# The Field of Norms

Kevin Keating
Department of Mathematics
University of Florida

May 29, 2013

# Sources


J. M. Fontaine, Corps de séries formelles et extensiones galoisiennes des corps locaux, Séminaire de Théorie des Nombres de Grenoble (1971-1972), 28–38.

J.-P. Wintenberger, Le corps des normes de certaines extensions infinies de corps locaux; applications, Ann. scient. Éc. Norm. Sup. (4) **16** (1983), 59–89.

J.-P. Wintenberger, Automorphismes des corps locaux de caractéristique $p$, J. Théor. Nombres Bordeaux **16**, no. 2, (2004), 429–456.

F. Laubie, Extensions de Lie et groupes d'automorphismes de corps locaux, Compositio Math. **67** (1988), 165–189.

I. B. Fesenko and S. V. Vostokov, *Local fields and their extensions. A constructive approach*, Amer. Math. Soc., Providence, RI, 1993.

# Notation

$K =$ local field

$\mathcal{O}_K \supset \mathcal{M}_K = \pi_K \mathcal{O}_K$

$\overline{K} = \mathcal{O}_K / \mathcal{M}_K$ is a finite field of characteristic $p$.

Hence $K \cong \overline{K}((T))$ or $[K : \mathbb{Q}_p] < \infty$.

$v_K : K \to \mathbb{Z} \cup \{\infty\}$ is the normalized valuation on $K$.

$v_K(K^\times) = \mathbb{Z}$

If $L/K$ is a finite extension then similar definitions apply to $L$.

# Ramification in Finite Galois Extensions

$L/K$ finite totally ramified Galois extension, $G = \mathrm{Gal}(L/K)$.

For $\sigma \in G$ define $i(\sigma) = v_L(\sigma(\pi_L) - \pi_L) - 1$.

For $x \geq 0$ set $G_x = \{\sigma \in G : i(\sigma) \geq x\}$. Then

1. $G_x \trianglelefteq G$,
2. $G_x = G_i$ with $i = \lceil x \rceil$,
3. $x \leq y \Rightarrow G_y \subset G_x$,
4. $G_x = \{1\}$ for $x \gg 0$.

For $i \geq 1$ there is a group embedding

$$\begin{aligned} G_i/G_{i+1} &\hookrightarrow \mathcal{M}_L^i/\mathcal{M}_L^{i+1} \\ \sigma G_{i+1} &\mapsto \frac{\sigma(\pi_L) - \pi_L}{\pi_L} + \mathcal{M}_L^{i+1}. \end{aligned}$$

Hence $G_i/G_{i+1}$ is an elementary abelian $p$-group.

# The Upper Ramification Numbering

Let $K \subset M \subset L$ and set $H = \mathrm{Gal}(L/M)$. Then $H_x = G_x \cap H$.

If $H \trianglelefteq G$, how to determine $(G/H)_x$? Define

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

$$\psi_{L/K}(x) = \phi_{L/K}^{-1}(x),$$

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

Then

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

**Herbrand's Theorem:** Let $K \subset M \subset L$ with $H = \mathrm{Gal}(L/M)$ normal in $G = \mathrm{Gal}(L/K)$. Then $(G/H)^x = G^x H/H$.

# Ramification in Infinite Galois Extensions

Let $L/K$ be an infinite totally ramified Galois extension, with $G = \mathrm{Gal}(L/K)$. Set

$$\mathcal{E}_{L/K} = \{K \subset M \subset L : [M : K] < \infty,\ M/K \text{ Galois}\}.$$

Then $L = \bigcup_{M \in \mathcal{E}_{L/K}} M$.

For $M \in \mathcal{E}_{L/K}$ set $H_M = \mathrm{Gal}(L/M)$.

Then $G \cong \varprojlim (G/H_M)$.

Define $G^x = \varprojlim (G/H_M)^x$.

This makes sense thanks to Herbrand's Theorem.

# Arithmetically Profinite Extensions

Say the totally ramified Galois extension $L/K$ is APF if $|G : G^x| < \infty$ for all $x \geq 0$.

In this case define:

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

$$\phi_{L/K}(x) = \psi_{L/K}^{-1}(x),$$

$$G_x = G^{\phi_{L/K}(x)}.$$

**Example:** Let $L/K$ be a totally ramified abelian extension. Then $L/K$ is APF by class field theory.

**Example:** Let $L/K$ be a totally ramified Galois extension such that $\mathrm{Gal}(L/K)$ is a $p$-adic Lie group. Then $L/K$ is APF.

# Ramification Breaks

**Definition:** Let $L/K$ be an APF extension. Say $b \geq 0$ is a "lower ramification break" for $L/K$ if $G_b \neq G_{b+\epsilon}$ for every $\epsilon > 0$.

Let $b_1 < b_2 < b_3 < \dots$ be the positive lower ramification breaks of $L/K$. For $n \geq 1$ let $L_n$ denote the fixed field of $G_{b_n}$. Then

1. $\mathrm{Gal}(L_n/K) \cong G/G_{b_n}$
2. $\mathrm{Gal}(L_{n+1}/L_n) \cong G_{b_n}/G_{b_{n+1}}$ is an elementary abelian $p$-group.
3. $\mathrm{N}_{L_{n+1}/L_n} : \mathcal{O}_{L_{n+1}} \to \mathcal{O}_{L_n}$ preserves $\cdot$, but not $+$.

# The Field of Norms

Let $L/K$ be a totally ramified APF extension, and for $n \geq 1$ set

$$s_n = \lceil (1 - p^{-1}) b_n \rceil$$

$$R_n = \mathcal{O}_{L_n} / \mathcal{M}_{L_n}^{s_n}.$$

Then $R_n \cong \overline{K}[T]/(T^{s_n})$.

**Theorem:** $\mathrm{N}_{L_{n+1}/L_n} : \mathcal{O}_{L_{n+1}} \to \mathcal{O}_{L_n}$ induces a well-defined surjective ring homomorphism $\overline{\mathrm{N}}_{n+1,n} : R_{n+1} \to R_n$.

**Definition:** The field of norms $X(L/K)$ of $L/K$ is defined by

$$R(L/K) = \varprojlim R_n \cong \overline{K}[[T]]$$

$$X(L/K) = \mathrm{Frac}(R(L/K)) \cong \overline{K}((T)).$$

# The Nottingham Group

The following are groups with the operation of power series composition:

$$\mathcal{A}(\overline{K}) = \{c_0 T + c_1 T^2 + c_2 T^3 + \cdots : c_i \in \overline{K},\ c_0 \neq 0\}$$
$$\mathcal{N}(\overline{K}) = \{T + c_1 T^2 + c_2 T^3 + \cdots : c_i \in \overline{K}\}$$

$\mathcal{N}(\overline{K})$ is known as the "Nottingham group". We have

$$\mathrm{Aut}_{\overline{K}}(\overline{K}((T))) \cong \mathcal{A}(\overline{K}).$$

# Group Actions

Let $L/K$ be a totally ramified APF extension.

Then $G = \mathrm{Gal}(L/K)$ acts on $R_n$, $R(L/K)$, and $X(L/K)$.

Hence there is an embedding

$$G \hookrightarrow \mathrm{Aut}_{\overline{K}}(X(L/K)).$$

By choosing a uniformizer $\omega$ for $X(L/K)$ we get isomorphisms

$$X(L/K) \cong \overline{K}((T))$$
$$\mathrm{Aut}_{\overline{K}}(X(L/K)) \cong \mathrm{Aut}_{\overline{K}}(\overline{K}((T))) \cong \mathcal{A}(\overline{K}).$$

Therefore we get an embedding

$$j_\omega : G \hookrightarrow \mathcal{A}(\overline{K}).$$

# A Conjugacy Class Associated to $L/K$

Choosing a different uniformizer $\omega'$ for $X(L/K)$ gives another embedding

$$j_{\omega'} : G \hookrightarrow \mathcal{A}(\overline{K})$$

which may be different from $j_\omega$.

However, the image $j_{\omega'}(G)$ is conjugate to $j_\omega(G)$ in $\mathcal{A}(\overline{K})$. In fact every subgroup of $\mathcal{A}(\overline{K})$ which is conjugate to $j_\omega(G)$ is equal to $j_{\omega'}(G)$ for some uniformizer $\omega'$ for $X(L/K)$.

Let $\mathcal{C}(L/K)$ denote the conjugacy class of subgroups $\mathcal{A}(\overline{K})$ corresponding to $L/K$:

$$\mathcal{C}(L/K) = \{j_\omega(G) : v_{X(L/K)}(\omega) = 1\}$$

# Ramification in $\mathcal{A}(\overline{K})$

For $h \in \mathcal{A}(\overline{K})$ define

$$i(h) = v_{\overline{K}((T))}(h(T) - T) - 1.$$

Thus $i(h) = n \geq 1$ if and only if there is $c_n \in \overline{K}^\times$ such that

$$h(T) = T + c_n T^{n+1} + \cdots .$$

Let $\Gamma \leq \mathcal{A}(\overline{K})$. By analogy with Galois groups we define

$$\Gamma_x = \{\sigma \in \Gamma : i(\sigma) \geq x\}$$

$$\phi_\Gamma(x) = \int_0^x \frac{dt}{|\Gamma_0 : \Gamma_t|}.$$

Suppose $L/K$ is an APF extension and $\omega$ is a uniformizer for $X(L/K)$ such that $\Gamma = j_\omega(G)$, where $G = \mathrm{Gal}(L/K)$. Then $\Gamma_x = j_\omega(G_x)$ for $x \geq 0$.

# $\mathbb{Z}_p$-subgroups of $\mathcal{N}(\overline{K})$

Let $h \in \mathcal{N}(\overline{K})$ have infinite order. Then the closure of the subgroup of $\mathcal{N}(\overline{K})$ generated by $h$ is isomorphic to $\mathbb{Z}_p$. Write

$$\widehat{\langle h \rangle} = h^{\mathbb{Z}_p} \cong \mathbb{Z}_p.$$

**Theorem (Wintenberger):** Let $\Gamma \leq \mathcal{A}(\overline{K})$ with $\Gamma \cong \mathbb{Z}_p$.

(a) There is $L/K$ such that $\Gamma \in \mathcal{C}(L/K)$.

(b) The extension $L/K$ is uniquely determined by $\Gamma$ up to $\overline{K}$-isomorphism.

# Partitioning $\mathcal{N}(\overline{K})$

$\mathcal{N}(\overline{K})$ can be partitioned into 3 classes:

$$\mathcal{N}_f(\overline{K}) = \{h \in \mathcal{N}(\overline{K}) : |h| < \infty\}$$
$$\mathcal{N}_p(\overline{K}) = \{h \in \mathcal{N}(\overline{K}) : \widehat{\langle h \rangle} \in \mathcal{C}(L/K) \text{ with } \mathrm{char}(K) = p\}$$
$$\mathcal{N}_0(\overline{K}) = \{h \in \mathcal{N}(\overline{K}) : \widehat{\langle h \rangle} \in \mathcal{C}(L/K) \text{ with } \mathrm{char}(K) = 0\}$$

**Theorem (Wintenberger):**
(a) $\mathcal{N}_0(\overline{K})$ is an open dense subset of $\mathcal{N}(\overline{K})$.
(b) The closure of $\mathcal{N}_f(\overline{K})$ in $\mathcal{N}(\overline{K})$ is $\mathcal{N}_f(\overline{K}) \cup \mathcal{N}_p(\overline{K})$.

$\mathcal{N}_0(\overline{K})$ can be further partitioned into subclasses:

$$\mathcal{N}_0^e(\overline{K}) = \{h \in \mathcal{N}(\overline{K}) : \widehat{\langle h \rangle} \in \mathcal{C}(L/K) \text{ with } v_K(p) = e\}$$

# Ramification in $\mathbb{Z}_p$-Subgroups of $\mathcal{A}(\overline{K})$

Let $\Gamma = \widehat{\langle h \rangle}$ be a $\mathbb{Z}_p$-subgroup of $\mathcal{A}(\overline{K})$. The lower ramification breaks of $\Gamma$ are given by $b_n = i(h^{p^n})$ for $n \geq 0$.

The $n$th upper ramification break of $\Gamma$ is $u_n = \phi_\Gamma(b_n)$. The upper breaks can be computed recursively by

$$u_0 = b_0, \quad u_n - u_{n-1} = p^{-n}(b_n - b_{n-1}) \text{ for } n \geq 1.$$

If $\Gamma \in \mathcal{C}(L/K)$ then the ramification breaks of $\Gamma$ are the same as those of $L/K$. Hence

$$\begin{aligned} u_n &= u_{n-1} + e(K) && \text{if } u_{n-1} > e(K)/(p-1), \\ u_n &\geq p u_{n-1} && \text{otherwise.} \end{aligned}$$

Suppose $u_n < p u_{n-1}$ for some $n \geq 1$. Then $\mathrm{char}(K) = 0$, $e(K) = u_n - u_{n-1}$, and $u_i = u_{i-1} + e(K)$ for every $i \geq n$. It follows that $b_i = b_{i-1} + e(K)p^i$ for $i \geq n$.

# Subgroups of $\mathcal{A}(\overline{K})$

**Question:** Which subgroups $\Gamma$ of $\mathcal{A}(\overline{K})$ (or $\mathcal{N}(\overline{K})$) come from an APF extension $L/K$?

$\Gamma$ must at least be closed and infinite.

**Theorem (Laubie):** Let $\Gamma \leq \mathcal{A}(\overline{K})$ be a solvable $p$-adic Lie group of dimension $\geq 1$. Then there is an APF extension $L/K$ such that $\Gamma \in \mathcal{C}(L/K)$.

**Question:** Let $\Gamma \leq \mathcal{A}(\overline{K})$ be a $p$-adic Lie group of dimension $\geq 1$. Is there $L/K$ as above such that $\Gamma \in \mathcal{C}(L/K)$?

**Answer:** Not necessarily. We need to be more careful.

# Computing $e(K)$

$L/K$ = totally ramified $p$-adic Lie extension.

$d_G$ = dimension of the $p$-adic Lie group $G = \mathrm{Gal}(L/K)$.

$e(K) = v_K(p)$ = absolute ramification index of $K$.

With the help of Sen's paper "Ramification in $p$-adic Lie extensions" we can compute $e(K)$ in terms of $d_G$ and the ramification data of $L/K$:

$$e(K) = \lim_{x\to\infty} \frac{d_G \cdot \phi_{L/K}(x)}{\log_p |G : G_x|}.$$

For a $p$-adic Lie group $\Gamma \le \mathcal{A}(\overline{K})$ of dimension $d_\Gamma \ge 1$ define

$$e(\Gamma) = \lim_{x\to\infty} \frac{d_\Gamma \cdot \phi_\Gamma(x)}{\log_p |\Gamma : \Gamma_x|}.$$

Suppose $\Gamma \in \mathcal{C}(L/K)$. Then $G$ has the same ramification data as $\Gamma$, so $e(K) = e(\Gamma)$.

# An Example

Let $F(X, Y)$ be a formal group law of height 2 over $\mathbb{F}_p$. Then $\mathrm{End}_{\mathbb{F}_{p^2}}(F)$ is isomorphic to the maximal order $B$ in the quaternion algebra over $\mathbb{Q}_p$.

Let $\Gamma = \mathrm{Aut}_{\mathbb{F}_{p^2}}(F) \leq \mathcal{A}(\mathbb{F}_{p^2})$. Then $\Gamma \cong B^\times$ is a $p$-adic Lie group of dimension 4.

The lower ramification breaks of $\Gamma$ are $b_k = p^k - 1$ for $k \geq 0$. For $k \geq 1$ we have

$$|\Gamma : \Gamma_{p^k-1}| = p^{2k} - p^{2k-2}$$
$$\phi_\Gamma(p^k - 1) = \frac{p^k - 1}{p^{k+2} - p^k}.$$

Hence

$$e(\Gamma) = \lim_{k\to\infty} \frac{4 \cdot \frac{p^k-1}{p^{k+2}-p^k}}{\log_p(p^{2k} - p^{2k-2})} = 0!?$$

# A Conjecture

The group $\Gamma \leq \mathcal{A}(\mathbb{F}_{p^2})$ in the preceding example does not come from any $p$-adic Lie extension $L/K$.

**Conjecture (Laubie):** Let $\Gamma \leq \mathcal{A}(\overline{K})$ be a $p$-adic Lie group such that $e(\Gamma) > 0$. Then there is a totally ramified $p$-adic Lie extension $L/K$ such that $\Gamma \in \mathcal{C}(L/K)$.

Laubie showed that it is enough to prove the conjecture in the case where $\Gamma$ is a simple $p$-adic Lie group.

# Extensions

Let $L/K$ be APF and let $M/L$ be a finite extension such that $M/K$ is Galois. Then $M/K$ is APF, and $X(M/K)/X(L/K)$ is a finite Galois extension. Denote $X(M/K)$ by $X_{L/K}(M)$.

If $M_1 \subset M_2$ then there is a natural $X(L/K)$-embedding of $X_{L/K}(M_1)$ into $X_{L/K}(M_2)$.

For an infinite Galois extension $E/K$ such that $E \supset L$ define

$$X_{L/K}(E) = \lim_{\rightarrow} X_{L/K}(M),$$

where the direct limit is taken over all finite subextensions $M/L$ of $E/L$ such that $M/K$ is Galois.

**Theorem (Wintenberger):** Let $L^{sep}$ be a separable closure of $L$. Then $X_{L/K}(K^{sep})$ is a separable closure of $X(L/K)$.

# Galois Groups

Let $E/L$ be such that $E/K$ is Galois. Then the action of $\mathrm{Gal}(E/L)$ on $X_{L/K}(E)$ induces an isomorphism

$$\mathrm{Gal}(E/L) \cong \mathrm{Gal}(X_{L/K}(E)/X(L/K)).$$

It follows that if $K$ is a local field with residue field $\overline{K}$ and $L/K$ is a totally ramified APF extension then

$$\mathrm{Gal}(L^{sep}/L) \cong \mathrm{Gal}(\overline{K}((T))^{sep}/\overline{K}((T))).$$

Hence $\mathrm{Gal}(L^{sep}/L)$ is independent of $L$ or even $\mathrm{char}(L)$.