Hereditary Associated Orders for Hopf-Galois Structures on Tame Extensions

Paul Truman

Keele University, UK

Maximal Associated Orders

- Let L/K be a finite Galois extension of p-adic fields and $H = L[N]^G$ a Hopf algebra giving a Hopf-Galois structure on the extension.
- Write $\Lambda = \mathfrak{O}_L[N]$. Note that $|N| = |G|$.

Theorem (PT)

Suppose that H is commutative and $p \nmid [L:K]$. Then Λ^G is the unique maximal order in H, $\mathfrak{A}_H = \Lambda^G$ and $\mathfrak{O}_L$ is a free Λ^G-module.

- The second and third conclusions follow from the first:
- Since Λ^G is a maximal order, it is hereditary.
- So $\mathfrak{O}_L$ is a finitely generated projective Λ^G-module.
- Also, $\mathfrak{O}_L \otimes_{\mathfrak{O}_K} K = L$ is a free $\Lambda^G \otimes_{\mathfrak{O}_K} K = H$-module of rank one.
- Since Λ^G is a maximal order, (or since H is commutative), this implies that $\mathfrak{O}_L$ is a free Λ^G-module.

Maximal Associated Orders

Theorem (PT)

Suppose that H is commutative and $p \nmid [L : K]$. Then Λ^G is the unique maximal order in H, $\mathfrak{A}_H = \Lambda^G$ and $\mathfrak{O}_L$ is a free Λ^G-module.

- Can we drop the hypothesis that H should be commutative?
- If H is noncommutative then it need not contain a unique maximal order, but if Λ^G is **a** maximal order in H, then the other conclusions will follow.
- Motivation: Hopf-Galois module structure of tame Galois extensions of degree pq. Would like to restrict attention to cases where the residue characteristic is either p or q.

Skew Group Rings

- Let R be a ring with unity and G a finite group of automorphisms of R.
- The Skew Group Ring $R * G$ is the free R-module whose basis is the elements of G, with multiplication defined by

$$(rg)(sh) = r({}^{g^{-1}}s)gh \text{ for all } r, s \in R, g, h \in G.$$

Proposition

Suppose that $|G|^{-1} \in R$, and let e denote the idempotent $\frac{1}{|G|}\sum_{g \in G} g$ of $R * G$. Then

$$R^G \cong e(R * G)e.$$

Proposition

Consider R as a right $R * G$-module. Then $R^G \cong \mathrm{End}_{R*G}(R)$.

Λ^G is a Hereditary Order

Theorem

Suppose that $p \nmid |G|$. Then $\Lambda * G$ and Λ^G are both hereditary.

Proof.

- Since $p \nmid |G| = |N|$, $\Lambda = \mathfrak{O}_L[N]$ is a maximal $\mathfrak{O}_L$-order in $L[N]$, so Λ is hereditary.
- Since Λ is hereditary and contains a central element of trace 1, $\Lambda * G$ is hereditary.
- Since $\Lambda * G$ is hereditary, $e(\Lambda * G)e \cong \Lambda^G$ is hereditary.

□

- So $\mathfrak{O}_L$ is a finitely generated projective Λ^G-module, and L is a free H-module.
- Does this imply that $\mathfrak{O}_L$ is a free Λ^G-module? One way to achieve this is to show that Λ^G is maximal.

Is Λ^G a Maximal Order?

- Continue to assume that $p \nmid |G| = |N|$.

Proposition

Suppose that Γ is a maximal $\mathfrak{O}_K$-order in a separable K-algebra A, and that M is a Γ-lattice. Then $\mathrm{End}_\Gamma(M)$ is a maximal $\mathfrak{O}_K$-order in $\mathrm{End}_A(KM)$.

- If $\Lambda * G$ is a maximal order in $L[N] * G$, then Λ is a $\Lambda * G$-lattice, and so $\mathrm{End}_{\Lambda * G}(\Lambda) \cong \Lambda^G$ is a maximal order in $\mathrm{End}_{L[N]*G}(L[N]) \cong H$.

Proposition

$\mathfrak{O}_L * G$ is a maximal order in $L * G$ is and only if L/K is unramified.

- In our case, it is certainly sufficient that L/K be unramified, but is it necessary?

Another Route: Conductors

- Suppose that Γ is a maximal $\mathfrak{O}_K$-order in H containing Λ^G.
- Define

$$\begin{aligned}\left[\Gamma, \Lambda^G\right]_l &= \left\{x \in H \mid x\Gamma \subseteq \Lambda^G\right\} \\ \left[\Gamma, \Lambda^G\right]_r &= \left\{x \in H \mid \Gamma x \subseteq \Lambda^G\right\}\end{aligned}$$

- Since Λ^G is Hereditary, we have

$$\Gamma \cdot \left[\Gamma, \Lambda^G\right]_l = \Gamma.$$

- Clearly $\left[\Gamma, \Lambda^G\right]_l$ is a right Γ-module. If it is also a left Γ-module, then we would have

$$\left[\Gamma, \Lambda^G\right]_l = \Gamma,$$

  and we would be done.
- So a sufficient condition for Λ^G to be maximal is that

$$\left[\Gamma, \Lambda^G\right]_l = \left[\Gamma, \Lambda^G\right]_r.$$

Symmetric Orders

- Call an order $\mathfrak{B}$ in a separable K-algebra A *Symmetric* if there is a nondegenerate symmetric bilinear form $\tau : \mathfrak{B} \times \mathfrak{B} \to \mathfrak{O}_K$ such $\mathfrak{B}$ is selfdual with respect to τ:

$$\mathfrak{B}^* = \{a \in A \mid \tau(a, b) \in \mathfrak{O}_K \text{ for all } b \in \mathfrak{B}\} = \mathfrak{B}.$$

Proposition

If $\mathfrak{B}$ is a symmetric order and Γ is a maximal order containing $\mathfrak{B}$ then

$$[\Gamma : \mathfrak{B}]_l = [\Gamma : \mathfrak{B}]_r \, .$$

Proposition

If $\mathfrak{B}$ is a symmetric order in A and $e \in \mathfrak{B}$ is an idempotent then $e\mathfrak{B}e$ is a symmetric order in eAe.

Symmetric Orders

- So if we can find a nondegenerate symmetric bilinear form on $L[N] * G$ with respect to which $\Lambda * G$ is selfdual, then $\Lambda^G \cong e(\Lambda * G)e$ is a symmetric order, and we will be done.
- There is a nondegenerate bilinear form on $L[N] * G$ with these properties, but it is not symmetric. It does induce a nondegenerate symmetric bilinear form on $\Lambda^G \cong e(\Lambda * G)e$, however.
- There is a nondegenerate symmetric bilinear form on H, but Λ^G is not selfdual with respect to this form!

Hattori's Theorem

- We do not actually **need** Λ^G to be maximal.
- What we need is a result such as

  "If M, N are finitely generated projective Λ^G modules and $K \otimes M \cong K \otimes N$ as $K \otimes \Lambda^G$-modules then $M \cong N$ as Λ^G-modules."
- Swan's Theorem is that such a result holds for group rings.
- One way to prove Swan's theorem is using Hattori's theorem:

Theorem (Hattori)

- *Let A be a finite $\mathfrak{O}_K$-algebra.*
- *Let $[A, A]$ be the $\mathfrak{O}_K$-submodule generated by all commutators $ab - ba$.*
- *Suppose that $A/[A, A]$ is $\mathfrak{O}_K$-torsion free.*

Then two finitely generated projective A-modules M, N are isomorphic if and only if $K \otimes M$ and $K \otimes N$ are isomorphic $K \otimes A$-modules.

Separability

- In the case of the group ring Λ, we have

$$\Lambda/[\Lambda,\Lambda] \cong Z(\Lambda) \text{ as } Z(\Lambda)\text{-modules.}$$

- Could this also be the case for Λ^G?
- We have
  - $Z(\Lambda^G) = Z(\Lambda)^G$.
  - $[\Lambda^G,\Lambda^G] \subseteq [\Lambda,\Lambda]^G$.
- A sufficient condition for

$$\Lambda^G/[\Lambda^G,\Lambda^G] \cong Z(\Lambda^G) \text{ as } \Lambda^G\text{-modules}$$

  is that Λ^G be separable over $\mathfrak{O}_K$.
- But this is stronger than Λ^G being maximal!

Separability

- In fact, it would be sufficient to show that Λ^G is separable over $Z(\Lambda^G)$ i.e. it is Azumaya.
- I can say a little about the centres:
  - $Z(\Lambda^G)$ is the unique maximal $\mathfrak{O}_K$-order in $Z(H)$
  - I think I have found a criterion for $Z(\Lambda^G)$ to be separable over $\mathfrak{O}_K$

  But neither of these seem to help very much!

- Thank you for your patience!
- Any thoughts?