HOPF GALOIS THEORY AND DESCENT

CORNELIUS GREITHER

1. Galois descent for Hopf algebras

Let N be any finite group and L/K a Galois extension of fields with group G. The canonical map $\mathrm{Aut}(N) \to \mathrm{Aut}_{Hopf}(L[N])$ is an isomorphism, and G acts trivially on the latter. Therefore 1-cocycles on G with values in $\mathrm{Aut}_{Hopf}(L[N])$ are the same thing as group homomorphisms $G \to \mathrm{Aut}(N)$. It remains to see just when two cocycles θ and θ' are cohomologous. By definition, this is the case iff there exists $\nu \in \mathrm{Aut}(N)$ such that

$$\theta'_g = \nu\theta_g\nu^{-1} \quad \text{for all } g \in G.$$

In particular, the trivial cocycle is only cohomologous to itself.

The form H_θ associated to a 1-cocycle θ is the fixed set under the semilinear action β of G on $L[N]$, where β_g acts as g on L and as θ_g on the group N.

A well-known example goes as follows. Let N be cyclic of order four, generated by t. Let $L/K = \mathbb{C}/\mathbb{R}$, and let the nontrivial element "conjugation" of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ act as inversion on N. Then H is the fixed subring of G on $\mathbb{C}[t]$ and can be described as $H = \mathbb{R}[c, s]$ with

$$c = t + t^3; \; s = i(t - t^3).$$

One finds $cs = 0, c^2 + s^2 = 4$ and $\Delta c = (c \otimes c - s \otimes s)/2, \Delta s = (c \otimes s + s \otimes c)/2$.

Generally, the L/K-forms of the Hopf algebra $K[N]$ are classified by the pointed set $\mathrm{Hom}(G, \mathrm{Aut}(N))$ modulo the relation "cohomologous", see above.

2. The cases $N = D_p,\ N = D_4,\ N = Q_8$

We begin with some general facts. If G is arbitrary and N is chosen to be G, then there is a particular Hopf form H_λ of $K[G]$. It is defined by $\theta : G \to \mathrm{Aut}(G)$, $g \mapsto c_g$ (conjugation with g). From what we said in §1 it easily follows that for nonabelian G, H_λ is never trivial as a Hopf form. But let us anticipate that for every G, H_λ will turn out to be *trivial as a form in the category of K-algebras.* This was first noted by Rob Underwood in the particular case $K = \mathbb{Q}$ and $G = S_3$.

In the preprint [KKTU17] the case $G = D_p$ is considered. If one insists on having a Hopf Galois situation, there are exactly three possible cases.

$$\begin{aligned} N &= D_p, \qquad H = K[N]; \\ N &= D_p, \qquad H = H_\lambda; \\ N &= C_{2p}. \end{aligned}$$

In the last case, $\theta : G \to \mathrm{Aut}(N)$ factors through $D_p \to C_2$, and the nontrivial element of C_2 acts as inversion on N. As an algebra, $H_\theta \cong K \times K \times M^{p-1}$, where M is the unique quadratic subfield of L/K.

The paper [KKTU19] (JPAA) considers $G = C_p \times C_p$. All eligible N are isomorphic to G, and G acts on N via some quotient $\bar{G}$ of order p. A generator of that quotient acts on N via the unipotent matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Assuming $\zeta_p \in K$, the authors establish that two occurring forms H and H' are isomorphic as algebras if and only they are isomorphic as Hopf algebras. In the nontrivial cases one has $H \cong K^p \times L_i^{p-1}$, where L_i ranges over the proper intermediate fields of L/K.

Finally we mention [TT19] (NYJM). This concerns $G = Q_8$, the quaternion group. Here all five groups N of order 8 can appear in a Hopf Galois context! We only discuss the two cases where N is not abelian. For $N = Q_8$, one only finds the Hopf forms H_θ one expects anyway: the trivial one, and H_λ. For $N = D_4$, the situation is more intricate. There are six Hopf Galois structures. The resulting Hopf algebras are pairwise non-isomorphic. As K-algebras, they all have the form $K^4 \times D$ where D is four-dimensional and central simple over K. The interesting point is that D can be a matrix algebra, just as well as a skew field. This depends on the quadratic subfields M of L, and whether -1 is a norm in M/K.

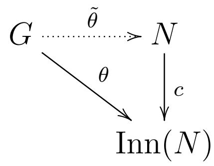
3. Trivial algebra structure

We keep all notation. Let $\theta : G \to \mathrm{Aut}(N)$ be any homomorphism; we recall this is the same as a 1-cocycle $G \to \mathrm{Aut}_{Hopf}\, L[N]$. As usual, $\mathrm{Inn}(N)$ denotes the group of inner automorphisms of N; this is a normal subgroup of $\mathrm{Aut}(M)$, and via the map $c : g \to c_g$ isomorphic to G modulo its center.

Definition:

(a) θ is an *inner* cocycle $\iff$ $\theta(G) \subset \mathrm{Inn}(N)$. If θ is not inner, we call it *outer*.

(b) An inner cocycle θ is *liftable,* if the following diagram can be filled by a group homomorphism $\tilde{\theta}$:



Remarks: (1) These notions are well behaved with respect to the relation "cohomologous".

(2) One puts $\mathrm{Out}(N) = \mathrm{Aut}(N)/\,\mathrm{Inn}(N)$. Then of course, if $\mathrm{Out}(N)$ is trivial, all cocycles are inner.

(3) If N has trivial center, then all inner cocycles are liftable.

The main result of this section is the following.

Theorem 3.1. *If the cocycle θ is inner and liftable, then the Hopf form H_θ attached to it is trivial as an algebra, that is, isomorphic to $K[N]$.*

Sketch proof: Show that the class $[\theta]$ comes from $\mathrm{H}^1(G, L[N]^\times)$; extract from the literature (or prove by hand) that this cohomology set is trivial (a generalization of Hilbert 90).

As a **Corollary,** we obtain that H_λ is always trivial as an algebra form. The simple reason is that the cocycle defining it is inner liftable. In fact the cocycle is c, and in a way this is the *universal inner liftable cocycle.*

4. Potentially nontrivial algebra structure

Above we said that for $G = Q_8$ and $N = D_4$, there exist cocycles θ that lead to nontrivial algebra structure (that is, the form involves a skew field). One may check that all occurring θ are inner; so some of them cannot be liftable, and one finds this is indeed so. In a way non-liftability is to be expected, since N has an element s of order 4; c_s is only of order two.

One needs to make things more precise, and it is convenient to split our group rings, and their forms, into an abelian and a non-abelian part. Here $L[N] = L^4 \times A$, with $A = \mathrm{Mat}_2(L)$; this is the non-abelian part, and $L^4 \cong L[N^{ab}]$ is the abelian part. All data, including θ, restrict naturally to the non-abelian part. There is a short exact sequence

$$1 \to L^\times \to A^\times \to \mathrm{Aut}_{L-Alg}(A) \to 1.$$

Since $\mathrm{H}^1(G, A^\times)$ is trivial, this provides an injective map ∂:

$$\mathrm{H}^1(G, \mathrm{Aut}(A)) \to \mathrm{H}^2(G, L^\times).$$

The latter H^2 is a part of the Brauer group of K, and we recover the results of [TT19] by expressing $\partial[\theta]$ as the class of a quaternion algebra $[-1, a]_K$. The element a is obtained as "the" element such that a certain (here we don't explain which) quadratic subfield of L is $K(\sqrt{a})$.

We also consider outer cocycles for $N = D_4$, now forgetting about the Hopf Galois context; we simply take G of order 2 or 4. Then it is again possible to find Hopf forms of $K[N]$ that are nontrivial as algebras, with a similar technique.

Finally, we discuss the case N non-abelian of exponent p and order p^3, where p is an odd prime. Initially we ignore the question whether our setting comes from a Hopf Galois context and take L/K $\bar{G}$-Galois with $\bar{G}$ of order p. The group N has the presentation

$$N = \langle u, v, t \mid uv = vu, u^t = uv, v^t = v, u^p = v^p = t^p = 1\rangle.$$

Both the center and the commutator subgroup of N are of order p, generated by v. All inner cocycles $\theta : \bar{G} \to \mathrm{Inn}(N)$ are liftable since N has exponent p, so it is natural to wonder about outer cocycles. For technical reasons, let us assume that the degree of $\zeta := \zeta_p$ over K is $p-1$ (that is, maximal possible). The group ring $K[N]$ splits in an abelian part of dimension p^2, and a nonabelian part B, which is a central simple algebra of dimension p over $K' := K(\zeta)$, see below.

Theorem 4.1. *If $p \geq 5$ and $\bar{G} = \mathrm{Gal}(L/K)$ is cyclic of order p, then every cocycle $\theta : \bar{G} \to \mathrm{Aut}(N)$ defines a Hopf form H_θ which is trivial as an algebra in the non-abelian part. For $p = 3$, some forms have a trivial non-abelian algebra part, and some others do not.*

Sketch proof: Let σ be a generator of $\bar{G}$, and $\theta : \bar{G} \to \mathrm{Aut}(N)$ be any cocycle. Let $\psi = \theta(\sigma)$. Of course, the case of interest is that ψ is outer. We only discuss a prototypical example. Let ψ be defined (!) as identity on u and v and by sending t to ut. (One can show that ψ generates a p-Sylow subgroup of $\mathrm{Out}(N)$, so in a vague sense, ψ is already pretty general.)

We need to describe B explicitly; it is isomorphic to $\mathrm{Mat}_p(K(\zeta))$, with the following identifications:

$$v \mapsto \zeta; \quad u \mapsto \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & \zeta & 0 & \dots & 0 \\ 0 & 0 & \zeta^2 & \dots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \dots & \zeta^{p-1} \end{pmatrix}; \quad t \mapsto \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Then ψ induces automorphisms of B, and of ${}_LB$. The cocycle θ sends the generator σ of $\bar{G}$ to ψ. We know, by the theorem of Skolem-Noether, that there must exist a nonsingular matrix $X \in \mathrm{Mat}_p(K(\zeta))$ such that ψ is conjugation by X. In order to find $\partial[\theta]$ we have to find X. One can show that this can be done as follows: since $\psi^p = id$, we know that X^p is ξ times the identity matrix, for a scalar $\xi \in K(\zeta)$, and then the obstruction we want to calculate is

$$\partial[\theta] = \Big(\frac{\xi}{L(\zeta)/K(\zeta)}\Big).$$

By some tricks one can identify $X = diag(1, 1, \zeta, \zeta^3, \zeta^6, \ldots)$, and one obtains $\xi = 1$! This shows that the corresponding form is trivial as an algebra, for this particular ψ. For general ψ the argument becomes more involved, and the distinction $p = 3$, $p > 3$ becomes relevant.

Remarks: (1) Nejabati Zenouz has classified all Hopf Galois contexts involving N (and the other nonabelian group of order p^3 as well). We found such a context leading to the above cocycle by hand. There is a Hopf Galois context (G, N) with G of order p^3 (and actually $G \cong N$ for $p > 3$) such that the resulting action of G on N factors through a quotient $\bar{G}$ of order p, and a generator σ of $\bar{G}$ acts exactly via the outer automorphism ψ from above.

(2) We can also treat the other nonabelian group of order p^3. The methods are very similar, but the results are not so clean-cut: all combinations "cocycle inner non-liftable/outer" versus "form trivial/nontrivial as an algebra" can occur.