A pseudo-associated order

Daniel Miller

November 12, 2012

This note is essentially an explication of the arguments in the first section of Bondarko's paper [Bon00].

1 Duality for group algebras

Let k be a commutative ring, Γ a finite group. We can consider the group algebra $k[\Gamma]$ as a Hopf algebra in the usual way. The dual of $k[\Gamma]$ is spanned as a k-module by the functionals $\hat{\sigma}(\tau) = \delta_{\sigma\tau}$. Instead of using different notation for $k[\Gamma]$ and its dual, we will use the $*$ to denote the product in the dual of $k[\Gamma]$. In other words,

$$\left(\sum a_\sigma \sigma\right) * \left(\sum b_\sigma \sigma\right) = \sum a_\sigma b_\sigma \sigma.$$

For the rest of this note, the *standard situation* consists of a Dedekind domain $\mathfrak{o}$ with field of fractions k, along with a finite Galois extension K/k. Put $\Gamma = \mathrm{Gal}(K/k)$, and write $\mathfrak{O}$ for the integral closure of $\mathfrak{o}$ in K. For fractional ideals $\mathfrak{a}, \mathfrak{b} \subset \mathfrak{O}$, put

$$\mathfrak{A}(\mathfrak{a}, \mathfrak{b}) = \{f \in k[\Gamma] : f\mathfrak{a} \subset \mathfrak{b}\}.$$

Write $\mathfrak{A} = \mathfrak{A}(\mathfrak{O}, \mathfrak{O})$. Note that $\mathfrak{A}$ is not, in general, closed under the multiplication $*$. We will define an $\mathfrak{o}$-subalgebra $Q \subset k[\Gamma]$ that is closed under $*$, and show that in certain instances, Q is monogenic under $*$, and gives an easily computable $\mathfrak{o}$-basis for $\mathfrak{A}$.

2 General nonsense with projectives

As before, let k be an arbitrary commutative ring. If E is a k-module, write $E^\vee = \hom_k(E, k)$. If E, F are finitely generated projective k-modules, there is a natural isomorphism

$$E^\vee \otimes F \xrightarrow{\sim} \hom(E, F) \qquad f \otimes x \mapsto f(-)x.$$

Return to the standard situation. There is a natural isomorphism $K[\Gamma] \to \hom_k(K, K)$. For fractional ideals $\mathfrak{a}, \mathfrak{b} \subset K$ put

$$\mathfrak{C}(\mathfrak{a}, \mathfrak{b}) = \hom_{\mathfrak{o}}(\mathfrak{a}, \mathfrak{b}) = \{f \in K[\Gamma] : f\mathfrak{a} \subset \mathfrak{b}\}.$$

If $\mathfrak{a} \subset K$ is a fractional ideal, we may identify $\mathfrak{a}^\vee$ with $\mathfrak{a}^* := \{x \in K : \mathrm{tr}(x\mathfrak{a}) \subset \mathfrak{o}\}$ via

$$\mathfrak{a}^* \to \mathfrak{a}^\vee \qquad x \mapsto \mathrm{tr}(x-).$$

In light of the above identifications, we have the following isomorphism of $\mathfrak{o}$-modules:

$$\mathfrak{a}^* \otimes \mathfrak{b} \xrightarrow{\sim} \mathfrak{a}^\vee \otimes \mathfrak{b} \xrightarrow{\sim} \hom_{\mathfrak{o}}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{C}(\mathfrak{a}, \mathfrak{b}) \qquad x \otimes y \mapsto \sum \sigma(x) y \sigma.$$

This suggests we define a map

$$\phi : K \otimes K \to K[\Gamma] \qquad x \otimes y \mapsto \sum \sigma(x) y \sigma.$$

It is well-known that if we give $K[\Gamma]$ the multiplication $*$, then ϕ is an isomorphism of k-algebras.

Write $\mathfrak{D}^{-1} = \mathfrak{O}^*$ for the inverse different of the extension K/k.

Definition 2.1. $Q = \mathfrak{C}(\mathfrak{D}^{-1}, \mathfrak{O}) \cap k[\Gamma]$.

Since $Q = \mathfrak{O} \otimes \mathfrak{O}$ as a subset of $K \otimes K$, it is closed under $*$.

3 Local fields

We remain in the standard situation, and moreover assume that K/k is a totally ramified extension of local fields. Write $\mathfrak{p}$ (resp. $\mathfrak{P}$) for the maximal ideal of $\mathfrak{o}$ (resp. $\mathfrak{O}$). We also assume that $\mathfrak{D} = \delta\mathfrak{O}$ for some $\delta \in k$. We call such extensions *perfectly ramified*. In this case, one has $Q = \delta\mathfrak{A}$. As a result, $\mathfrak{O}$ is free over $\mathfrak{A}$ if and only if $\mathfrak{O} = Qx$ for some $x \in \mathfrak{D}^{-1}$.

For the moment, we drop the assumption that K/k is perfectly ramified (but still assume it is totally ramified). Let $n = [K : k]$ and let v be the normalized valuation on K. Put $d = v(\mathfrak{D})$ and $r = n - d - 1$.

Theorem 3.1. *If $v(a) = r$, then $\operatorname{tr} a \in \mathfrak{o}^\times$.*

Proof. Let $\pi \in K$ be a uniformizer, $f \in \mathfrak{o}[X]$ its minimal polynomial. It is well-known that $d = v(f'(\pi))$. So, if we let $x = \pi^{n-1}/f'(\pi)$, then $v(x) = n - d - 1$, and by a theorem of Euler, $\operatorname{tr} x = 1$. If $v(y) = v(x)$, then $y = \varepsilon x + z$, where $\varepsilon \in \mathfrak{o}^\times$ and $v(z) > 0$. Then $v(\operatorname{tr} z) > 0$, so $\operatorname{tr} y = \varepsilon + \operatorname{tr} z \in \mathfrak{o}\times$. □

Theorem 3.2. *Let $\alpha = 1 \otimes x + \sum x_i \otimes y_i \in \mathfrak{O} \otimes \mathfrak{O}$ with $v(x) < n$ and $v(x_i) > 0$. If $v(a) = r$, then $v(\phi(\alpha)(a)) = v(x)$.*

Proof. Consider the following computation, where π_0 is a uniformizer in $\mathfrak{o}$:

$$\begin{aligned}\phi(\alpha)(a) &= x \operatorname{tr}(a) + \sum \operatorname{tr}(x_i a) y_i \\ &= x \operatorname{tr}(a) + \sum \pi_0 y_i \operatorname{tr}\left(\frac{x_i a}{\pi_0}\right).\end{aligned}$$

Since $v(a) = r$, the arguments of the trace on the right have valuation at least $-d$, so the sum on the right has valuation $> n$, whence the result. □

In particular, if $\operatorname{tr} a = 1$, then $\phi(\alpha)(a) \equiv x \pmod{\mathfrak{P}^e}$, where $e = v(\mathfrak{p})$ is the index of ramification.

Theorem 3.3. *Let $f, g \in Q$ and $v(a) = r$. If $v(f(a)) = i$, $v(g(a)) = j$ and $i, j, i + j < n$, then $v((f * g)(a)) = i + j$.*

Proof. Write $f = \phi(\alpha)$, $g = \phi(\beta)$ where $\alpha = 1 \otimes x + \sum x_i \otimes y_i$ and $\beta = 1 \times u + \sum u_j \otimes v_j$ as in Theorem 3.2. Then $v(x) = i$ and $v(y) = j$. We have

$$f * g = \phi(\alpha\beta) = 1 \otimes ux + \sum x_i u_j \otimes y_i v_j.$$

By Theorem 3.2, it follows that $(f * g)(a)$ has valuation $v(ux) = i + j$. □

As a matter of fact, note that if $\operatorname{tr} a = 1$, then $(f * g)(a) \equiv f(a)g(a) \pmod{\mathfrak{P}^e}$.

For $f \in K[\Gamma]$, define $f^{*0} = \operatorname{tr}$, and $f^{*(i+1)} = f * f^{*i}$. If $f \in Q$, then $f^{*i} \in Q$ for all i. Suppose $v(f(a)) = 1$ for some a with $v(a) = r$. Then by Theorem 3.3, $f^{*i}(a)$ has valuation i for all $0 \leqslant i < n$. Thus $\{f^{*0}(a), \ldots, f^{*(n-1)}(a)\}$ is an $\mathfrak{o}$-basis for $\mathfrak{O}$.

Theorem 3.4. *If $v(a) = r$ and $f(a)$ is a uniformizer, then $\{f^{*0}, \ldots, f^{*(n-1)}\}$ is an $\mathfrak{o}$-basis for Q.*

Proof. First note that the f^{*i} form a k-basis for $K[\Gamma]$. Moreover, for $g \in k[\Gamma]$, $g = 0$ if and only if $g(a) = 0$. Indeed, writing $g = \sum a_i f^{*i}$, we get $g(a) = \sum a_i f^{*i}(a)$. The ith term on the right has valuation $i \pmod{n}$, so the only way $g(a)$ can be zero is for each $a_i = 0$. Thus if $g \in Q$, then we have $g(a) = a_i f^{*i}(a)$ for some $a_i \in \mathfrak{o}$ for each $0 \leqslant i < n$. It follows that $g - \sum a_i f^{*i}$ kills a, whence $g = \sum a_i f^{*i}$. □

4 Back to the associated order

Suppose K/k is perfectly ramified, that is $\mathfrak{D} = \mathfrak{O}\delta$ for $\delta \in k$. Then $\mathfrak{A} = \delta^{-1}Q$. So, if there exists $f \in Q$ such that $f(a)$ is prime for some a with $v(a) = r$, we have $\mathfrak{A} \cdot a = \mathfrak{O}$, and $\{\delta^{-1} f^{*i}\}$ forms an $\mathfrak{o}$-basis for $\mathfrak{A}$.

Theorem 4.1. *$\mathfrak{A}$ is Hopf if and only if $\Delta(\delta^{-1}\operatorname{tr}) \in \mathfrak{A} \otimes \mathfrak{A}$.*

Proof. Since Δ is k-linear, it suffices to prove that $\Delta(Q) \subset \mathfrak{A} \otimes Q$ if and only if $\Delta(\operatorname{tr}) \in \mathfrak{A} \otimes Q$. In fact, this always holds (even if K/k is not perfectly ramified). One implication is obvious. To prove the other, we show that for $f \in k[\Gamma]$, we have

$$\Delta(f) = (f \otimes \operatorname{tr}) * \Delta(\operatorname{tr}).$$

Indeed, writing $f = \sum a_\sigma \sigma$, we compute

$$\begin{aligned}\Delta(f) &= \sum a_\sigma \sigma \otimes \sigma \\ &= \left(\sum_{a,\tau} a_\sigma \sigma \otimes \tau\right) * \left(\sum_{\gamma} \gamma \otimes \gamma\right) \\ &= (f \otimes \operatorname{tr}) * \Delta(\operatorname{tr}).\end{aligned}$$

Since $\Delta(\operatorname{tr}) \in \mathfrak{A} \otimes Q$ and $(Q \otimes Q)(\mathfrak{A} \otimes Q) \subset \mathfrak{A} \otimes Q$, the result follows. □

5 Functoriality

Finally, we show that Q is functorial in K. Let K'/K be a finite Galois extension, $\Gamma' = \operatorname{Gal}(K'/K)$, and $G = \operatorname{Gal}(K'/k)$. There is an obvious functorial surjection $\Gamma' \twoheadrightarrow \Gamma$. This extends to a (functorial) map of k-Hopf algebras $k[\Gamma'] \to k[\Gamma]$. It induces an injection $\rho : k[\Gamma]^\vee \to k[\Gamma']^\vee$, via

$$\rho(\sigma) = \sum_{\tau \mapsto \sigma} \tau.$$

One can easily check that if $f \in Q_K$, then $\rho(f) \in Q_{K'}$. Since the maps $\Gamma' \to \Gamma$ are functorial, so are the ρ. To conclude, Q defines a functor from the category of finite Galois extensions of k to the category of $\mathfrak{o}$-algebras.

References

[Bon00] Mikhail Bondarko. “Local Leopoldt’s problem for rings of integers in abelian p-extensions of complete discrete valuation fields”. In: *Doc. Math.* 5 (2000), 657–693 (electronic).