Trace, Norm, Etc.

Kevin Keating
Department of Mathematics
University of Florida

May 26, 2016

Local Fields

Let K be a field which is complete with respect to a discrete valuation $v_K : K^\times \to \mathbb{Z}$, whose residue field $\overline{K}$ is a perfect field of characteristic p. Also let

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

$$\pi_K = \text{ uniformizer for } \mathcal{O}_K \text{ (i. e., } v_K(\pi_K) = 1)$$

$$\mathcal{M}_K = \pi_K \cdot \mathcal{O}_K$$
$$= \text{ unique maximal ideal of } \mathcal{O}_K$$

Then $\overline{K} = \mathcal{O}_K/\mathcal{M}_K$.

Let L/K be a separable totally ramified extension of degree $[L : K] = n$.

Symmetric Polynomials and Extensions

For $1 \leq h \leq n$ let

$$e_h(X_1, \ldots, X_n) = \sum_{1 \leq t_1 < \cdots < t_h \leq n} X_{t_1} \ldots X_{t_h}$$

be the hth elementary symmetric polynomial in n variables.

Define $E_h : L \to K$ by $E_h(\alpha) = e_h(\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$, where $\sigma_1, \ldots, \sigma_n$ are the K-embeddings of L into K^{sep}. Then

$e_1(X_1, \ldots, X_n) = X_1 + \cdots + X_n \Rightarrow E_1(\alpha) = \mathrm{Tr}_{L/K}(\alpha)$

$e_n(X_1, \ldots, X_n) = X_1 X_2 \ldots X_n \Rightarrow E_n(\alpha) = \mathrm{N}_{L/K}(\alpha)$

Suppose $L = K(\alpha)$ and $f_\alpha(X) = X^n + \sum_{h=1}^{n} (-1)^h b_h X^{n-h}$ is the minimum polynomial for α over K. Then $E_h(\alpha) = b_h$.

The Problem

Problem: Determine $E_h(\mathcal{M}_L^r)$.

But $E_h(\mathcal{M}_L^r)$ can be quite complicated. In particular, it does not have to be a (fractional) ideal.

Easier problem: Determine $\mathcal{O}_K \cdot E_h(\mathcal{M}_L^r) = \mathcal{M}_K^h$.

Equivalently, determine $g_h : \mathbb{Z} \to \mathbb{Z}$ defined by

$$g_h(r) = \min\{v_K(E_h(\alpha)) : \alpha \in \mathcal{M}_L^r\}.$$

Of course, $\mathcal{O}_K \cdot E_n(\mathcal{M}_L^r) = \mathcal{O}_K \cdot \mathrm{N}_{L/K}(\mathcal{M}_L^r) = \mathcal{M}_K^r$, so $g_n(r) = r$.

$E_1(\mathcal{M}_L^r) = \mathrm{Tr}_{L/K}(\mathcal{M}_L^r)$ is also well-understood:

The Trace and the Different

Let $\delta_{L/K} = \mathcal{M}_L^d$ be the different of L/K. Then $\mathrm{Tr}_{L/K}(\mathcal{M}_L^{-d}) \subset \mathcal{O}_K$ but $\mathrm{Tr}_{L/K}(\mathcal{M}_L^{-d-1}) \not\subset \mathcal{O}_K$. Hence

$$\begin{aligned}
\mathrm{Tr}_{L/K}(\mathcal{M}_L^r) \subset \mathcal{M}_K^s &\Leftrightarrow \mathcal{M}_K^{-s}\mathrm{Tr}_{L/K}(\mathcal{M}_L^r) \subset \mathcal{O}_K \\
&\Leftrightarrow \mathrm{Tr}_{L/K}(\mathcal{M}_K^{-s}\mathcal{M}_L^r) \subset \mathcal{O}_K \\
&\Leftrightarrow \mathrm{Tr}_{L/K}(\mathcal{M}_L^{r-ns}) \subset \mathcal{O}_K \\
&\Leftrightarrow -d \leq r - ns \\
&\Leftrightarrow s \leq \frac{r+d}{n}.
\end{aligned}$$

It follows that $\mathrm{Tr}_{L/K}(\mathcal{M}_L^r) = \mathcal{M}_K^{\lfloor (r+d)/n \rfloor}$. Hence

$$E_1(\mathcal{M}_L^r) = \mathcal{M}_K^{\lfloor (r+d)/n \rfloor}$$

$$g_1(r) = \left\lfloor \frac{r+d}{n} \right\rfloor.$$

Indices of Inseparability (Fried, Heiermann)

Let π_L be a uniformizer for L, and let

$$\begin{aligned} f(X) &= \sum_{h=0}^{n} (-1)^h a_h X^{n-h} \\ &= X^n - a_1 X^{n_1} + \cdots + (-1)^{n-1} a_{n-1} X + (-1)^n a_n \end{aligned}$$

be the minimum polynomial for π_L over K.

Write $n = up^\nu$ with $p \nmid u$, and for $0 \leq j \leq \nu$ define

$$\begin{aligned} i_j^* &= \min\{v_L(a_h \pi_L^{n-h}) : 0 \leq h < n,\ v_p(n-h) \leq j\} - n \\ i_j &= \min\{i_{j'}^* + (j'-j) v_L(p) : j \leq j' \leq \nu\}. \end{aligned}$$

If $\mathrm{char}(K) = p$ then $i_j = i_j^*$. In general, i_j does not depend on the choice of π_L.

We have $0 = i_\nu < i_{\nu-1} \leq \cdots \leq i_1 \leq i_0$.

An Example

Let $K = \mathbb{F}_3((t))$ and let $L = K(\pi_L)$, where π_L is a root of the Eisenstein polynomial

$$f(X) = X^9 + t^5X^7 + t^4X^6 - t^5X^4 + t^5X^3 - t.$$

Then

$$\begin{aligned} i_0 &= \min\{v_L(t^5\pi_L^7), v_L(-t^5\pi_L^4)\} - 9 \\ &= \min\{5\cdot 9 + 7, 5\cdot 9 + 4\} - 9 = 40 \\ i_1 &= \min\{v_L(t^5\pi_L^7), v_L(t^4\pi_L^6), v_L(-t^5\pi_L^4), v_L(t^5\pi_L^3)\} - 9 \\ &= \min\{5\cdot 9 + 7, 4\cdot 9 + 6, 5\cdot 9 + 4, 5\cdot 9 + 3\} - 9 = 33 \\ i_2 &= 0. \end{aligned}$$

Ramification Data

Let L/K be finite Galois, with $G = \mathrm{Gal}(L/K)$.

For $t \geq 0$ define the tth lower ramification group of L/K by

$$G_t = \{\sigma \in G : v_L(\sigma(\pi_L) - \pi_L) \geq t + 1\}.$$

The Hasse-Herbrand function of L/K is

$$\phi_{L/K}(x) = \int_0^x \frac{dt}{[G : G_t]}.$$

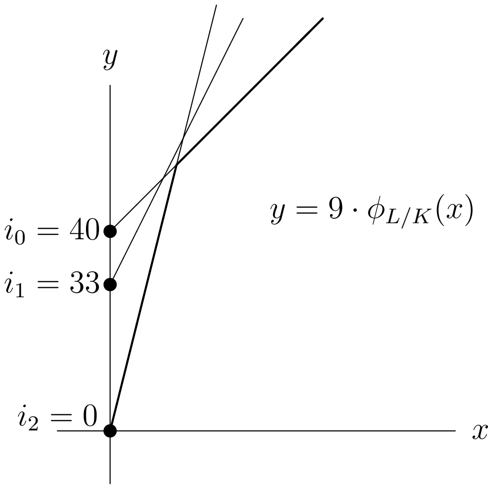
The Hasse-Herbrand function can also be defined when L/K is separable but not Galois.

Theorem (Fried, Heiermann): For $x \geq 0$,

$$\phi_{L/K}(x) = \frac{1}{n} \cdot \min\{i_j + p^j x : 0 \leq j \leq \nu\}.$$

$\phi_{L/K}$ for the Example

The Hasse-Herbrand function for the example can be deduced from the indices of inseparability:



The Containment Theorem

Containment Theorem: Let L/K be a totally ramified extension of degree $n = up^{\nu}$. Let $r \in \mathbb{Z}$ and $1 \leq h \leq n$, and set $j = \min\{v_p(h), \nu\}$. Then

$$E_h(\mathcal{M}_L^r) \subset \mathcal{M}_K^{\lceil (i_j + hr)/n \rceil}$$
$$g_h(r) \geq \left\lceil \frac{i_j + hr}{n} \right\rceil .$$

Remark: Since

$$E_h(\mathcal{M}_L^{r+nt}) = E_h(\pi_K^t \mathcal{M}_L^r) = \pi_K^{ht} E_h(\mathcal{M}_L^r)$$
$$\left\lceil \frac{i_j + h(r+nt)}{n} \right\rceil = ht + \left\lceil \frac{i_j + hr}{n} \right\rceil$$

we may assume $1 \leq r \leq n$.

When do we Have Equality?

Sharp Theorem: Let K be a local field of characteristic p and let L/K be a totally ramified extension of degree $n = up^{\nu}$. Let $0 \leq j \leq \nu$. If $i_j = i_{j-1}$ assume that $|\overline{K}| \geq p^j$. Then

$$\mathcal{O}_K \cdot E_{p^j}(\mathcal{M}_L^r) = \mathcal{M}_K^{\lceil (i_j + rp^j)/n \rceil}$$
$$g_{p^j}(r) = \left\lceil \frac{i_j + rp^j}{n} \right\rceil .$$

Remark: As with the Containment Theorem we may assume $1 \leq r \leq n$. Furthermore, we may assume

$$\left\lceil \frac{i_j + rp^j}{n} \right\rceil < \left\lceil \frac{i_j + (r+1)p^j}{n} \right\rceil .$$

Sharp Theorem for $j = 0$, $\mathrm{char}(K) = p$

Let π_L be a uniformizer for L, and let $f(X)$ be the minimum polynomial for π_L over K. Then the different $\delta_{L/K} = \mathcal{M}_L^d$ is generated by $f'(\pi_L)$.

The terms of $f(X)$ whose degree is divisible by p give 0 in $f'(X)$. Therefore we have $d = v_L(f'(\pi_L)) = i_0 + n - 1$.

It follows that

$$\begin{aligned} g_1(r) &= \left\lfloor \frac{r+d}{n} \right\rfloor \\ &= \left\lfloor \frac{r+i_0+n-1}{n} \right\rfloor \\ &= \left\lceil \frac{i_0+r}{n} \right\rceil . \end{aligned}$$

Crazy Idea$^{\text{TM}}$

The Sharp Theorem holds for $j = 0$ because of the relation between i_0 and the different of L/K.

The Sharp Theorem also holds for $j \geq 1$, at least if $\overline{K}$ is large.

Can we interpret the indices of inseparabilty i_j for $1 \leq j \leq \nu$ as higher order differents of L/K?

Monomial Symmetric Functions

Let $\boldsymbol{\mu} = (\mu_1, \ldots, \mu_h)$ be a partition of some positive integer w.

View $\boldsymbol{\mu}$ as a multiset, and let $\boldsymbol{\mu}'$ be the union of $\boldsymbol{\mu}$ with the multiset consisting of $n - h$ copies of 0.

The monomial symmetric function in n variables associated to $\boldsymbol{\mu}$ is

$$m_{\boldsymbol{\mu}}(X_1, \ldots, X_n) = \sum_{\boldsymbol{\omega}} X_1^{\omega_1} X_2^{\omega_2} \ldots X_n^{\omega_n},$$

where the sum is taken over all distinct permutations $\boldsymbol{\omega} = (\omega_1, \ldots, \omega_n)$ of $\boldsymbol{\mu}'$.

For $\alpha \in L$ set $M_{\boldsymbol{\mu}}(\alpha) = m_{\boldsymbol{\mu}}(\sigma_1(\alpha), \ldots, \sigma_n(\alpha)) \in K$.

Proving the Containment Theorem

Elements of $\mathcal{M}_L^r$ can be expressed in the form $c_0\pi_L^r + c_1\pi_L^{r+1} + \dots$ with $c_i \in \mathcal{O}_K$.

Therefore if $\alpha \in E_h(\mathcal{M}_L)$ then α is a sum of terms of the form $c_{\mu_1}c_{\mu_2}\dots c_{\mu_h}M_\mu(\pi_L)$, where $\boldsymbol{\mu} = (\mu_1, \dots, \mu_h)$ is a partition with h parts, all $\geq r$. Hence $w := \mu_1 + \dots + \mu_h \geq rh$.

$m_{\boldsymbol{\mu}}(X_1, \dots, X_n)$ can be expressed as a polynomial in the elementary symmetric functions:

$$m_{\boldsymbol{\mu}} = \sum_{\boldsymbol{\lambda}} d_{\boldsymbol{\lambda\mu}} \cdot e_{\lambda_1}e_{\lambda_2}\dots e_{\lambda_k},$$

where the sum is taken over all partitions $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_k)$ of w whose parts λ_i are at most n. Furthermore we have $d_{\boldsymbol{\lambda\mu}} \in \mathbb{Z}$.

Proving the Containment Theorem (continued)

To prove the theorem it suffices to show that for each such $\boldsymbol{\mu}$ and $\boldsymbol{\lambda}$ we have

$$d_{\boldsymbol{\lambda}\boldsymbol{\mu}} \cdot E_{\lambda_1}(\pi_L)E_{\lambda_2}(\pi_L)\ldots E_{\lambda_k}(\pi_L) \in \mathcal{M}_K^{\lceil (i_j+hr)/n \rceil}.$$

Recall that $E_{\lambda_i}(\pi_L) = a_i$ is a coefficient of the minimum polynomial for π_L over K. Hence it suffices to show that

$$d_{\boldsymbol{\lambda}\boldsymbol{\mu}} \cdot a_{\lambda_1}a_{\lambda_2}\ldots a_{\lambda_k} \in \mathcal{M}_K^{\lceil (i_j+hr)/n \rceil}.$$

There are two cases to consider:

- If $p^{j+1} \nmid \lambda_i$ for some i show $a_{\lambda_1}a_{\lambda_2}\ldots a_{\lambda_k} \in \mathcal{M}_K^{\lceil (i_j+hr)/n \rceil}$.
- If $p^{j+1} \mid \lambda_i$ for all i show $p^t \mid d_{\boldsymbol{\lambda}\boldsymbol{\mu}}$ for some $t \geq 1$.

For the second case we need to compute $d_{\boldsymbol{\lambda}\boldsymbol{\mu}}$.

Proving the Sharp Theorem

In general we can find a partition $\boldsymbol{\lambda}$ of some $w \geq p^j r$ such that

$$v_K(a_{\lambda_1} \dots a_{\lambda_k}) = \left\lceil \frac{i_j + rp^j}{n} \right\rceil .$$

In fact, write $i_j = an - b$ with $0 < b < n$ and set $\lambda_i = n$ for $1 \leq i < k$ and $\lambda_k = b$, for appropriate k.

The problem is making sure there is another partition $\boldsymbol{\mu} = (\mu_1, \dots, \mu_{p^j})$ of w with $\mu_i \geq r$ such that $p \nmid d_{\boldsymbol{\lambda\mu}}$.

If $i_j = i_{j-1}$ there may be multiple terms to consider. We need to assume $\overline{K}$ is large in this case to be sure we can avoid cancellations.

Tilings of Cycle Digraphs

We say that a directed graph Γ is a cycle digraph if its components are all directed cycles of length ≥ 1.

We denote the vertex set of Γ by $V(\Gamma)$.

We define the sign of Γ to be $\operatorname{sgn}(\Gamma) = (-1)^{w-c}$, where $w = |V(\Gamma)|$ and c is the number of components of Γ.

Let Γ be a cycle digraph with w vertices and let $\boldsymbol{\lambda}$ be a partition of w. A $\boldsymbol{\lambda}$-tiling of Γ is a set S of subgraphs of Γ such that

1. Each $\gamma \in S$ is a directed path of length ≥ 0.
2. $\{V(\gamma) : \gamma \in S\}$ is a partition of $V(\Gamma)$.
3. The multiset $\{|V(\gamma)| : \gamma \in S\}$ is equal to $\boldsymbol{\lambda}$.

Bibrick Permutations

Let $\boldsymbol{\lambda}, \boldsymbol{\mu}$ be partitions of w. A $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-bibrick permutation is a triple (Γ, S, T), where Γ is a cycle digraph with w vertices, S is a $\boldsymbol{\lambda}$-tiling of Γ, and T is a $\boldsymbol{\mu}$-tiling of Γ.

An isomorphism from a $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-bibrick permutation (Γ, S, T) to a $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-bibrick permutation (Γ', S', T') is an isomorphism of digraphs $\eta : \Gamma \to \Gamma'$ which carries S onto S' and T onto T'.

We say that a bibrick permutation is admissible if it has no nontrivial automorphisms.

Let $\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma)$ denote the number of isomorphism classes of admissible $(\boldsymbol{\lambda}, \boldsymbol{\mu})$-bibrick permutations (Γ, S, T).

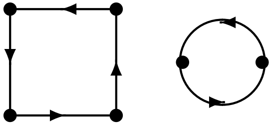
Let $\ell(\boldsymbol{\mu})$ denote the number of parts of $\boldsymbol{\mu}$.

An Example

$$\lambda = (2, 2, 2)$$

$$\mu = (2, 2, 1, 1)$$

$\Gamma :$



Computing $d_{\boldsymbol{\lambda}\boldsymbol{\mu}}$

Let $\boldsymbol{\mu} = (\mu_1, \ldots, \mu_h)$ be a partition of w with $h = \ell(\boldsymbol{\mu}) \leq n$.

Kulikauskas and Remmel showed how to express $m_{\boldsymbol{\mu}}$ in terms of elementary symmetric functions:

Theorem: Write

$$m_{\boldsymbol{\mu}}(X_1, \ldots, X_n) = \sum_{\boldsymbol{\lambda}} d_{\boldsymbol{\lambda}\boldsymbol{\mu}} \cdot e_{\lambda_1} e_{\lambda_2} \ldots e_{\lambda_k},$$

where the sum is over all partitions $\boldsymbol{\lambda}$ of w whose parts are $\leq n$. Then

$$d_{\boldsymbol{\lambda}\boldsymbol{\mu}} = (-1)^{\ell(\boldsymbol{\lambda})+\ell(\boldsymbol{\mu})} \sum_{\Gamma} \mathrm{sgn}(\Gamma)\eta_{\boldsymbol{\lambda}\boldsymbol{\mu}}(\Gamma),$$

where the sum is over all isomorphism classes of cycle digraphs Γ with w vertices.

An Example

Let $K = \mathbb{F}_2((t))$ and $L = K(\pi_L)$, where π_L is a root of the Eisenstein polynomial

$$f(X) = X^8 + tX^3 + tX^2 + t.$$

The indices of inseparability of L/K are $i_0 = 3$, $i_1 = i_2 = 2$, and $i_3 = 0$. Hence

$$\left\lceil \frac{i_2 + 2^2 \cdot 1}{8} \right\rceil = 1 \qquad \left\lceil \frac{i_2 + 2^2 \cdot 2}{8} \right\rceil = 2.$$

By the containment theorem we get $E_4(\mathcal{M}_L^2) \subset \mathcal{M}_K^2$. Furthermore, if π_L' is any uniformizer for L then the coefficient of X^4 in the minimum polynomial of π_L' over K has K-valuation ≥ 2.

So $E_4(\mathcal{M}_L) \subset \mathcal{M}_K^2$.

A More General Sharp Theorem?

Question: Let L/K be a totally ramified extension of degree $n = up^{\nu}$, let $1 \leq h \leq n$, and set $j = \min\{v_p(h), \nu\}$. Is it true that if $\overline{K}$ is sufficiently large then

$$\mathcal{O}_K \cdot E_h(\mathcal{M}_L^r) = \mathcal{M}_K^{\lceil (i_j + hr)/n \rceil}?$$