + 51.$$

Using [JoRo] we find that $L/\mathbb{Q}_3$ is a totally ramified C_9-extension with lower ramification breaks $b_1 = 1$ and $b_2 = 4$. Therefore the Hasse-Herbrand function $\phi_{L/\mathbb{Q}_3}(x)$ has the following graph:



Herbrand's Theorem

Theorem (Herbrand)

Let L/K be a totally ramified Galois extension and let M/K be a Galois subextension of L/K. Set $G = Gal(L/K)$ and $H = Gal(L/M)$. Then for $x \geq 0$ we have

- $(G/H)_x = G_{\psi_{L/M}(x)}H/H$
- $(G/H)^x = G^x H/H.$

We may assign multiplicities to the upper ramification breaks of L/K just as we did for the lower breaks. We denote the multiset of upper ramification breaks of L/K by $\mathcal{U}_{L/K}$.

It follows from Herbrand's theorem that $\mathcal{U}_{M/K} \subset \mathcal{U}_{L/K}$.

The Hasse-Arf Theorem

The following was proved by Hasse [Ha30] under the assumption that the residue field $\overline{K}$ is finite, and by Arf [Ar39] for $\overline{K}$ an arbitrary perfect field.

Theorem (Hasse-Arf)

Let L/K be a finite abelian extension of local fields. Then the upper ramification breaks of L/K are integers.

Let L/K be a totally ramified abelian extension of degree ap^ν, with $p \nmid a$, and let $b_1 \leq b_2 \leq \cdots \leq b_\nu$ be the positive lower ramification breaks of L/K. Then the Hasse-Arf theorem for L/K is equivalent to the statement that $b_{i+1} \equiv b_i \pmod{ap^i}$ for $1 \leq i \leq n-1$.

Applications of the Hasse-Arf theorem

- Relation between local class field theory and ramification subgroups: Suppose $\overline{K}$ is finite and L/K is an abelian extension. Then local class field theory gives an onto homomorphism $\omega_{L/K} : K^\times \to G$, with $G = \mathrm{Gal}(L/K)$. For $x > 0$ define $U_K^x = \{\alpha \in \mathcal{O}_K : v_K(\alpha - 1) \geq x\}$. Then for $x > 0$ we have $\omega_{L/K}(U_K^x) = G^x$.
- Lubin's proof of the local Kronecker-Weber theorem: Let $F(X, Y)$ be a Lubin-Tate formal group law over $\mathcal{O}_K$, and let M be the extension generated by the union of the torsion points of $[\pi_K^r]_F(X)$ for all $r \geq 1$. Then M is a maximal totally ramified abelian extension of K.
- The existence of the Artin representation of a finite Galois extension L/K of local fields is proved using the Hasse-Arf theorem. Hence the Artin conductor depends on the Hasse-Arf theorem.

Converse to the Hasse-Arf theorem

Theorem

Let $p > 2$ and let G be a nonabelian group which is the Galois group of some totally ramified finite Galois extension E/F of local fields with residue characteristic p. Then there exists a local field K with residue characteristic p and a totally ramified G-extension L/K such that L/K has a nonintegral upper ramification break.

In fact the groups G we must consider are of the form $G = P \rtimes C_a$, where P is a finite p-group and C_a is a cyclic group whose order a is relatively prime to p.

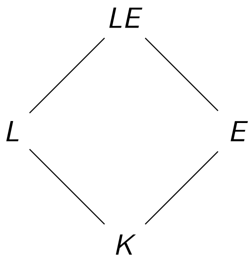
Let $\overline{K}$ be a perfect field of characteristic $p > 2$ and set $K = \overline{K}((t))$. We show that for each group $G = P \rtimes C_a$ there exists a totally ramified G-extension L/K which has a nonintegral upper ramification break.

One can get a totally ramified G-extension L'/K' in characteristic 0 with the same ramification data as L/K with the help of [De84].

A different converse to Hasse-Arf

Let L/K be a totally ramified abelian extension. It follows from the Hasse-Arf theorem that for every finite totally ramified abelian extension E/K, the upper ramification breaks of LE/K are all integers.

In [Fe95] Fesenko proved the converse to this statement:



Theorem (Fesenko)

Let L/K be a finite totally ramified Galois extension of local fields such that for every finite totally ramified abelian extension E/F, the upper ramification breaks of LE/K are all integers. Then $Gal(L/K)$ is abelian.

Fesenko's converse to Hasse-Arf gives information about a specific extension L/K, whereas ours gives information about a group G.

In both cases, knowing that the upper ramification breaks of infinitely many extensions are integers implies that a certain group is abelian.

Proving the theorem

As mentioned earlier, we can assume that G is a nonabelian group of the form $G = P \rtimes C_m$ for some finite p-group G and some a with $p \nmid a$.

We will focus on the case where $a = 1$ and $G = P$ is a p-group. The proof for $a > 1$ uses different arguments, at least when C_a acts nontrivially on P.

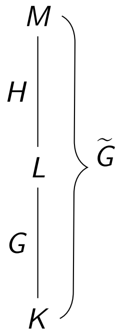
Given a local field K of characteristic $p > 2$ and a nonabelian p-group G, we wish to show that there exists a totally ramified G-extension L/K which has a nonintegral upper ramification break.

Embedding problems

Let L/K be a finite Galois extension and set $G = \mathrm{Gal}(L/K)$. Let $\widetilde{G}$ be an extension of G by a finite group H.

Let M/L be a finite extension. We say that M solves the embedding problem associated to L/K and $\widetilde{G}$ if M/K is Galois and there is an isomorphism of short exact sequences

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



Witt [Wi36] proved the following:

Theorem (Witt)

Let K be a local field of characteristic p and let L/K be a finite totally ramified Galois extension with Galois group G. Let $\widetilde{G}$ be an extension of G by a finite p-group H. Then the embedding problem associated to L/K and $\widetilde{G}$ has a solution M/L such that M/K is totally ramified.

Minimal nonabelian p-groups

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

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:

- *G is nilpotent of class 2.*
- *$Z(G)$ is cyclic of order p^d for some $d \geq 1$.*
- *$[G, G]$ is the subgroup of $Z(G)$ of order p.*
- *$G/Z(G)$ 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 on $G/Z(G)$ with values in $[G, G]$.*

Group theorists call these "groups of symplectic type" (see [Th68], [Go80]). But they don't state that these groups are $\preccurlyeq$-minimal.

Explicit descriptions of minimal nonabelian p-groups

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 $1 \leq i \leq n$. Thus $H(1, 1)$ is the Heisenberg p-group, and $H(n, 1)$ is an extraspecial p-group. $H(n, d)$ is a central product of $H(n, 1)$ with C_{p^d}.

We define another group $A(n, d)$ of order p^{2n+d} generated by $x_1, \ldots, x_n, y_1, \ldots, y_n, z$. In $A(n, d)$ we have $|x_i| = p$ for $2 \leq i \leq n$, $|y_i| = p$ for $1 \leq i \leq n$, 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 $1 \leq i \leq n$. Thus $A(1, 1)$ is the metacyclic group of order p^3, and $A(n, 1)$ is an extraspecial p-group. $A(n, d)$ is a central product of $A(n, 1)$ with C_{p^d}.

Proposition

Let $p > 2$. Then G is a minimal nonabelian p-group if and only if either $G \cong H(n, d)$ or $G \cong A(n, d)$ for some $n, d \geq 1$.

What we need to prove

It follows from Witt's theorem and the classification of minimal nonabelian p-groups that to prove the converse to Hasse-Arf for totally ramified p-extensions it suffices to prove the following:

Theorem

Let $\overline{K}$ be a perfect field of characteristic $p > 2$ and set $K = \overline{K}((t))$. Then for every $n, d \geq 1$ there exists an $H(n, d)$-extension L/K which has a nonintegral upper ramification break, and an $A(n, d)$-extension M/K which has a nonintegral upper ramification break.

We will focus on proving the existence of an $H(n, d)$-extension which has a nonintegral upper break.

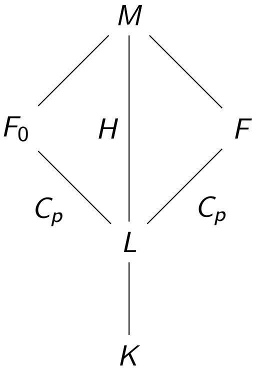
Big Break Rule

Proposition

Let L be a local field such that $\mathrm{char}(\overline{L}) = p$ and let M/L be a totally ramified C_p^2-extension with upper ramification breaks $x < y$. Then there is a unique C_p-subextension F_0/L with upper break x; all other C_p-subextensions F/L of M/L have upper break y.

Corollary

Let M/K be a totally ramified Galois extension of local fields and set $G = Gal(M/K)$. Let $H \leq Z(G)$ satisfy $H \cong C_p^2$ and set $L = M^H$. Assume that M/K has upper ramification breaks $u < v$ with multiplicity 1 such that $\mathcal{U}_{M/K} = \mathcal{U}_{L/K} \cup \{u, v\}$. Then there is a unique C_p-subextension F_0/L such that $\mathcal{U}_{F_0/K} = \mathcal{U}_{L/K} \cup \{u\}$; for all other C_p-subextensions F/L of M/L we have $\mathcal{U}_{F/K} = \mathcal{U}_{L/K} \cup \{v\}$.



A toehold and a bootstrap

In 2019, Griff Elder proved the following in his Omaha talk:

Proposition (Toehold)

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

This is useful in conjunction with the following:

Proposition (Bootstrap)

Let $n, d \geq 1$. Then $H(n,d)$ is a central product of $H(n-1,d)$ and $H(1,1)$. More precisely,

$$H(n,d) \cong (H(n-1,d) \times H(1,1))/B$$

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

Constructing an $(H(n-1,d) \times H(1,1))$-extension

Let N_1/K be a totally ramified $H(n-1,d)$-extension and let v be the largest upper ramification break of N_1/K. Let b, c be integers such that $c > b > v$, $p \nmid b$, and $c \not\equiv 0, -b \pmod{p}$. Then by the Toehold there is an $H(1,1)$-extension N_2/K such that $\mathcal{U}_{N_2/K} = \{b, c, c + p^{-1}b\}$.

Set $N = N_1 N_2$. Since $\mathcal{U}_{N_1/K}$ and $\mathcal{U}_{N_2/K}$ are disjoint we have $N_1 \cap N_2 = K$ and $\mathcal{U}_{N/K} = \mathcal{U}_{N_1/K} \cup \mathcal{U}_{N_2/K}$. 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 commutator of $\mathrm{Gal}(N_i/K)$. Then $\mathrm{Gal}(N_i/M_i) \cong C_p$. Set $M = M_1 M_2$; then $\mathrm{Gal}(N/M) \cong C_p^2$.

Since $\mathrm{Gal}(N_i/M_i)$ is contained in every nontrivial normal subgroup of $\mathrm{Gal}(N_i/K)$, $\mathrm{Gal}(N_i/M_i)$ is the smallest nontrivial ramification subgroup of $\mathrm{Gal}(N_i/K)$. Therefore $\mathcal{U}_{M_1/K} = \mathcal{U}_{N_1/K} \smallsetminus \{v\}$ and $\mathcal{U}_{M_2/K} = \{b, c\}$.

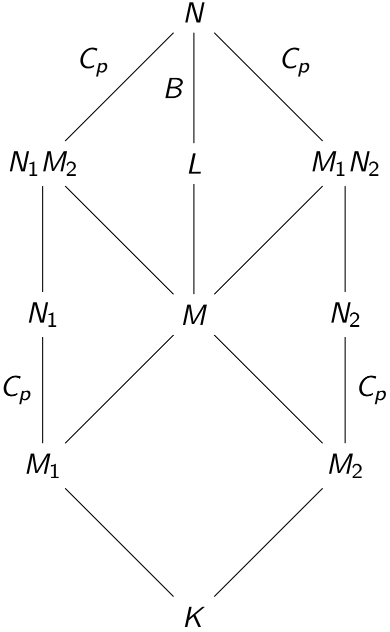
Constructing an $H(n,d)$-extension

It follows from the preceding slide that $\mathcal{U}_{N/K} = \mathcal{U}_{M/K} \cup \{v, c + p^{-1}b\}$ and $\mathcal{U}_{N_1M_2/K} = \mathcal{U}_{M/K} \cup \{v\}$.

By the Bootstrap there is a subgroup $B \leq \mathrm{Gal}(N/M)$ such that $\mathrm{Gal}(N/K)/B \cong H(n,d)$. Let $L = N^B$ be the fixed field of B; then L/K is an $H(n,d)$-extension. By construction we have $L \neq N_1M_2$.

Since $c + p^{-1}b > v$ and v is the largest upper ramification break of N_1M_2/K it follows from the Big Break Rule that $c + p^{-1}b$ is an upper ramification break of L/K.

And of course, $c + p^{-1}b \notin \mathbb{Z}$.



What about $p = 2$?

If $p = 2$ our proof breaks down in two places.

First, our classification of minimal nonabelian p-groups is invalid for $p = 2$. However, with a little more work it should be possible to carry out this classification.

Second, if K is a local field of characteristic 2 and L/K is a totally ramified D_4-extension then the upper ramification breaks of L/K must be integers. Therefore our approach to proving the converse to Hasse-Arf based on constructing extensions in characteristic p fails in characteristic 2.

However, in the Database of Local Fields [JoRo] there are eight D_4-extensions of $\mathbb{Q}_2$ which have nonintegral upper ramification breaks. So the converse to Hasse-Arf may be valid for $p = 2$.

What about extensions which are not totally ramified?

The Hasse-Arf theorem applies to arbitrary abelian extensions of local fields, not just to totally ramified extensions.

Ideally, a converse to the Hasse-Arf theorem would apply to any group which is a Galois group for an extension of local fields with residue characteristic p. However ...

Example

Let $p > 2$ and let F be a local field whose residue field is $\mathbb{F}_p$. Let E be the splitting field of $X^{p+1} - \pi_F$. Then E/F is a Galois extension with $\mathrm{Gal}(E/F) \cong D_{p+1}$, a nonabelian group. If L/K is a D_{p+1}-extension of local fields with residue characteristic p then L/K is (at most) tamely ramified. Therefore the only possible upper ramification breaks of L/K are the integers $-1, 0$.

A Better Version?

It would be nice to know the answer to the following question: Let K be a local field with residue characteristic p and let L/K be a finite totally ramified Galois extension with nonabelian Galois group G. Must there exist a totally ramified G-extension L'/K which has a nonintegral upper ramification break?

If $\mathrm{char}(K) = p > 2$ then the answer is yes.

If $\mathrm{char}(K) = 2$ then the answer is no.

If $\mathrm{char}(K) = 0$ then the answer is ??

References

[Ar39] C. Arf, Untersuchungen über reinverzweigte Erweiterungen diskret bewerteter perfekter Körper, J. Reine Angew. Math. **181** (1939), 1–44.

[De84] P. Deligne, *Les corps locaux de caractéristique p, limites de corps locaux de caractéristique* 0, appearing in *Representations of reductive groups over a local field*, Hermann, Paris, 1984, 119–157.

[Fe95] I. B. Fesenko, Hasse-Arf property and abelian extensions, Math. Nachr. **174** (1995), 81–87.

[Go80] D. Gorenstein, *Finite groups*, Second edition, Chelsea, New York, 1980.

[Ha30] H. Hasse, Führer, Diskriminante und Verzweigungskörper relativ-Abelscher Zahlkörper, J. Reine Angew. Math. **162** (1930), 169–184.

[JoRo] J. Jones and D. Roberts, Database of Local Fields, `https://math.la.asu.edu/~jj/localfields/`

[Th68] J. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable, Bull. Amer. Math. Soc. **74** (1968), 383–437.

Another reference

[Wi36] E. Witt, Konstruktion von galoisschen Körpen der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f, J. Reine Angew. Math. **174** (1936), 237–245.