Bondarko's work on local Galois modules

Part II: How he did it

Kevin Keating
Department of Mathematics
University of Florida

May 22, 2018

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 $G = \mathrm{Gal}(L/K)$.

A Pairing on $L[G]$

By viewing elements of $L[G]$ as K-endomorphisms of L we get an isomorphism $L[G] \cong \mathrm{End}_K(L)$. If we replace $L[G]$ with the smash product $L\#K[G]$ this becomes an isomorphism of K-algebras.

Define a K-bilinear pairing $L[G] \times L[G] \to K$ by

$$\left\langle \sum_{\sigma\in G} a_\sigma \sigma, \sum_{\sigma\in G} b_\sigma \sigma \right\rangle_{L[G]} = \sum_{\sigma\in G} \mathrm{Tr}_{L/K}(a_\sigma b_\sigma).$$

It follows from the nondegeneracy of the trace pairing that $\langle\ ,\ \rangle_{L[G]}$ is nondegenerate.

A Pairing on $L \otimes_K L$

Define a K-bilinear pairing $(L \otimes_K L) \times (L \otimes_K L) \to K$ by setting

$$\langle a \otimes b, c \otimes d \rangle_{\otimes} = \mathrm{Tr}_{L/K}(ac) \cdot \mathrm{Tr}_{L/K}(bd).$$

Then $\langle \ , \ \rangle_{\otimes}$ is well-defined.

Proposition

$\langle \ , \ \rangle_{\otimes}$ is nondegenerate.

Proof: Let $\{x_1, x_2, \ldots, x_q\}$ be a basis for L over K, and let A be the matrix of the trace pairing $L \times L \to K$ with respect to this basis.

Then the matrix B of $\langle \ , \ \rangle_{\otimes}$ with respect to the K-basis $\{x_i \otimes x_j : 1 \leq i, j \leq q\}$ for $L \otimes_K L$ is a Kronecker product of A with itself. Since A is invertible, so is B.

The Maps ϕ and ψ_σ

Let $T = \sum_{\sigma \in G} \sigma$ be the trace element of $L[G]$. Define a K-linear map $\phi : L \otimes_K L \to L[G]$ by

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

Then for $\alpha \in L \otimes_K L$ we get

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

For $c \in L$ we have

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

ϕ is an isometry

Proposition

For $\alpha, \beta \in L \otimes_K L$ we have $\langle \phi(\alpha), \phi(\beta) \rangle_{L[G]} = \langle \alpha, \beta \rangle_{\otimes}$.

Proof: Let $a, b, c, d \in L$. Then

$$
\begin{aligned}
\langle \phi(a \otimes b), \phi(c \otimes d) \rangle_{L[G]} &= \left\langle \sum_{\sigma \in G} a\sigma(b)\sigma, \sum_{\sigma \in G} c\sigma(d)\sigma \right\rangle_{L[G]} \\
&= \sum_{\sigma \in G} \mathrm{Tr}_{L/K}(ac \cdot \sigma(bd)) \\
&= \mathrm{Tr}_{L/K}(ac) \cdot \mathrm{Tr}_{L/K}(bd) \\
&= \langle a \otimes b, c \otimes d \rangle_{\otimes}.
\end{aligned}
$$

The claim follows from this.

ϕ is an isomorphism

Proposition

ϕ is an isomorphism of K-vector spaces.

Proof: Suppose $\alpha \in \ker(\phi)$. Then for all $\beta \in L \otimes_K L$ we get

$$\langle \alpha, \beta \rangle_{\otimes} = \langle \phi(\alpha), \phi(\beta) \rangle_{L[G]} = \langle 0, \phi(\beta) \rangle_{L[G]} = 0.$$

Hence $\alpha = 0$ by the nondegeneracy of $\langle \ , \ \rangle_{\otimes}$. Therefore ϕ is one-to-one.

Since $\dim(L \otimes_K L) = \dim(L[G]) = q^2$ it follows that ϕ is also onto.

Some Lattices in $L[G]$ and $K[G]$

Let I_1 and I_2 be fractional ideals of $\mathcal{O}_L$. Define

$$\begin{aligned} \mathfrak{C}(I_1, I_2) &= \mathrm{Hom}_{\mathcal{O}_K}(I_1, I_2) \\ \mathfrak{A}(I_1, I_2) &= \mathfrak{C}(I_1, I_2) \cap K[G] \\ \mathfrak{A}(I_1) &= \mathfrak{A}(I_1, I_1). \end{aligned}$$

Let $\mathfrak{D} = \mathcal{M}_L^d$ denote the different of the extension L/K.

Duals of Lattices

Definition

Suppose M and N are $\mathcal{O}_K$-lattices in L. Let M^* denote the dual of M with respect to the trace pairing, and let $(M \otimes_{\mathcal{O}_K} N)^*$ denote the dual of $M \otimes_{\mathcal{O}_K} N$ with respect to $\langle\ ,\ \rangle_{\otimes}$.

Lemma

Let M, N be $\mathcal{O}_K$-lattices in L. Then $(M \otimes_{\mathcal{O}_K} N)^* = M^* \otimes_{\mathcal{O}_K} N^*$.

Proof: Let $\{x_1, \ldots, x_q\}$, $\{y_1, \ldots, y_q\}$ be $\mathcal{O}_K$-bases for M, N. Let $\{x_1^*, \ldots, x_q^*\}$, $\{y_1^*, \ldots, y_q^*\}$ be the dual bases with respect to the trace pairing. Then $\{x_i \otimes y_j : 1 \le i, j \le q\}$ is an $\mathcal{O}_K$-basis for $M \otimes_{\mathcal{O}_K} N$, and $\{x_i^* \otimes y_j^* : 1 \le i, j \le q\}$ is the dual basis with respect to $\langle\ ,\ \rangle_{\otimes}$. Hence

$$(M \otimes_{\mathcal{O}_K} N)^* = \mathrm{Span}_{\mathcal{O}_K}\{x_i^* \otimes y_j^* : 1 \le i, j \le q\} = M^* \otimes_{\mathcal{O}_K} N^*.$$

Characterizing $\mathfrak{C}(I_1, I_2)$

Proposition

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

Proof: First, if $a \in I_2$, $b \in \mathfrak{D}^{-1} I_1^{-1}$, and $x \in I_1$ then $\phi(a \otimes b)(x) = a\mathrm{Tr}_{L/K}(bx)$. Since $bx \in \mathfrak{D}^{-1}$ we get $\mathrm{Tr}_{L/K}(bx) \in \mathcal{O}_K$, and hence $\phi(a \otimes b)(x) \in I_2$. Thus $\phi(I_2 \otimes \mathfrak{D}^{-1} I_1^{-1}) \subset \mathfrak{C}(I_1, I_2)$.

Now let $f \in \mathfrak{C}(I_1, I_2)$. Define

$$\theta_f : \mathfrak{D}^{-1} I_2^{-1} \otimes_{\mathcal{O}_K} I_1 \longrightarrow \mathcal{O}_K$$

by setting

$$\theta_f(a \otimes b) = \mathrm{Tr}_{L/K}(af(b)).$$

Then θ_f is an $\mathcal{O}_K$-module homomorphism.

Characterizing $\mathfrak{C}(I_1, I_2)$ ...

By the nondegeneracy of $\langle\ ,\ \rangle_\otimes$ there is $\alpha \in L \otimes_K L$ such that $\theta_f(\beta) = \langle \alpha, \beta \rangle_\otimes$ for all $\beta \in \mathfrak{D}^{-1} I_2^{-1} \otimes_{\mathcal{O}_K} I_1$.

It follows from the lemma that

$$\begin{aligned}
\alpha \in (\mathfrak{D}^{-1} I_2^{-1} \otimes_{\mathcal{O}_K} I_1)^* &= (\mathfrak{D}^{-1} I_2^{-1})^* \otimes_{\mathcal{O}_K} I_1^* \\
&= \mathfrak{D}^{-1} (\mathfrak{D}^{-1} I_2^{-1})^{-1} \otimes \mathfrak{D}^{-1} I_1^{-1} \\
&= I_2 \otimes \mathfrak{D}^{-1} I_1^{-1}.
\end{aligned}$$

Characterizing $\mathfrak{C}(I_1, I_2)$ ...

We have $f = \sum_{\sigma \in G} a_\sigma \sigma$ for some $a_\sigma \in L$. For $x \in \mathfrak{D}^{-1} I_2^{-1}$, $y \in I_1$ we get

$$\begin{aligned}
\langle \phi(\alpha), \phi(x \otimes y) \rangle_{L[G]} &= \langle \alpha, x \otimes y \rangle_{\otimes} \\
&= \theta_f(x \otimes y) \\
&= \mathrm{Tr}_{L/K}(xf(y)) \\
&= \sum_{\sigma \in G} \mathrm{Tr}_{L/K}(a_\sigma \cdot x\sigma(y)) \\
&= \left\langle \sum_{\sigma \in G} a_\sigma \sigma, \sum_{\sigma \in G} x\sigma(y)\sigma \right\rangle_{L[G]} \\
&= \langle f, \phi(x \otimes y) \rangle_{L[G]}.
\end{aligned}$$

Hence for all $\beta \in L \otimes_K L$ we have $\langle \phi(\alpha), \phi(\beta) \rangle_{L[G]} = \langle f, \phi(\beta) \rangle_{L[G]}$. It follows from the nondegeneracy of $\langle\ ,\ \rangle_{L[G]}$ that $\phi(\alpha) = f$.

A partial order

Let $H = \langle (q, -q) \rangle \leq \mathbb{Z} \times \mathbb{Z}$

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

For $[a, b], [c, d] \in (\mathbb{Z} \times \mathbb{Z})/H$ say $[a, b] \leq [c, d]$ if there is $t \in \mathbb{Z}$ such that $a \leq c + tq$ and $b \leq d - tq$.

Lemma

Let $[h, k], [a, b] \in (\mathbb{Z} \times \mathbb{Z})/H$. *Then*

$$[h, k] \not\leq [a, b] \Leftrightarrow [a + 1, b - q + 1] \leq [h, k].$$

Proof: Suppose $[h, k] \not\leq [a, b]$. We may assume that $h \leq a \leq h + q - 1$. Then $k \geq b + 1$. Hence

$$[a + 1, b - q + 1] = [a - q + 1, b + 1] \leq [h, k].$$

The proof of the converse is similar.

Diagrams

We have coset representatives for $(\mathbb{Z} \times \mathbb{Z})/H$:

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

Let $\mathcal{T}$ be the set of Teichmüller representatives of K.

Given $\beta \in L \otimes_k L$ there are $a_{ij} \in \mathcal{T}$ such that

$$\beta = \sum_{(i,j) \in \mathcal{F}} a_{ij} \pi_L^i \otimes \pi_L^j.$$

Define

$$R(\beta) = \{[i, j] : (i, j) \in \mathcal{F}, a_{ij} \neq 0\}$$
$$D(\beta) = \{[h, k] \in (\mathbb{Z} \times \mathbb{Z})/H : [i, j] \leq [h, k] \text{ for some } [i, j] \in R(\beta)\}$$
$$G(\beta) = \{[a, b] \in D(\beta) : [a, b] \text{ minimal }\}.$$

Shifts Associated to $[a, b] \in G(\beta)$

Theorem

Let $\beta \in L \otimes_K L$ and let $[a, b] \in G(\beta)$. Then for all $y \in L$ with $v_L(y) = -b - i_0$ we have $v_L(\phi(\beta)(y)) = a$.

Proof: It follows from the minimality of $[a, b]$ that for all $[h, k] \in D(\beta) \smallsetminus \{[a, b]\}$ we have $[h, k] \not\leq [a, b]$. It follows by the lemma that $[a + 1, b - q + 1] \leq [h, k]$.

Therefore there are $c_{ij} \in \mathcal{T}$ and $c \in \mathcal{T} \smallsetminus \{0\}$ with

$$\beta = c\pi_L^a \otimes \pi_L^b + (\pi_L^{a+1} \otimes \pi_L^{b-q+1}) \sum_{i,j \geq 0} c_{ij}\pi_L^i \otimes \pi_L^j$$

$$\phi(\beta)(y) = c\pi_L^a \mathrm{Tr}_{L/K}(\pi_L^b y) + \sum_{i,j \geq 0} c_{ij}\pi_L^{a+1+i}\mathrm{Tr}_{L/K}(\pi_L^{b-q+1+j} y).$$

Shifts Associated to $[a, b] \in G(\beta)$ ...

Since $v_L(\pi_L^b y) = -i_0$ we have $v_K(\mathrm{Tr}_{L/K}(\pi_L^b y)) = 0$. Hence

$$v_L(c\pi_L^a \mathrm{Tr}_{L/K}(\pi_L^b y)) = a.$$

In addition, since

$$v_L(\pi_L^{b-q+1+j} y) \geq -i_0 - q + 1 = -d$$

we have $\mathrm{Tr}_{L/K}(\pi_L^{b-q+1+j} y) \in \mathcal{O}_K$, and hence

$$v_L(\pi_L^{a+1+i} \mathrm{Tr}_{L/K}(\pi_L^{b-q+1+j} y)) > a.$$

We conclude that $v_L(\phi(\beta)(y)) = a$.

Shifts of Endomorphisms of L

Theorem

Let $\beta \in L \otimes_K L$ with $\beta \neq 0$ and let $u \in \mathbb{Z}$. Let $b \in \mathbb{Z}$ be maximum such that $b \leq u$ and $[a, b] \in G(\beta)$ for some a. Then

$$\min\{v_L(\phi(\beta)(x)) : v_L(x) = -i_0 - u\} = a.$$

Proof: If $b = u$ then the claim follows from the previous theorem.

Suppose $b < u$. Our choice of b implies that $[a-1, u] \notin D(\beta)$. Therefore for all $[h, k] \in D(\beta)$ we have $[h, k] \not\leq [a-1, u]$. Hence by the lemma we get $[a, u-q+1] \leq [h, k]$.

Shifts of Endomorphisms of L ...

It follows that there are $c_{ij} \in \mathcal{T}$ such that

$$\beta = (\pi_L^a \otimes \pi_L^{u-q+1}) \sum_{i,j \geq 0} c_{ij} \pi_L^i \otimes \pi_L^j.$$

Let $x \in L$ with $v_L(x) = -i_0 - u$. Then

$$\phi(\beta)(x) = \sum_{i,j \geq 0} c_{ij} \pi_L^{a+i} \mathrm{Tr}_{L/K}(\pi_L^{u-q+1+j} x).$$

Since

$$v_L(\pi_L^{u-q+1+j} x) \geq -i_0 - q + 1 = -d$$

we have $\mathrm{Tr}_{L/K}(\pi_L^{u-q+1+j} x) \in \mathcal{O}_K$. Hence $v_L(\phi(\beta)(x)) \geq a$.

Shifts of Endomorphisms of L ...

Suppose $v_L(\beta(x)) > a$. There is $y \in L$ with

$$v_L(y) = -i_0 - b > -i_0 - u = v_L(x)$$

and hence

$$v_L(\phi(\beta)(y)) = a < v_L(\phi(\beta)(x))$$

by the previous theorem. It follows that

$$\begin{aligned} v_L(x+y) &= -i_0 - u \\ v_L(\beta(x+y)) &= v_L(\beta(x) + \beta(y)) = a. \end{aligned}$$

Hence we can choose x with $v_L(x) = -i_0 - u$ and $v_L(\phi(\beta)(x)) = a$.

Some Definitions

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

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

For $n \in \mathbb{Z}$ let

$$\mathfrak{C}_n = \{\gamma \in \mathrm{End}_K(L) : \hat{v}_L(\gamma) \geq n\}.$$

Also let X_n be the $\mathcal{O}_K$-submodule of $L \otimes_K L$ generated by all elements of the form $c \otimes d$, with $v_L(c) + v_L(d) \geq n$.

Characterizing $\mathfrak{C}_n$

Theorem

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

Proof: Let $c \otimes d \in L \otimes L$ with $v_L(c) = h$, $v_L(d) = k$ such that $h + k \geq n - i_0$. Let $x \in L^\times$ satisfy $v_L(x) = -i_0 - u$ and $k \leq u < k + q$. We have $G(c \otimes d) = \{[h, k]\}$, so by the previous theorem we get

$$\begin{aligned} v_L(\phi(c \otimes d)(x)) - v_L(x) &\geq h - (-i_0 - u) \\ &\geq h + i_0 + k \\ &\geq n. \end{aligned}$$

Hence $\phi(X_{n-i_0}) \subset \mathfrak{C}_n$.

Characterizing $\mathfrak{C}_n$ . . .

On the other hand, suppose $\beta \in L \otimes_K L$ satisfies $\phi(\beta) \in \mathfrak{C}_n$.

By the previous theorem but one we get $a - (-i_0 - b) \geq n$ for all $[a, b] \in G(\beta)$.

It follows that $h + k + i_0 \geq n$ for all $[h, k] \in D(\beta)$. Hence $\beta \in X_{n-i_0}$.

We conclude that $\mathfrak{C}_n \subset \phi(X_{n-i_0})$.