The Hasse-Arf Theorem and Nonabelian Extensions

Kevin Keating
Department of Mathematics
University of Florida

May 27, 2021

This is joint work with

G. Griffith Elder — University of Nebraska Omaha

Notation for Local Fields

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

Associated to K we have the following:

$$\mathcal{O}_K = \{x \in K : v_K(x) \geq 0\} = \text{ring of integers of } K$$

$$\mathcal{M}_K = \{x \in K : v_K(x) \geq 1\} = \text{maximal ideal of } \mathcal{O}_K.$$

Say that $\overline{K} = \mathcal{O}_K/\mathcal{M}_K$ is the residue field of K. A uniformizer of K is $\pi_K \in K$ such that $v_K(\pi_K) = 1$.

We will be considering Galois extensions L/K of degree p^n, where $p = \text{char}(\overline{K})$.

In most cases we will assume that L/K is totally ramified. When this holds we have $\overline{L} = \overline{K}$ and $|\mathbb{Z} : v_L(K^\times)| = p^n$. In addition, we choose π_L so that $\text{N}_{L/K}(\pi_L) \equiv \pi_K \pmod{\mathcal{M}_K^2}$.

Higher Ramification Theory

Let L/K be a Galois extension of degree p^n. For $x \in \mathbb{R}$ with $x \geq 0$ 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 $b \in \mathbb{R}$, $b \geq 0$. 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 lower ramification break of L/K 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}.

Thus the lower breaks of L/K form a nondecreasing sequence $b_1 \leq b_2 \leq \cdots \leq b_n$ of integers.

Even Higher Ramification

Let $H \leq G$ and set $M = L^H$. Then for $x \geq 0$ we get $H_x = H \cap G_x$.

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

Define a function $\phi_{L/K} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ 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 $\psi_{L/K} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ 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 $x \geq 0$. Then we get

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

Say $u \geq 0$ 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.

Herbrand's Theorem

Theorem

Let M/K be a Galois subextension of L/K. Set $G = Gal(L/K)$ and $H = Gal(L/M)$.

- *(Herbrand's Theorem) For $y \geq 0$ we have $(G/H)^y = G^y H/H$.*
- *(Tower Rule) Let M/K be a Galois subextension of L/K. Then $\phi_{L/K} = \phi_{M/K} \circ \phi_{L/M}$ and $\psi_{L/K} = \psi_{L/M} \circ \psi_{M/K}$.*

It follows from Herbrand's theorem that if u is an upper ramification break of M/K then u is also an upper ramification break of L/K.

Let $H \trianglelefteq G$ and set $M = L^H$. Let $x \geq 0$ and set $y = \phi_{M/K}(x)$. By the tower rule we get

$$\psi_{L/K}(y) = \psi_{L/M}(\psi_{M/K}(y)) = \psi_{L/M}(x).$$

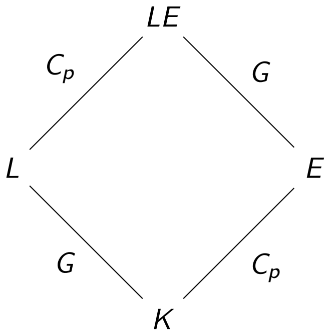
Hence by Herbrand's Theorem we deduce that

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

A Ramification Theory Lemma

Lemma

Let L/K be a Galois extension of degree p^n and set $G = Gal(L/K)$. Let E/K be a C_p-extension such that $[LE : L] = [E : K] = p$. Let v be the ramification break of E/K and let v' be the ramification break of LE/L. Then $v' \leq \psi_{L/K}(v)$, with equality if v is not an upper ramification break of L/K.



The Hasse-Arf Theorem

Theorem (Hasse-Arf)

Let L/K be an abelian extension. Then the upper ramification breaks of L/K are integers.

Suppose $\overline{K}$ is finite and L/K is an abelian extension. Then local class field theory gives an onto homomorphism $\omega_{L/K} : K^\times \to G = \mathrm{Gal}(L/K)$.

For $x > 0$ define

$$U_K^x = \{\alpha \in \mathcal{O}_K : v_K(\alpha - 1) \geq x\}.$$

Then for $x > 0$ we have $\omega_{L/K}(U_K^x) = G^x$.

A Question

Let G be a group of order p^n and let

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_{n-1} \leq G_n = G$$

be normal subgroups of G such that $|G_i| = p^i$ for $0 \leq i \leq n$.

Consider the set of all totally ramified Galois extensions L/K with $\mathrm{Gal}(L/K) \cong G$ such that every ramification subgroup of $\mathrm{Gal}(L/K)$ is equal to G_i for some i.

We get a tower of fields $L_0 \subset L_1 \subset \cdots \subset L_n$, with $L_i = L^{G_{n-i}}$.

Question: What are the possibilities for the upper ramification breaks $u_1 \leq u_2 \leq \cdots \leq u_n$ of such extensions?

Miki and Maus determined the possibilities for the upper breaks when $G = C_{p^n}$ is cyclic.

Embedding Problems

Let L/K be a totally ramified Galois extension whose Galois group $G = \mathrm{Gal}(L/K)$ has order p^n.

Let $\widetilde{G}$ be an extension of the group G by C_p, and let M_1, M_2 be two field extensions of L which solve the associated embedding problem.

Thus for $i = 1, 2$, M_i/K is a Galois extension and there is an isomorphism of exact sequences

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

Sets of Upper Breaks

Let $e_K = v_K(p)$ denote the absolute ramification index of K; thus $e_K = \infty$ if $\mathrm{char}(K) = p$. Set

$$B'_K = \left\{ b \in \mathbb{N} : b < \frac{pe_K}{p-1},\ p \nmid b \right\}.$$

Let B_K denote the set of all possible ramification breaks of C_p-extensions E/K.

If K does not contain a primitive pth root of unity then

$$B_K = B'_K \cup \{-1\},$$

while if K does contain a primitive pth root of unity then

$$B_K = B'_K \cup \left\{ -1, \frac{pe_K}{p-1} \right\}.$$

In particular, if $\mathrm{char}(K) = p$ then $B_K = \{b \in \mathbb{N} : p \nmid b\} \cup \{-1\}$.

Main Theorem

Theorem

Let $b^{(i)}$ be the unique (upper and lower) ramification break of M_i/L. Then $b^{(i)}$ is a lower break of M_i/K, so we may let $u^{(i)} = \phi_{M_i/K}(b^{(i)}) = \phi_{L/K}(b^{(i)})$ be the corresponding upper ramification break of M_i/K. Assume that

- *$u^{(i)}$ is the largest upper ramification break of M_i/K for $i = 1, 2$.*
- *$u^{(1)} \notin B_K$.*

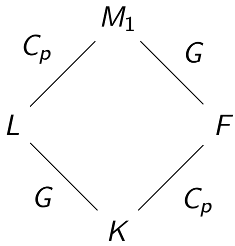
Then $u^{(2)} \geq u^{(1)}$.

Some consequences:

- If $u^{(2)} > u^{(1)}$ then $u^{(2)} \in B_K$. In particular, if $u^{(2)} > u^{(1)}$ then $u^{(2)}$ is an integer.
- Suppose $\mathrm{char}(K) = p$. Then there are finitely many solutions M_1/K to the embedding problem such that $u^{(1)}$ is not an integer, and infinitely many solutions such that $u^{(1)}$ is an integer.

Proof of Main Theorem (First Step)

We first note that if the extension $\widetilde{G}$ of G by C_p is split then there is a Galois extension F/K with $\mathrm{Gal}(F/K) \cong C_p$ such that $LF = M_1$ and $L \cap F = K$.



Let $v \in B_K$ be the ramification break of F/K. Then v is an upper ramification break of M_1/K, so we have $v \leq u^{(1)}$.

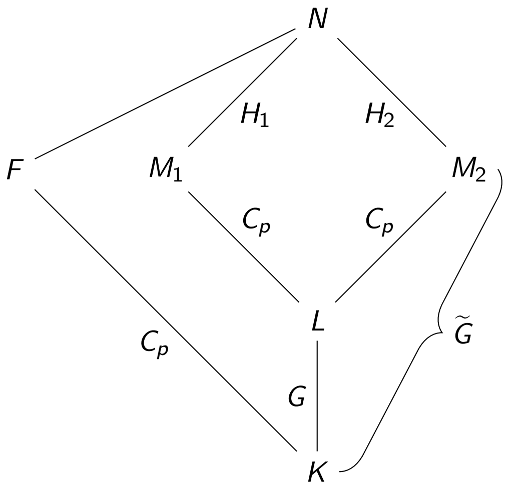
By the lemma we have $b^{(1)} \leq \psi_{L/K}(v)$, and hence $u^{(1)} = \phi_{L/K}(b^{(1)}) \leq v$.

It follows that $u^{(1)} = v \in B_K$, a contradiction.

Therefore $\widetilde{G}$ is a nonsplit extension of G by C_p.

Proof of Main Theorem (continued)

Let $N = M_1 M_2$. Then N/K is Galois. Set $\Gamma = \mathrm{Gal}(N/K)$ and $H_i = \mathrm{Gal}(N/M_i)$ for $i = 1, 2$. Then $\Gamma/H_i \cong \mathrm{Gal}(M_i/K)$ and $\Gamma/H_1 H_2 \cong \mathrm{Gal}(L/K) = G$.



A Bit of Group Theory

It follows from (1) that there is an isomorphism $\psi : \Gamma/H_1 \to \Gamma/H_2$ which induces the identity on Γ/H_1H_2.

Hence for $x \in \Gamma$ there is unique $\delta(x) \in H_1$ such that $\psi(xH_1) = x\delta(x)H_2$.

Let $x, y \in \Gamma$. Since H_1 is contained in the center of the p-group Γ we get

$$\begin{aligned} \psi(xyH_1) &= \psi(xH_1)\psi(yH_1) \\ &= x\delta(x)H_2 \cdot y\delta(y)H_2 \\ &= xy\delta(x)\delta(y)H_2. \end{aligned}$$

Hence $\delta(xy) = \delta(x)\delta(y)$, so $\delta : \Gamma \to H_1$ is a homomorphism.

If $x \in H_1$ then $\delta(x) = x^{-1}$. Therefore $H_1 \not\subset \ker(\delta)$. It follows that δ is nontrivial, and hence onto.

Therefore $\ker(\delta)$ is a normal subgroup of Γ with index p.

Proof of the Main Theorem (continued)

Let F be the subfield of N fixed by $\ker(\delta)$.

Then $\mathrm{Gal}(F/K) \cong C_p$, Also, $M_iF = N$ and $M_i \cap F = K$ for $i = 1, 2$.

Let $v \in \mathbb{N}$ be the unique (upper and lower) ramification break of F/K.

Suppose $v > u^{(1)}$. Then by the maximality of $u^{(1)}$ we see that v is not an upper ramification break of L/K.

By the lemma we deduce that $\psi_{L/K}(v)$ is an upper break of LF/L.

Therefore the (distinct) upper breaks of N/L are $\psi_{L/K}(v)$ and $b^{(1)} = \psi_{L/K}(u^{(1)})$.

Since $\psi_{L/K}(v) > \psi_{L/K}(u^{(1)})$ and $M_2 \neq M_1$, the upper break of M_2/L is $\psi_{L/K}(v)$. Hence $u^{(2)} = v > u^{(1)}$.

Completing the Proof of the Main Theorem

Suppose $v \leq u^{(1)}$. Then $v < u^{(1)}$ since $u^{(1)} \notin B_K$.

Hence by the lemma the upper ramification break of LF/L is less than $\psi_{L/K}(u^{(1)}) = b^{(1)}$.

It follows that the ramification break of M_2/L is $b^{(1)}$, so we get $u^{(2)} = \phi_{L/K}(b^{(1)}) = u^{(1)}$.

An Example

Let K be a local field of characteristic p and let L/K be a totally ramified cyclic extension of degree $p-1$.

Let π_L, π_K be uniformizers for K, L such that $\pi_L^{p-1} = \pi_K$.

Let $d > 0$ with $p \nmid d$ and let M_d be the extension of L generated by the roots of $X^p - X - \pi_L^{-d}$.

Then M_d/K is a Galois extension of degree $p(p-1)$ with upper ramification breaks $0, d/(p-1)$.

Therefore the hypothesis that G is a p-group in our main Theorem is necessary.

Another Theorem

Theorem

Let K be a local field and let L/K be a finite totally ramified Galois extension of degree p^n. Assume that $G = Gal(L/K)$ has order p^n and let $\widetilde{G}$ be an extension of G by C_p. Let M/L be a C_p-extension which solves the embedding problem associated to this group extension. Let w be the ramification break of M/L and let $v = \phi_{M/K}(w) = \phi_{L/K}(w)$ be the upper ramification break of M/K that is associated to w. Assume that

- *w is the smallest ramification break associated to a solution of the embedding problem.*
- *v is not an upper ramification break of L/K.*

Then

$$v \notin B'_K = \left\{ b \in \mathbb{N} : b < \frac{pe_K}{p-1}, \, p \nmid b \right\}.$$

An Invariant for C_p-extensions

Let E/K be a ramified C_p-extension with ramification break b. Let v be an integer with $v \leq b$ and let $\sigma \in \mathrm{Gal}(L/K)$. We define an invariant $\lambda_v(E/K, \sigma) \in \overline{K}$ as follows:

Let π_E be a uniformizer for E such that $\mathrm{N}_{E/K}(\pi_E) \equiv \pi_K \pmod{\mathcal{M}_K}$. Then there is $c \in \mathcal{O}_K$ such that

$$\sigma(\pi_E) \equiv \pi_E + c\pi_E^{v+1} \pmod{\mathcal{M}_E^{v+2}}.$$

Define $\lambda_v(E/K, \sigma) = c + \mathcal{M}_K \in \mathcal{O}_K/\mathcal{M}_K = \overline{K}$. Then $\lambda_v(E/K, \sigma)$ does not depend on the choices of π_E and c.

Proposition

Let $v \in B'_K$ and $c \in \overline{K}$. Then there is a ramified C_p-extension E/K with ramification break $b \geq v$ and a generator σ for Gal(E/K) such that $\lambda_v(E/K, \sigma) = c$.

Proof: Artin-Schreier plus MacKenzie-Whaples.

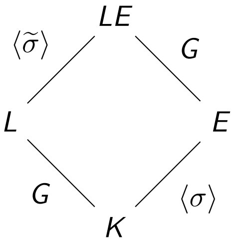
Shifting a C_p-extension

Recall that L/K is a totally ramified Galois extension of degree p^n, with $G = \mathrm{Gal}(L/K)$.

Let $v \in B'_K$ be such that v is not an upper ramification break of L/K and set $w = \psi_{L/K}(v)$.

Let E/K be a C_p-extension with ramification break v. Then LE/L is a C_p-extension with ramification break w (by the lemma).

Let σ be a generator for $\mathrm{Gal}(E/K)$ and let $\widetilde{\sigma}$ be the unique element of $\mathrm{Gal}(LE/L)$ such that $\widetilde{\sigma}|_E = \sigma$.



λ-invariants in Extensions

Proposition

Let $v \in B'_K$ be such that v is not an upper ramification break of L/K and set $w = \psi_{L/K}(v)$. There is a group isomorphism $\rho^v_{L/K} : (\overline{K}, +) \to (\overline{K}, +)$ such that for every pair $(E/K, \sigma)$ consisting of a C_p-extension E/K with ramification break v and a generator σ for $Gal(E/K)$ we have

$$\rho^v_{L/K}(\lambda_v(E/K, \sigma)) = \lambda_w(LE/L, \widetilde{\sigma}).$$

Proof: Suppose L/K is a C_p-extension with ramification break $u \neq v$. Then there is $a \in \mathcal{O}_K$ such that for all $c \in \mathcal{O}_E$ we have

$$\begin{aligned} \mathrm{N}_{LE/E}(\pi_{LE} + c\pi_{LE}^{w+1}) &\equiv \pi_E + c^p \pi_E^{v+1} \pmod{\mathcal{M}_E^{v+2}} \text{ if } v < u, \\ &\equiv \pi_E + ca\pi_E^{v+1} \pmod{\mathcal{M}_E^{v+2}} \text{ if } u < v, \end{aligned}$$

which proves the claim. The general case now follows by induction.

Outline of the Proof of the Other Theorem

Recall that M/L is a solution to the embedding problem associated to the extension $\widetilde{G}$ of $G = \mathrm{Gal}(L/K)$ by C_p, and that $w = \psi_{L/K}(v)$ is the ramification break of M/L.

Suppose w is the smallest break associated to a solution of the embedding problem, v is not an upper ramification break of L/K, and $v \in B'_K$.

Let τ be a generator for $\mathrm{Gal}(M/L) \cong C_p$. By the preceding proposition there is a C_p-extension E/K with ramification break v and a generator σ for $\mathrm{Gal}(E/K)$ such that

$$\lambda_w(LE/L, \widetilde{\sigma}) = \lambda_w(M/L, \tau).$$

Then ME/L is a $C_p \times C_p$-extension with two distinct upper ramification breaks x, w with $x < w$.

Hence there is a C_p-subextension M'/L of ME/L with ramification break x which solves the embedding problem. This contradicts the minimality of v.