Bondarko's work on local Galois module theory

Part I: What he did

Kevin Keating
Department of Mathematics
University of Florida

May 21, 2018

Sources

Bondarko, M. V., Local Leopoldt's problem for rings of integers in abelian p-extensions of complete discrete valuation fields, Doc. Math. **5** (2000), 657–693.

Bondarko, M. V., Local Leopoldt's problem for ideals in totally ramified p-extensions of complete discrete valuation fields, Algebraic number theory and algebraic geometry, 27–57, Contemp. Math. 300, Amer. Math. Soc., Providence, RI, 2002.

Bondarko, M. V., The Leopoldt problem for totally ramified abelian extensions of complete discrete valuation fields (Russian), Algebra i Analiz **18** (2006), 99–129; translation in St. Petersburg Math. J. **18** (2007), 757–778.

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

$$\begin{aligned} \mathcal{O}_K &= \{\alpha \in K : v_K(\alpha) \geq 0\} \\ &= \text{ring of integers of } K \\ \pi_K &= \text{uniformizer for } \mathcal{O}_K \text{ (i.e., } v_K(\pi_K) = 1) \\ \mathcal{M}_K &= \pi_K \mathcal{O}_K \\ &= \text{unique maximal ideal of } \mathcal{O}_K \end{aligned}$$

Let L/K be a finite totally ramified Galois extension of degree q, and set $G = \mathrm{Gal}(L/K)$.

Galois Modules

L is a module over the ring $K[G]$.

In fact, by the normal basis theorem, L is free of rank 1 over $K[G]$.

$\mathcal{O}_L$ is a module over $\mathcal{O}_K[G]$.

If L/K is tamely ramified then $\mathcal{O}_L$ is free of rank 1 over $\mathcal{O}_K[G]$.

However, if L/K has some wild ramification then $\mathcal{O}_L$ is not free over $\mathcal{O}_K[G]$.

Associated Orders

Definition

Let $\mathcal{M}_L^i$ be a (fractional) ideal of $\mathcal{O}_L$. The associated order of $\mathcal{M}_L^i$ is

$$\mathfrak{A}(\mathcal{M}_L^i) = \{\gamma \in K[G] : \gamma(\mathcal{M}_L^i) \subset \mathcal{M}_L^i\}.$$

We have $\mathcal{O}_K[G] \subset \mathfrak{A}(\mathcal{M}_L^i)$, with $\mathcal{O}_K[G] = \mathfrak{A}(\mathcal{O}_L)$ if and only if L/K is tamely ramified. In particular, if L/K has wild ramification then

$$\pi_K^{-1} T \in \mathfrak{A}(\mathcal{O}_L) \setminus \mathcal{O}_K[G],$$

where $T = \sum_{\sigma \in G} \sigma$ is the trace element of $K[G]$.

$\mathcal{M}_L^i$ is a module over $\mathfrak{A}(\mathcal{M}_L^i)$.

Leopoldt Problem: When is $\mathcal{M}_L^i$ a free module over $\mathfrak{A}(\mathcal{M}_L^i)$?

K-linear Endomorphisms of L

Let $\mathrm{End}_K(L)$ denote the K-vector space of K-linear endomorphisms of L.

Elements of $L[G]$ induce K-linear endomorphisms of L. By the linear independence of automorphisms of L we get an isomorphism of K-vector spaces

$$L[G] \cong \mathrm{End}_K(L).$$

This becomes an isomorphism of K-algebras if we define multiplication on $L[G]$ so that

$$a\sigma \cdot b\tau = a\sigma(b) \cdot \sigma\tau$$

for $a, b \in L$, $\sigma, \tau \in G$.

The isomorphism above identifies $K[G]$ with a K-subalgebra of $\mathrm{End}_K(L)$.

The Maps ϕ and ψ_σ

There is a K-linear map $\phi : L \otimes_K L \to L[G]$ defined by

$$\phi(a \otimes b) = aTb = \sum_{\sigma \in G} a\sigma(b)\sigma.$$

For $c \in L$ we get

$$\phi(a \otimes b)(c) = \sum_{\sigma \in G} a\sigma(bc) = a\mathrm{Tr}_{L/K}(bc).$$

Proposition

ϕ is an isomorphism of K-vector spaces.

For $\sigma \in G$ define $\psi_\sigma : L \otimes_K L \to L$ by $\psi_\sigma(a \otimes b) = a\sigma(b)$. Then ψ_σ is a K-algebra homomorphism, and for $\beta \in L \otimes_K L$ we have

$$\phi(\beta) = \sum_{\sigma \in G} \psi_\sigma(\beta)\sigma.$$

Some Lattices in $\text{End}_K(L)$

Let $I_1 = \mathcal{M}_L^{a_1}$ and $I_2 = \mathcal{M}_L^{a_2}$ be fractional ideals of $\mathcal{O}_L$. Define

$$\mathfrak{C}(I_1, I_2) = \text{Hom}_K(I_1, I_2)$$
$$\mathfrak{A}(I_1, I_2) = \mathfrak{C}(I_1, I_2) \cap K[G].$$

Then $\mathfrak{A}(I_1, I_1) = \mathfrak{A}(I_1)$.

Every element of $\mathfrak{C}(I_1, I_2)$ extends uniquely to a K-endomorphism of L. Hence we may view $\mathfrak{C}(I_1, I_2)$ as an $\mathcal{O}_K$-submodule of $\text{End}_K(L)$.

Let $\mathfrak{D}$ denote the different of the extension L/K.

Proposition

$\phi(I_2 \otimes \mathfrak{D}^{-1} I_1^{-1}) = \mathfrak{C}(I_1, I_2)$

Note that $\mathfrak{D}^{-1} I_1^{-1} = I_1^*$ is the dual of I_1 with respect to the trace pairing for L/K.

The Smallest Shift Valuation

Definition

For $\gamma \in \mathrm{End}_K(L) \cong L[G]$ set

$$\hat{v}_L(\gamma) = \min\{v_L(\gamma(x)) - v_L(x) : x \in L^\times\}.$$

(This is parallel to the definition of the norm of a linear operator.)

For $n \in \mathbb{Z}$ we get $\mathcal{O}_K$-submodules of $\mathrm{End}_K(L)$ by setting

$$\begin{aligned}\mathfrak{C}_n &= \{\gamma \in \mathrm{End}_K(L) : \hat{v}_L(\gamma) \geq n\} \\ &= \bigcap_{k \in \mathbb{Z}} \mathfrak{C}(\mathcal{M}_L^k, \mathcal{M}_L^{k+n}) \\ \mathfrak{A}_n &= \mathfrak{C}_n \cap K[G].\end{aligned}$$

Describing $\mathfrak{A}_n$ in Terms of ϕ

For $n \in \mathbb{Z}$ let X_n be the $\mathcal{O}_K$-submodule of $L \otimes_K L$ generated by all elements of the form $a \otimes b$, with $v_L(a) + v_L(b) \geq n$.

Write $\mathfrak{D} = \mathcal{M}_L^d$ and set $i_0 = d - q + 1$.

Theorem

Let $n \in \mathbb{Z}$. Then $\mathfrak{C}_n = \phi(X_{n-i_0})$.

A Partial Order

Let H be the subgroup of $\mathbb{Z} \times \mathbb{Z}$ generated by the element $(q, -q)$.

For $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ write $[a, b]$ for the coset $(a, b) + H$.

We define a partial order on the quotient group $(\mathbb{Z} \times \mathbb{Z})/H$ by $[a, b] \leq [c, d]$ if and only if there is $t \in \mathbb{Z}$ such that $a \leq c + tq$ and $b \leq d - tq$.

We sometimes represent $(\mathbb{Z} \times \mathbb{Z})/H$ by the set

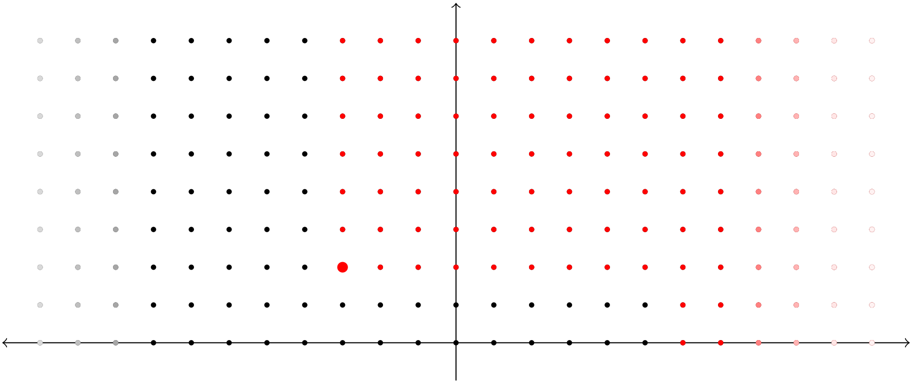
$$\mathcal{F} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : 0 \leq b < q\}$$

of coset representatives.

An Example

Let $q = 9$. Here is the set

$$\{(c, d) \in \mathcal{F} : [-3, 2] \leq [c, d]\}.$$



Expansions in $L \otimes_K L$

Fix a uniformizer π_L for L, and let $\mathcal{T}$ be the set of Teichmüller representatives of K.

Let $\beta \in L \otimes_K L$. Then there are unique $b_j \in L$ and $a_{ij} \in \mathcal{T}$ such that

$$\begin{aligned} \beta &= \sum_{j=0}^{q-1} b_j \otimes \pi_L^j \\ &= \sum_{(i,j)\in\mathcal{F}} a_{ij}\pi_L^i \otimes \pi_L^j. \end{aligned}$$

Let

$$R(\beta) = \{[i,j] : (i,j) \in \mathcal{F},\ a_{ij} \neq 0\}.$$

Diagrams

Definition

Define the diagram of $\beta \in L \otimes_K L$ to be

$$D(\beta) = \{[x,y] \in (\mathbb{Z} \times \mathbb{Z})/H : [i,j] \leq [x,y] \text{ for some } [i,j] \in R(\beta)\}.$$

Proposition

$D(\beta)$ does not depend on the choice of uniformizer π_L for L.

Let $G(\beta)$ denote the set of minimal elements of $D(\beta)$. Then $G(\beta)$ is also the set of minimal elements of $R(\beta)$. Furthermore, we have

$$D(\beta) = \{[x,y] \in (\mathbb{Z} \times \mathbb{Z})/H : [i,j] \leq [x,y] \text{ for some } [i,j] \in G(\beta)\}.$$

Theorem

Let $\beta \in L \otimes_K L$ be such that $\gamma := \phi(\beta) \in K[G]$. Let $[a,b] \in G(\beta)$. Then for all $y \in L$ with $v_L(y) = -b - i_0$ we have $v_L(\gamma(y)) = a$.

An Example

Let $q = 9$ and set

$$\beta = \pi_L^5 \otimes \pi_L + \pi_L^3 \otimes \pi_L^3 - \pi_L^3 \otimes \pi_L^5 - 1 \otimes \pi_L^7 + \pi_L^{-3} \otimes \pi_L^6.$$

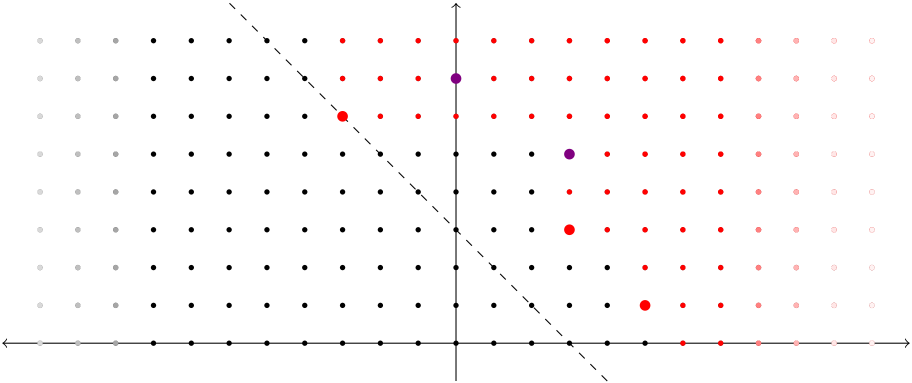
We get

$$R(\beta) = \{[5,1],[3,3],[3,5],[0,7],[-3,6]\}$$
$$G(\beta) = \{[5,1],[3,3],[-3,6]\}.$$

The subset of $\mathcal{F}$ corresponding to $D(\beta)$ is ...

Example Diagram

$$q = 9, \;\; \beta = \pi_L^5 \otimes \pi_L + \pi_L^3 \otimes \pi_L^3 - \pi_L^3 \otimes \pi_L^5 - 1 \otimes \pi_L^7 + \pi_L^{-3} \otimes \pi_L^6$$



Diagonals

For $\beta \in L \otimes_K L$ with $\beta \neq 0$ define

$$d(\beta) = \min\{i + j : [i, j] \in D(\beta)\}.$$

Define the (lower) diagonal of β to be

$$N(\beta) = \{[i, j] \in D(\beta) : i + j = d(\beta)\}.$$

Then $N(\beta) \subset G(\beta)$.

In the preceding example we have $d(\beta) = 3$ and $N(\beta) = \{[-3, 6]\}$.

Semistable Extensions

Definition

Say that the extension L/K is semistable if there is $\beta \in L \otimes_K L$ such that $\phi(\beta) \in K[G]$, $p \nmid d(\beta)$, and $|N(\beta)| = 2$.

As a lame example, let $K = \mathbb{Q}_2$, $L = \mathbb{Q}_2(\sqrt{3})$ and $G = \mathrm{Gal}(L/K) = \langle \sigma \rangle$. Set $\pi_L = \sqrt{3} - 1$, so that $\pi_L^2 + 2\pi_L - 2 = 0$ and $\sigma(\pi_L) = -\pi_L - 2$. Then $\beta = \pi_L \otimes 1 + (1 + \pi_L) \otimes \pi_L$ satisfies

$$\begin{aligned}\phi(\beta) &= 2\pi_L + \pi_L^2 + (\pi_L + (1 + \pi_L)(-2 - \pi_L))\sigma \\ &= 2 - 4\sigma \in \mathbb{Q}_2[G]\end{aligned}$$

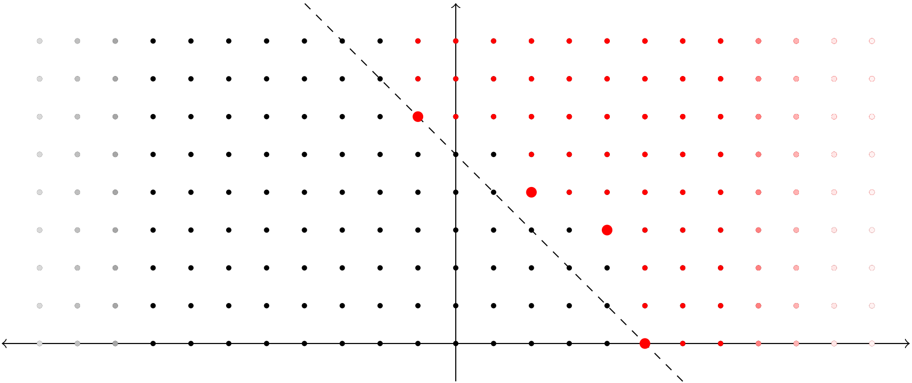
$$N(\beta) = G(\beta) = \{[1, 0], [0, 1]\}.$$

Since $d(\beta) = 1$ is not divisible by 2 we deduce that L/K is a semistable extension.

Diagram for a Semistable Extension

$$q = 9, \;\; \beta = a_{50}\pi_L^5 \otimes 1 + a_{43}\pi_L^4 \otimes \pi_L^3 + a_{24}\pi_L^2 \otimes \pi_L^4 + a_{-1,6}\pi_L^{-1} \otimes \pi_L^6$$

$$G(\beta) = R(\beta) = \{[5,0],[4,3],[2,4],[-1,6]\}, \;\; N(\beta) = \{[5,0],[-1,6]\}$$



Smallest Shift Elements

Definition

Say that $y \in L$ is a smallest shift element for L/K if for every $\gamma \in K[G]$ with $\gamma \neq 0$ we have $\hat{v}_L(\gamma) = v_L(\gamma(y)) - v_L(y)$.

Theorem

Assume that $q = [L : K]$ is a power of p, and that $\mathfrak{D} \not\subset q\mathcal{O}_L$. Then the following statements are equivalent:

1. *The extension L/K is semistable.*
2. *There exists a smallest shift element y for L/K.*
3. *Every $y \in L$ such that $v_L(y) \equiv -i_0 \pmod{q}$ is a smallest shift element for L/K.*

Properties of Semistable Extensions

Theorem

Let L/K be a semistable extension. Then

1. $p \nmid i_0$.
2. *If b is a lower ramification break of L/K then* $b \equiv -i_0 \pmod{q}$.

Galois Modules and Semistable Extensions

Theorem

Let L/K be a semistable extension. Then for all $n \in \mathbb{Z}$ there is an isomorphism of $\mathcal{O}_K[G]$-modules $\mathfrak{A}_n \cong \mathcal{M}_L^{n-i_0}$.

Theorem

Let L/K be a semistable extension. Then $\mathfrak{A}(\mathcal{M}_L^{-i_0}) = \mathfrak{A}_0$.

Corollary

Let L/K be a semistable extension. Then $\mathcal{M}_L^{-i_0}$ is a free $\mathfrak{A}(\mathcal{M}_L^{-i_0})$-module of rank 1.