NON-ABELIAN HOPF COHOMOLOGY

PHILIPPE NUSS, MARC WAMBST
Institut de Recherche Mathématique Avancée, Université Louis-Pasteur et CNRS, 7, rue René-Descartes, 67084 Strasbourg Cedex, France. e-mail: nuss@math.u-strasbg.fr and wambst@math.u-strasbg.fr

Abstract. We introduce non-abelian cohomology sets of Hopf algebras with coefficients in Hopf modules. We prove that these sets generalize Serre’s non-abelian group cohomology theory. Using descent techniques, we establish that our construction enables to classify as well twisted forms for modules over Hopf-Galois extensions as torsors over Hopf-modules.

MSC 2000 Subject Classifications. Primary: 18G50, 16W30, 16W22, 14A22; Secondary: 16S38, 20J06.

Key-words: non-abelian cohomology, noncommutative descent theory, Hopf-Galois extension, Hopf-module, twisted form, torsor, Hilbert’s Theorem 90

INTRODUCTION. The aim of this article is to extend to Hopf algebras the concept of non-abelian cohomology of groups. Introduced in 1958 by Lang and Tate ([8]) for Galois groups with coefficients in an algebraic group, the non-abelian cohomology theory in degree 0 and 1 was formalized by Serre ([12], [13]). For an arbitrary group \( G \) acting on a group \( A \) which is not necessarily abelian, Serre constructs a 0-cohomology group \( H^0(G, A) \) and a 1-cohomology pointed set \( H^1(G, A) \). These objects generalize the two first groups of the classical Eilenberg-MacLane cohomology sequence \( H^*(G, A) = \text{Ext}^*_G(Z, A) \), defined only when \( A \) is abelian. It is well-known that the non-abelian cohomology set \( H^1(G, A) \) classifies the torsors on \( A \) (see [13]).

The non-abelian cohomology theory of groups comes naturally into play in the particular case where \( S/R \) is a \( G \)-Galois extension of rings in the sense of [9]. The situation is the following: a finite group \( G \) acts on a ring extension \( S/R \) and, in a compatible way, on an \( S \)-module \( M \). The coefficient group is then the group of \( S \)-automorphisms \( A = \text{Aut}_S(M) \) of \( M \). In [10], one of the authors showed that the set \( H^1(G, \text{Aut}_S(M)) \) classifies as well descent cocycles on \( M \) as twisted forms of \( M \).

Galois extensions of rings may be viewed as particular cases of Hopf-Galois extensions defined by Kreimer-Takeuchi ([7]), where a Hopf algebra \( H \) (non necessarily commutative nor cocommutative) plays the rôle of the Galois group. Indeed, given a group \( G \), a \( G \)-Galois extension of rings is nothing but a \( Z^G \)-Hopf-Galois extension of rings, where \( Z^G \) stands for the dual Hopf algebra of the group ring \( Z[G] \).

Suppose now fixed a ground ring \( k \), a Hopf algebra \( H \) over \( k \), and an \( H \)-comodule algebra \( S \) (for instance, any \( H \)-Hopf-Galois extension \( S/R \) is based on such a datum). For any \((H, S)\)-Hopf module \( M \), that is an abelian group \( M \) endowed with an \( S \)-action and a compatible \( H \)-coaction, we define in the cosimplicial spirit a 0-cohomology group \( H^0(H, M) \) and a 1-cohomology pointed set \( H^1(H, M) \).

The philosophy behind the construction is the following (precise definitions will be given in the core of the paper). Start with a \( G \)-Galois extension \( S/R \), where \( G \) is a finite group, and with \( M \) a \((G, S)\)-Galois module, i.e. an abelian group \( M \) endowed with two compatible \( S \)- and \( G \)-actions. The group \( \text{Aut}_S(M) \) inherits a \( G \)-action by conjugation. Let \( k^G \) be the dual Hopf algebra of the group ring \( k[G] \). A 1-cocycle in the sense of Serre is represented by a certain map \( \alpha : G \to \text{Aut}_S(M) \). By duality, \( \alpha \) formally defines an element in \( M \otimes_k M^* \otimes_k k^G \), which can also be seen as a map \( \Phi_\alpha : M \to M \otimes_k k^G \) satisfying some conditions. Assume now given, instead of \( G \), a Hopf-algebra \( H \) coacting on a ring \( S \). Let \( M \) be an \((H, S)\)-Hopf module, that is a module on which both \( H \) and \( S \) act in a compatible
way. We replace the former map $\Phi_\alpha : M \to M \otimes_k k^G$ by a map $\Phi : M \to M \otimes_k H$ and state
general requirements – the cocycle conditions –, which reflect the group-cocycle condition on $\alpha$. This
construction gives rise to a 1-cohomology pointed set $H^1(H,M)$.

We establish two mains results. The first Theorem shows that the 1-cohomology set $H^1(H,M)$
generalizes the non-abelian group 1-cohomology set of Serre. The second one relates $H^1(H,M)$ to
Twist$(S/R, N_0)$, the isomorphy class of the twisted forms of an extended module $M = N_0 \otimes_R S$. More
precisely, we prove the two following statements:

**Theorem A.** For a group $G$ and a $(k^G, S)$-Hopf module $M$, there is an isomorphism of pointed sets

$$H^1(k^G, M) \cong H^1(G, \text{Aut}_S(M)).$$

**Theorem B.** For a Hopf-algebra $H$ and an $(H, S)$-Hopf module $M$ of the form $M = N_0 \otimes_R S$, there
is an isomorphism of pointed sets

$$H^1(H, M) \cong \text{Twist}(S/R, N_0).$$

The precise wording of Theorem A will be found in Theorem 3.2, and that of Theorem B in Theorem 1.2. As a consequence of Theorem B, we deduce (Corollary 1.3) a Hopf version of the celebrated
Theorem 90 stated in 1897 by Hilbert in his *Zahlbericht*.

In order to prove these two results, we bring in an auxiliary cohomology theory $D^i(H, M)$
($i = 0, 1$) related to Descent Theory. The pointed set $D^1(H, M)$ classifies the $(H, S)$-Hopf module
structures on $M$ and, in the case of a Hopf-Galois extension, the descent data on $M$. Moreover, it
may be viewed as torsors on $M$ (Proposition 2.8).

We mention here that A. Blanco Ferro ([1]), generalizing a construction due to M. Sweedler
([14]), defined a 1-cohomology set $H^1(H, A)$, where $H$ is a Hopf-algebra and $A$ is an $H$-module
algebra. He applied his theory, which is in some sense dual to ours, to a commutative particular case:
not only does $H$ have to be a commutative finitely generated $k$-projective Hopf algebra, but $S/k$ is a
commutative Hopf-Galois extension. For any $k$-module $N$, setting $A = \text{End}_S(N \otimes_k S)$, Blanco Ferro
showed in this particular case that his set $H^1(H^*, A)$ classifies the twisted forms of $N \otimes_k S$ where $H^*$
stands for the dual Hopf algebra of $H$.

0. Conventions.
Let $k$ be a fixed commutative and unital ring. The unadorned symbol $\otimes$ between a right $k$-module
and a left $k$-module stands for $\otimes_k$. By algebra we mean a unital associative $k$-algebra. A division
algebra is either a commutative field or a skew-field. By module over a ring $R$, we always understand
a right $R$-module unless otherwise stated. Denote by $\mathcal{M}_R$ the category of $R$-modules and by $\mathcal{S}$
the category of sets.

Let $H$ be a finite-dimensional Hopf-algebra over $k$ with multiplication $\mu_H$, unity map $\eta_H$, comultiplication $\Delta_H$, counity map $\varepsilon_H$, and antipode $\sigma_H$. Let $S$ be an algebra, $\mu_S$ its multiplication, $\eta_S$ its
unity map. We assume that $S$ is a right $H$-comodule algebra, in other words that $S$ is equipped with
an $H$-coaction map $\Delta_S : S \to S \otimes H$ which is a morphism of algebras. Let $M$ be both an $S$-module
and an $H$-comodule with the $H$-coaction map $\Delta_M : M \to M \otimes H$. If $\Delta_M$ verifies the equality

$$\Delta_M(ms) = \Delta_M(m)\Delta_S(s),$$

for any $m \in M$ and $s \in S$, we say that $M$ is an $(H, S)$-Hopf module (also called a relative Hopf module
in the literature) and that $\Delta_M : M \to M \otimes H$ is $(H, S)$-linear. A morphism $f : M \to M'$ of
(H, S)-Hopf modules is an S-linear map f such that \((f \otimes \text{id}_M) \circ \Delta_M = \Delta_M \circ f\). To denote the coactions on elements, we use the Sweedler-Heyneman convention, that is, for \(m \in M\), we write \(\Delta_M(m) = m_0 \otimes m_1\), with summation implicitly understood. More generally, when we write down a tensor we usually omit the summation sign \(\sum\).

Denote by \(R\) the algebra of \(H\)-coinvariants of \(S\), that is \(R = \{s \in S \mid \Delta_S(s) = s \otimes 1\}\). An \(S\)-module \(M\) is said to be extended if there exists an \(R\)-module \(N_0\) such that \(M\) is equal to \(N_0 \otimes_R S\). The inclusion map \(\psi : R \hookrightarrow S\) is a (right) \(H\)-Hopf-Galois extension if \(\psi\) is faithfully flat and the map \(\Gamma_\psi : S \otimes_R S \hookrightarrow S \otimes H\), called Galois map, given on an indecomposable tensor \(s \otimes t \in S \otimes_R S\) by

\[
\Gamma_\psi(s \otimes t) = s\Delta(t),
\]

is a \(k\)-linear isomorphism. By Hopf-Galois descent theory ([5], [11]), every \((H, S)\)-Hopf module is isomorphic to an extended \(S\)-module. Conversely, an extended \(S\)-module \(M = N_0 \otimes_R S\) owns an \((H, S)\)-Hopf module structure with the canonical coaction \(\Delta_M = \text{id}_{N_0} \otimes \Delta_S : N_0 \otimes_R S \to N_0 \otimes_R S \otimes H\).

Let \(G\) be a finite group. Denote by \(k^G\) the \(k\)-free Hopf algebra over the \(k\)-basis \(\{\delta_g\}_{g \in G}\), with the following structure maps: the multiplication is given by \(\delta_g \cdot \delta_g' = \delta_{gg'}\), where \(\delta_{gg'}\) stands for the Kronecker symbol of \(g\) and \(g'\); the comultiplication \(\Delta_{k^G}\) is defined by \(\Delta_{k^G}(\delta_g) = \sum \delta_{ag} \otimes \delta_{bg}\); the unit in \(k^G\) is the element \(1 = \sum \delta_g\); the counit \(\varepsilon_{k^G}\) is defined by \(\varepsilon_{k^G}(\delta_g) = \delta_{g,1}\); the antipode \(\sigma_{k^G}\) sends \(\delta_g\) on \(\delta_{g^{-1}}\). When \(k\) is a field, then \(k^G\) is the dual of the usual group Hopf-algebra \(k[G]\). It is easy to see that a \(k^G\)-Hopf-Galois extension is the same as a \(G\)-Galois extension of \(k\)-algebras in the sense of [9]. To give an action of \(G\) on \(S\) is equivalent to give a coaction map of \(k^G\) on \(S\), the two structures being related by the equality

\[
\Delta_S(s) = \sum_{g \in G} g(s) \otimes \delta_g.
\]

An \(S\)-module \(M\) will be called a \((G, S)\)-Galois module if it is endowed with a \((G, S)\)-action, that is a \(G\)-action \(\gamma : G \to \text{Aut}_k(M)\) such that following twisted \(S\)-linearity condition:

\[
g(ms) = g(m)g(s)
\]

holds for any \(g \in G, m \in M\), and \(s \in S\) (when no confusion about \(\gamma\) is possible, we denote for simplicity \(g(m)\) instead of \(\gamma(g)(m)\)). When \(\gamma\) verifies (2), we say that the morphism \(\gamma\) is \((G, S)\)-linear. Denote by \(\text{Aut}^G_k(M)\) the subgroup of \(\text{Aut}_k(M)\) which is the image of \(\gamma\).

To give a \((G, S)\)-Galois module structure on \(M\) is equivalent to give a \((k^G, S)\)-Hopf module structure on \(S\). By Galois descent theory, a \((G, S)\)-Galois module is isomorphic to an extended module \(N \otimes_R S\).

1. Non-abelian Hopf cohomology theory.

In this section we define a non-abelian Hopf cohomology theory, and state our main result, Theorem 1.2, which compares in the Hopf-Galois context the 1-Hopf cohomology set with twisted forms. We deduce a Hopf-Galois version of Hilbert’s Theorem 90.

1.1. Definition of the non-abelian Hopf cohomology sets.

Let \(H\) be a Hopf-algebra and \(S\) be an \(H\)-comodule algebra. For any \(S\)-module \(M\), we endow \(M \otimes H^\otimes n\) with an \(S\)-module structure given by

\[
(m \otimes h)s = ms \otimes h,
\]

for \(m \in M, h \in H^\otimes n\), and \(s \in S\).
Set $W^n_k(M) = \text{Hom}_k(M, M \otimes H^{\otimes n})$ and $W^n_S(M) = \text{Hom}_S(M, M \otimes H^{\otimes n})$. We equip the $k$-module $W^n_k(M)$ with a composition-type product $\circ : W^n_k(M) \otimes W^n_k(M) \rightarrow W^n_k(M)$, defined by

$$
\begin{cases}
  \varphi \circ \varphi' = \varphi \circ \varphi' & \text{if } n = 0 \\
  \varphi \circ \varphi' = (\text{id}_M \otimes \mu_H) \circ (\varphi \otimes \varphi) \circ \Delta_M & \text{if } n > 0
\end{cases}
$$

for $\varphi, \varphi' \in W^n_k(M)$; here $\chi_n : H^{\otimes n} \otimes H^{\otimes n} \rightarrow (H \otimes H)^{\otimes n}$ denotes the intertwining operator given by

$$
\chi_n((a_1 \otimes \ldots \otimes a_n)(b_1 \otimes \ldots \otimes b_n)) = (a_1 \otimes b_1) \otimes \ldots \otimes (a_n \otimes b_n).
$$

It restricts to a product still denoted $\circ$ on $W^n_S(M)$. Thanks to the product $\circ$, the modules $W^n_k(M)$ and $W^n_S(M)$ become a monoid: the associativity of $\circ$ is a direct consequence of the coassociativity of $\Delta_H$ and the neutral element is $v_n = \text{id}_M \otimes \eta_H^{\otimes n}$. Further we shall use that the group of invertible elements of the monoid $W^n_S(M)$ is $\text{Aut}_S(M)$.

Suppose that $M$ is an $H$-comodule. Denote by $T$ the flip of $H \otimes H$, the automorphism of $H \otimes H$ which sends an indecomposable tensor $h \otimes h'$ to $h' \otimes h$. We define two maps $d^i : W^n_k(M) \rightarrow W^1_k(M)$ $(i = 0, 1)$ and three maps $d^i : W^1_S(M) \rightarrow W^2_S(M)$ $(i = 0, 1, 2)$ by the formulae

$$
d^0\varphi = (\text{id}_M \otimes \mu_H) \circ (\Delta_M \otimes \text{id}_H) \circ (\varphi \otimes \sigma_H) \circ \Delta_M
$$

$$
d^1\varphi = (\text{id}_M \otimes \eta_H) \circ \varphi
$$

$$
d^0\Phi = (\text{id}_M \otimes \mu_H \otimes \text{id}_H) \circ (\Delta_M \otimes T) \circ (\Phi \otimes \sigma_H) \circ \Delta_M
$$

$$
d^1\Phi = (\text{id}_M \otimes \Delta_H) \circ \Phi
$$

$$
d^2\Phi = (\text{id}_M \otimes \text{id}_H \otimes \eta_H) \circ \Phi = \Phi \otimes \eta_H,
$$

where $\varphi : M \rightarrow M$ and $\Phi : M \rightarrow M \otimes H$ are $k$-linear morphisms.

**Lemma 1.1.** Let $M$ be an $(H, S)$-Hopf-module. The restriction of the above defined maps to the corresponding monoids $W^n_S(M)$ and $W^1_S(M)$ are morphisms of monoids which may be organized in the following cosimplicial diagram:

$$
\begin{array}{ccc}
  W^0_S(M) & \xrightarrow{d^0} & W^1_S(M) \\
  \vphantom{d^0} & \xrightarrow{d^1} & \vphantom{d^0} \\
  W^1_S(M) & \xrightarrow{d^2} & W^2_S(M)
\end{array}
$$

(3)

**Proof.** We adopt the Sweedler-Heyneman convention and use the Hopf yoga, for instance, the fact that for any $x, y \in H$, one has $x_0 \otimes \varepsilon_H(x_1)\cdot x_2 y = x_0 \otimes \varepsilon_H(x_1) y = x_0 y$. First one has to show that $d^0\varphi$ and $d^0\Phi$ are $S$-linear. This assertion is obvious for $d^1\varphi$. Let us prove it for $d^0\varphi$. We get, for any $m \in M$ and $s \in S$, the equalities

$$
\begin{align*}
  d^0\varphi(ms) &= [(\text{id}_M \otimes \mu_H) \circ (\Delta_M \otimes \text{id}_H) \circ (\varphi \otimes \sigma_H) \circ \Delta_M](ms) \\
  &= [(\text{id}_M \otimes \mu_H) \circ (\Delta_M \otimes \text{id}_H)]((\varphi(m_0)s_0 \otimes \sigma_H(m_1s_1)) \\
  &= (\text{id}_M \otimes \mu_H)((\varphi(m_0)s_0 \otimes \varphi(m_0)_1s_1 \otimes \sigma_H(s_2))\sigma_H(m_1)) \\
  &= \varphi(m_0)s_0 \otimes \varphi(m_0)_1s_1 \otimes \sigma_H(s_2)\sigma_H(m_1) \\
  &= \varphi(m_0)s \otimes \varphi(m_0)_1s_1 \otimes \sigma_H(m_1) \\
  &= d^0\varphi(m)s.
\end{align*}
$$
The \( S \)-linearity of \( d^1 \Phi \) and \( d^2 \Phi \) is obvious. We prove it for \( d^0 \Phi \). For any \( m \in M \) and \( s \in S \), set \( \Phi(m) = m' \circ m'' \). We have \( d^0 \Phi(m) = ((m_0)'_0 \circ (m_0)'_1 \sigma_H(m_1) \circ (m_0)'' \), hence

\[
d^0 \Phi(ms) = [\langle id_M \otimes \mu_H \otimes id_H \rangle \circ (\Delta_M \otimes T) \circ (\Phi \otimes \sigma_H) \circ \Delta_M](ms)
\]

\[
= [\langle id_M \otimes \mu_H \otimes id_H \rangle \circ (\Delta_M \otimes T)]((m_0)'_0 \circ (m_0)'_1 s_0 \circ (m_0)'' \circ \sigma_H(m_1 s_1))
\]

\[
= (id_M \otimes \mu_H \otimes id_H)[((m_0)'_0 s_0 \circ (m_0)''_1 s_1 \circ \sigma_H(s_2) \sigma_H(m_1) \circ (m_0)'_1)
\]

\[
= (id_M \otimes \mu_H \otimes id_H)((m_0)'_0 s_0 \circ (m_0)'_1 \sigma_H(m_1) \circ (m_0)''
\]

\[
= d^0 \Phi(m)s.
\]

We prove now that \( d^i \) respects the monoid structures on \( W^S_0(M) \), that is

\[
d^i \varphi \circ d^i \varphi' = d^i(\varphi \circ \varphi'), \quad d^i \Phi \circ d^i \Phi' = d^i(\Phi \circ \Phi'), \quad \text{and} \quad d^i(v_k) = v_{k+1}
\]

for any \( \varphi, \varphi' \in W^S_0(M) \), any \( \Phi, \Phi' \in W^1_0(M) \), \( k \in \{0, 1\} \), and any appropriate index \( i \). Let us prove this on the 0-level for \( \varphi \) and \( \varphi' \) in \( W^0(M) \). For any \( m \in M \), we have:

\[
(d^0 \varphi' \circ d^0 \varphi)(m) = (id_M \otimes \mu_H)(d^0 \varphi' \otimes id_H)(d^0 \varphi(m))
\]

\[
= (id_M \otimes \mu_H)(d^0 \varphi' \otimes id_H)(\varphi(m)_0 \otimes \varphi(m)_1 \sigma_H(m_1))
\]

\[
= \varphi'(\varphi(m)_0) \otimes \varphi'(\varphi(m)_1) \sigma_H(m_1) \varphi(m)_0 \sigma_H(m_1)
\]

\[
= (id_M \otimes id_H)((\Delta_M \circ \varphi') \otimes id_H)(\varphi(m)_0 \otimes \varphi(m)_1) \sigma_H(m_1)
\]

\[
= d^0(\varphi' \circ \varphi)(m)
\]

and

\[
d^1 \varphi \circ d^1 \varphi'(m) = (id_M \otimes \mu_H)(d^1 \varphi' \otimes id_H)(d^1 \varphi(m))
\]

\[
= (id_M \otimes \mu_H)(d^1 \varphi' \otimes id_H)(\varphi(m) \otimes 1)
\]

\[
= (id_M \otimes \mu_H)(\varphi'(\varphi(m)) \otimes 1 \otimes 1)
\]

\[
= \varphi'(\varphi(m)) \otimes 1
\]

\[
= d^1(\varphi' \circ \varphi)(m).
\]

We do not write down the computations on the 1-level, which are very similar to the previous ones. We leave to the reader the straightforward proof of \( d^i(v_k) = v_{k+1} \) and also the easy checking of the following three formulae

\[
d^2 d^0 = d^0 d^2, \quad d^1 d^0 = d^0 d^1, \quad d^2 d^1 = d^1 d^2,
\]

which mean that the diagram (3) is precosimplicial.

\[\square\]

We define the 0-cohomology group \( H^0(H, M) \) and the 1-cohomology set \( H^1(H, M) \) in the following way. Let

\[
H^0(H, M) = \{ \varphi \in \text{Aut}_S(M) \mid d^0 \varphi = d^0 \varphi \}
\]

be the equalizer of the pair \( (d^0, d^1) \). It is obviously a group since \( d^i \) is a morphism of monoids.
The set $Z^1(H, M)$ of 1-Hopf cocycles of $H$ with coefficients in $M$ is the subset of $W^1_H(M)$ defined by

$$Z^1(H, M) = \left\{ \Phi \in W^1_H(M) \right\}$$

where

$$\begin{align*}
\Phi(s) &= \Phi(m)s, \text{ for all } m \in M \text{ and } s \in S \\
\Phi(1) &= \Phi(m) = \Phi(s) = \Phi(m) = \Phi(s)
\end{align*}$$

The group $\text{Aut}_S(M)$ acts on the right on $Z^1(H, M)$ by

$$(\Phi \mapsto f) = d^1 f^{-1} \circ \Phi \circ d^0 f,$$

where $\Phi \in Z^1(H, M)$ and $f \in \text{Aut}_S(M)$. Two 1-Hopf cocycles $\Phi$ and $\Phi'$ are said to be cohomologous if they belong to the same orbit under the action of $\text{Aut}_S(M)$ on $Z^1(H, M)$. We denote by $H^1(H, M)$ the quotient set $\text{Aut}_S(M)\backslash Z^1(H, M)$; it is pointed with distinguished point the class of the map $v_1 = \text{id}_M \otimes \eta_H$.

For $i = 0, 1$, we call $H^i(H, M)$ the $i$th-Hopf cohomology set of $H$ with coefficients in the $(H, S)$-Hopf module $M$.

1.2. The main theorem: Comparison of the 1-Hopf cohomology set with twisted forms in the Hopf-Galois context.

Let $H$ be a Hopf-algebra, $\psi : R \to S$ be an $H$-Hopf-Galois extension, and $M = N_0 \otimes_R S$ be the extended $S$-module of an $R$-module $N_0$. We endow $M$ with the canonical $(H, S)$-Hopf module structure given by the coaction $\Delta_M = \text{id}_{N_0} \otimes \Delta_S$. The central result of this paper asserts that the Hopf 1-cohomology set $H^1(H, M)$ is isomorphic to the pointed set $\text{Twist}(S/R, N_0)$ of twisted forms of $N_0$ up to isomorphisms.

Let $\psi : R \to S$ be any extension of rings and $N_0$ be an $R$-module. Recall that a twisted form of $N_0$ (over $S/R$) is a pair $(N, \varphi)$, where $N$ is an $R$-module and $\varphi : N \otimes_R S \to N_0 \otimes_R S$ is an $S$-linear isomorphism. Let $\text{twist}(S/R, N_0)$ be the set of twisted forms of $N_0$. Two twisted forms $(N, \varphi)$ and $(N', \varphi')$ of $N_0$ are isomorphic if $N$ and $N'$ are isomorphic as $R$-modules. Following [6], we denote by $\text{Twist}(S/R, N_0)$ the pointed set of isomorphism classes of twisted forms of $N_0$, the distinguished point being the class of $(N_0, \text{id}_{N_0} \otimes \text{id}_S)$. We mention here that all the results of [10] involving equivalence classes of twisted forms are actually proven for this definition of $\text{Twist}(S/R, N_0)$ and not for the one given in [10, §6.3], where the equivalence relation is too restrictive.

**Theorem 1.2.** Let $H$ be a Hopf-algebra, $\psi : R \to S$ be an $H$-Hopf-Galois extension, and $M = N_0 \otimes_R S$ be the extended $S$-module of an $R$-module $N_0$. There is an isomorphism of pointed sets

$$H^1(H, M) \cong \text{Twist}(S/R, N_0).$$

Theorem 1.2 allows us to state the following noncommutative generalization of Noether’s cohomological form of Hilbert’s Theorem 90.

**Corollary 1.3.** Let $H$ be a Hopf-algebra and $\psi : K \to L$ be an $H$-Hopf-Galois extension of division algebras. Then, for any positive integer $n$, we have

$$H^1(H, L^n) = \{1\}.$$
Proof of Corollary 1.3. Observe that $L^n$ is isomorphic to the extended $L$-module $K^n \otimes_K L$. By Theorem 1.2, the pointed set $H^1(H, L^n)$ is isomorphic to $\text{Twist}(L/K, K^n)$, which is known to be trivial ([10, Corollary 6.21]).

The rest of the paper is mainly devoted to the proof of Theorem 1.2. This is done in two steps. At first we introduce a non-abelian cohomology theory $D^i(H, M)$, for $i = 0, 1$, which is related to noncommutative descent theory. In Theorem 2.6, we prove the isomorphism $D^1(H, M) \cong \text{Twist}(S/R, N_0)$. Subsequently we show that the Hopf cohomology sets $H^i(H, M)$ are isomorphic to the descent cohomology sets $D^i(H, M)$.

2. Descent cohomology sets.

In this section we introduce two descent cohomology sets. We compute them in the Galois case and relate them to the usual non-abelian group cohomology theory. In addition, in the Hopf-Galois context, we prove that the 1-descent cohomology set classifies twisted forms and interpret it in terms of torsors on the module of coefficients.

2.1. Definition of descent cohomology sets.

Let $H$ be a Hopf-algebra, $S$ be an $H$-comodule algebra, and $M$ be an $(H, S)$-Hopf module with coaction $\Delta_M : M \rightarrow M \otimes H$. We define the 0-cohomology group $D^0(H, M)$ by

$$D^0(H, M) = \{ \alpha \in \text{Aut}_S(M) \mid (\alpha \otimes \text{id}_H) \circ \Delta_M = \Delta_M \circ \alpha \}.$$ 

It is the set of the $S$-linear automorphisms of $M$ which are maps of $H$-comodules. This set obviously carries a group structure given by the composition of automorphisms.

**Lemma 2.1.** Let $H$ be a Hopf-algebra and $S$ be an $H$-comodule algebra. Any isomorphism $f : M \rightarrow M'$ of $(H, S)$-Hopf modules induces an isomorphism of groups $f^* : D^0(H, M') \rightarrow D^0(H, M)$ given on $\alpha' \in D^0(H, M')$ by:

$$f^* \alpha' = f^{-1} \circ \alpha' \circ f.$$ 

**Proof.** The $S$-linearity of $f^* \alpha'$ immediately follows from the $S$-linearity of $f$ and that of $\alpha'$. In order to prove that $f^* \alpha'$ belongs to $D^0(H, M)$, it is sufficient to observe that the following diagram is commutative.

![Diagram]
Lemma 2.2. Let $C^1(H, M)$ be a Hopf-algebra and $S$ be an $H$-comodule algebra. Any isomorphism $f : M \to M'$ of $S$-modules induces a bijection $f^* : C^1(H, M') \to C^1(H, M)$ given on $F' \in C^1(H, M')$ by

$$f^* F' = (f^{-1} \otimes id_H) \circ F \circ f.$$

For any $S$-module $M$, one has

$$(id_M)^* = id_{C^1(H, M)}.$$

For any composable isomorphisms of $S$-modules $f : M \to M'$ and $f' : M' \to M''$, the following equality holds

$$(f' \circ f)^* = f^* \circ f'^*.$$

If moreover $f : M \to M'$ is an isomorphism of $(H, S)$-Hopf modules, then $f^*$ realizes an isomorphism of pointed sets between $C^1(H, M')$ and $C^1(H, M)$.

Proof. Let $f : M \to M'$ be an isomorphism of $S$-modules. The $(H, S)$-linearity of $f^* F'$ immediately follows from the $S$-linearity of $f$ and from the $(H, S)$-linearity of $F'$. The coassociativity of $f^* F'$ comes from the commutativity of the diagram

While the compatibility of $f^* F'$ with the counity of $H$ is expressed by the commutativity of the diagram

We introduce now a 1-cohomology set $D^1(H, M)$ in the following way. The set $C^1(H, M)$ of 1-descent cocycles of $H$ with coefficients in $M$ is defined to be the set of all $k$-linear $H$-coactions $F : M \to M \otimes H$ on $M$ making $M$ an $(H, S)$-Hopf module. In other words, one has:

$$C^1(H, M) = \left\{ F : M \to M \otimes H \mid \begin{array}{l} (CC_1) \quad F(ms) = F(m)\Delta_S(s), \text{ for all } m \in M \text{ and } s \in S \\ (CC_2) \quad (id_M \otimes \varepsilon_H) \circ F = id_M \\ (CC_3) \quad (F \otimes id_H) \circ F = (id_M \otimes \Delta_H) \circ F \end{array} \right\}.$$
Hence we have shown that $f^*F'$ belongs to $C^1(H, M)$. By the very definition, $f^*F'$ is bijective and $(\text{id}_M)^* = \text{id}_{C^1(H, M)}$.

Let $f : M \rightarrow M'$ and $f' : M' \rightarrow M''$ be two isomorphisms of $S$-modules. One has, for any $F' \in C^1(H, M')$, the following equalities

$$(f' \circ f)^*(F') = ((f' \circ f)^{-1} \circ \text{id}_H) \circ F' \circ (f' \circ f) = ((f^{-1} \circ f^{-1}) \circ \text{id}_H) \circ F' \circ (f' \circ f) = f^*(f^*F').$$

Moreover, if $f$ is an isomorphism of $(H, S)$-Hopf modules, the map $f^*$ preserves the distinguished points: indeed, the equality $f^*\Delta_{M'} = \Delta_M$ is equivalent to the fact that $f$ is a morphism of $(H, S)$-Hopf modules.

From Lemma 2.2, one readily obtains the following result:

**Corollary 2.3.** Let $H$ be a Hopf-algebra, $S$ be an $H$-comodule algebra, and $M$ be an $(H, S)$-Hopf module. The group $\text{Aut}_S(M)$ acts on the right on $C^1(H, M)$ by

$$(F \leftarrow f) = f^*F = (f^{-1} \circ \text{id}_H) \circ F \circ f,$$

where $F \in C^1(H, M)$ and $f \in \text{Aut}_S(M)$.

Two 1-descent cocycles $F$ and $F'$ are said to be cohomologous if they belong to the same orbit under the action of $\text{Aut}_S(M)$ on $C^1(H, M)$. We denote by $D^1(H, M)$ the quotient set $\text{Aut}_S(M)/C^1(H, M)$; it is pointed with distinguished point the class of the coaction $\Delta_M$.

For $i = 0, 1$, we call $D^i(H, M)$ the $i$-th descent cohomology set of $H$ with coefficients in $M$. The choice of this name finds its motivation in the following observation. Suppose that $\psi : R \rightarrow S$ is an $H$-Hopf-Galois extension. As shown in [11], an $(H, S)$-Hopf module may always be descended to an $R$-module $N_0$, that is $M$ is isomorphic to an extended $S$-module $N_0 \otimes_R S$. The set $C^1(H, M)$ is exactly those of all descent data on $M$ described in [10].

**Corollary 2.4.** Let $H$ be a Hopf-algebra and $S$ be an $H$-comodule algebra.

- Any isomorphism $f : M \rightarrow M'$ of $S$-modules induces a bijection $f^* : D^1(H, M') \rightarrow D^1(H, M)$.
- Any isomorphism $f : M \rightarrow M'$ of $(H, S)$-Hopf modules induces an isomorphism of pointed sets $f^* : D^1(H, M') \rightarrow D^1(H, M)$.

**Proof.** Suppose that $F_1$ and $F_2$ are two cohomologous 1-cocycles of $C^1(H, M')$, with $g \in \text{Aut}_S(M')$ such that $F_1 = g^*F_2$. Then $f^*F_2 = f^*g^*F_1 = f^*g^*(f^{-1})^*f^*F_1 = (f^{-1}gf)^*(f^*F_1)$, so $f^*F_1$ and $f^*F_2$ are cohomologous in $C^1(H, M)$. 

2.2. Application to the Galois case.

We work now with the Hopf algebra $k^G$ dual to the group algebra $k[G]$ for $G$ a finite group. Let $\psi : R \rightarrow S$ be a $k^G$-Galois extension and $M$ a $(G, S)$-Galois module. We may assume that $M$ is already extended, so that $M$ is equal to $N_0 \otimes_R S$ for an $R$-module $N_0$. Endow $M$ with the canonical $(H, S)$-Hopf module structure given by the coaction $\Delta_M = \text{id}_M \otimes \Delta_S$. In this paragraph, we compute the descent cohomology set of $k^G$ with coefficients in $M = N_0 \otimes_R S$ in terms of the Galois 1-cohomology set of $G$ with coefficients in $\text{Aut}_S(M)$.

Recall that for any group $G$ and any (left) $G$-group $A$, one classically defines two non-abelian cohomology sets of $G$ with coefficients in $A$ (see [12] and [13]). This is done in the following way. The 0-cohomology group $H^0(G, A)$ is the group $A^G$ of invariant elements of $A$ under the action of $G$. The set $Z^1(G, A)$ of 1-cocycles is given by

$$Z^1(G, A) = \{ \alpha \in \text{Ext}(G, A) \mid \alpha(gg') = \alpha(g)\alpha(g'), \ \forall \ g, g' \in G \}.$$  

It is pointed with distinguished point the constant map $1 : G \rightarrow A$. 

The group $A$ acts on the right on $\mathbb{Z}^1(G, A)$ by

$$(\alpha \leftarrow a)(g) = a^{-1}\alpha(g) \cdot a,$$

where $a \in A$, $\alpha \in \mathbb{Z}^1(G, A)$, and $g \in G$. Two 1-cocycles $\alpha$ and $\alpha'$ are cohomologous if they belong to the same orbit under this action. The non-abelian 1-cohomology set $H^1(G, A)$ is the left quotient $A/\mathbb{Z}^1(G, A)$. Then $H^1(G, A)$ is pointed with distinguished point the class of the constant map $1 : G \to A$.

Let $G$ be a finite group, $\psi : R \to S$ be a $G$-Galois extension, and $M = N_0 \otimes_R S$ be the extended $S$-module of an $R$-module $N_0$. The $S$-module $M$ is a $(G, S)$-Galois module by the canonical action given on an indecomposable tensor $n \otimes s \in N_0 \otimes_R S$ by

$$g(n \otimes s) = n \otimes g(s),$$

where $g \in G$, $n \in N_0$, and $s \in S$. The group $G$ acts by automorphisms on $\text{Aut}_S(M)$ by

$$gf = (\text{id}_{N_0} \otimes g) \circ f \circ (\text{id}_{N_0} \otimes g^{-1}),$$

where $g \in G$ and $f \in \text{Aut}_S(M)$. Hence $\text{Aut}_S(M)$ becomes a $G$-group and we get at our disposal the two non-abelian cohomology sets $H^0(G, \text{Aut}_S(M))$ and $H^1(G, \text{Aut}_S(M))$.

**Proposition 2.5.** Let $G$ be a finite group, $\psi : R \to S$ be a $G$-Galois extension, and $M = N_0 \otimes_R S$ be the extended $S$-module of an $R$-module $N_0$. There is the equality of groups

$$D^0(k^G, M) = H^0(G, \text{Aut}_S(M))$$

and an isomorphism of pointed sets

$$D^1(k^G, M) \cong H^1(G, \text{Aut}_S(M)).$$

**Proof.** Let us prove the equality between the groups. It is sufficient to show that for any $f \in \text{Aut}_S(M)$, the condition $(f \otimes \text{id}_M) \circ \Delta_M = \Delta_M \circ f$ is equivalent to the fact that $f$ is $G$-invariant. Indeed, the first condition reflects that $f$ belongs to $D^0(k^G, M)$, whereas $H^0(G, \text{Aut}_S(M))$ is precisely the group $\text{Aut}_S(M)^G$ of $G$-invariant automorphisms in $\text{Aut}_S(M)$. Pick $f \in \text{Aut}_S(M)$, $n \in N_0$, and $s \in S$. One has

$$((f \otimes \text{id}_M) \circ \Delta_M)(n \otimes s) = \sum_{g \in G} (f \otimes \text{id}_M)(n \otimes g(s) \otimes g) = \sum_{g \in G} (f \circ (\text{id}_{N_0} \otimes g))(n \otimes s) \otimes g.$$

On the other hand, setting $f(n \otimes s) = n' \otimes s'$, one gets

$$(\Delta_M \circ f)(n \otimes s) = \Delta_M(n' \otimes s') = \sum_{g \in G} (n' \otimes g(s')) \otimes g = \sum_{g \in G} ((\text{id}_{N_0} \otimes g) \circ f)(n \otimes s) \otimes g.$$

Since $\{g\}_{g \in G}$ is a basis of $k^G$, the relation $(f \otimes \text{id}_M) \circ \Delta_M = \Delta_M \circ f$ is equivalent to the set of equalities $f \circ (\text{id}_{N_0} \otimes g) = (\text{id}_{N_0} \otimes g) \circ f$, with $g$ running through $G$. This exactly means that $f$ is $G$-invariant in $\text{Aut}_S(M)$. 
We prove now the isomorphism on the 1-cohomology level. Let us show that any \( F \in C^1(k^G, M) \) induces a \((G, S)\)-Galois module action \( \gamma \in \text{Aut}_S^1(M) \) defined by

\[
F(m) = \sum_{g \in G} (\gamma(g))(m) \otimes \delta_g.
\]

For simplicity denote \( \gamma(g)(m) \) by \( g(m) \). The \( k \)-linearity of \( F \) tells us that \( g(m + m') = g(m) + g(m') \), for any \( g \in G \) and \( m, m' \in M \); the equality \((\text{id}_M \otimes \varepsilon_{k^G}) \circ F = \text{id}_M\) implies that \( 1(m) = m \); the coassociativity condition of \( F \) says that \( (g g')(m) = g(g'(m)) \), for any \( g, g' \in G \) and \( m \in M \); finally the \((k^G, S)\)-linearity of \( F \) is equivalent to the \((G, S)\)-linearity of \( \gamma \). As shown in [10], the action map \( \gamma \) gives rise to the 1-Galois cocycle \( \alpha : G \rightarrow \text{Aut}_S(M) \) defined by

\[
\alpha(g) = \gamma(g) \circ (\text{id}_{N_0} \otimes g^{-1}).
\]

It is easy to check that the correspondence between \( F \) and \( \alpha \) is bijective. Thus already at the 1-cocycle level there exists a bijection between \( Z^1(G, \text{Aut}_S(M)) \) and \( C^1(k^G, M) \).

Take two cocycles \( F \) and \( F' \) in \( C^1(k^G, M) \). Denote by \( \gamma \) (respectively \( \gamma' \)) the corresponding Galois actions and by \( \alpha \) (respectively \( \alpha' \)) the Galois cocycles associated with \( \gamma \) (respectively \( \gamma' \)). Suppose that the cocycles \( F \) and \( F' \) are cohomologous, with \( f \in \text{Aut}_S(M) \) such that \((f \otimes \text{id}_{k^G}) \circ F = F' \circ f\). Then \( f \circ \gamma(g) = \gamma'(g) \circ f \), for all \( g \in G \), or equivalently \( \gamma(g) = f^{-1} \circ \gamma'(g) \circ f \). Therefore

\[
\alpha(g) = f^{-1} \circ \alpha'(g) \circ f \circ (\text{id}_{N_0} \otimes g^{-1})
\]

which means that \( \alpha \) and \( \alpha' \) are Galois-cohomologous. Conversely, the previous equalities show that two cohomologous Galois cocycles \( \alpha \) and \( \alpha' \) give rise to two cohomologous cocycles \( F \) and \( F' \) in \( C^1(k^G, M) \).

2.3. Comparison between the 1-descent cohomology set and the set of twisted forms in the Hopf-Galois context.

Let \( H \) be a Hopf-algebra, \( \psi : R \rightarrow S \) be an \( H \)-Hopf-Galois extension, and \( M = N_0 \otimes_R S \) be the extended \( S \)-module of an \( R \)-module \( N_0 \). We endow \( M \) with the canonical \((H, S)\)-Hopf module structure given by the coaction \( \Delta_M = \text{id}_{N_0} \otimes \Delta_S \). The main result of this paragraph asserts that the descent 1-cohomology set \( D^1(H, M) \) is isomorphic to the pointed set \( \text{Twist}(S/R, N_0) \) of twisted forms of \( N_0 \) up to isomorphisms.

**Theorem 2.6.** Let \( H \) be a Hopf-algebra, \( \psi : R \rightarrow S \) be an \( H \)-Hopf-Galois extension, and \( M = N_0 \otimes_R S \) be the extended \( S \)-module of an \( R \)-module \( N_0 \). Then there is an isomorphism of pointed sets

\[
D^1(H, M) \cong \text{Twist}(S/R, N_0).
\]

In order to prove Theorem 2.6, we need an intermediate result. For any \( F \in C^1(H, M) \) denote by \( N_F \) the \( R \)-module of \( F \)-coinvariants, that is \( N_F = \{m \in M \mid F(m) = m \otimes 1\} \). We state the following lemma:
Lemma 2.7. Under the same hypotheses as in Theorem 2.6, for any \( F \in C^1(H, M) \), there exists an isomorphism
\[
\varphi_F : N_F \otimes_R S \xrightarrow{\sim} M
\]
given by \( \varphi_F(m \otimes s) = ms \), for any \( m \in N_F \) and \( s \in S \).

Proof. The existence of the isomorphism \( \varphi_F \) results from Hopf-Galois descent theory [11, Theorem 3.7] (see also [5]). Indeed, consider the functor “restriction of scalars” \( \psi^* : \mathcal{M}_{dS} \rightarrow \mathcal{M}_R \) and its left adjoint functor \( \psi_! : \mathcal{M}_R \rightarrow \mathcal{M}_{dS} \), the functor “extension of scalars”. Then \( \varphi_F \) is nothing but a counit for the comonad on \( \mathcal{M}_{dS} \) induced by the adjunction \( \psi_! \dashv \psi^* \) (see, e.g., [4]).

We explicit now the expression of \( \varphi_F \). By arguments stemming from descent theory ([3], [10]), the \( S \)-module \( M \) is isomorphic to \( N_d \otimes_R S \), where \( N_d \) is the \( R \)-module deduced from the Cipolla descent data \( d \) on \( M \) associated to the \((H, S)\)-Hopf module structure of \( M \). By [10, Prop. 4.10], \( d \) is the map given by the composition
\[
M \xrightarrow{F} M \otimes H \xrightarrow{\beta} M \otimes_S (S \otimes H) \xrightarrow{id_M \otimes \Gamma_{s}} M \otimes_S (S \otimes_R S) \xrightarrow{\beta'} M \otimes_R S,
\]
where \( \beta \) (respectively \( \beta' \)) is the obvious \( k \)-linear (respectively \( S \)-linear) isomorphism and \( \Gamma_s \) is the Galois isomorphism mentioned in the Conventions.

Let us now compute \( d \). For \( m \in M \), set \( F(m) = \sum_i m_i \otimes h_i \in M \otimes H \). For any fixed index \( i \), set \( \Gamma_{s}^{-1}(1 \otimes h_i) = \sum_j s_{ij} \otimes t_{ij} \), or equivalently \( \sum_j s_{ij} \Delta_{S}(t_{ij}) = 1 \otimes h_i \). So
\[
d(m) = \sum_i \sum_j m_i s_{ij} \otimes t_{ij}.
\]
According to [10, Cor. 4.11], we have \( N_d = \{ m \in M \mid \sum_i \sum_j m_i s_{ij} \Delta_{S}(t_{ij}) = m \otimes 1 \} \), therefore
\[
N_d = \{ m \in M \mid \sum_i m_i \otimes h_i = m \otimes 1 \} = \{ m \in M \mid F(m) = m \otimes 1 \} = N_F.
\]
It is proven in [3] that the descent isomorphism from \( N_d \otimes_R S \) to \( M \) is given by the correspondence \( m \otimes s \mapsto ms \) for \( m \in N_d \) and \( s \in S \).

Proof of Theorem 2.6. Let \( F \) be an element of \( \text{C}^1(H, M) \) and \( \varphi_F \) be the isomorphism from \( N_F \otimes_R S \) to \( M = N_0 \otimes_R S \) given by the previous lemma. The datum \((N_F, \varphi_F)\) is a twisted form of \( N_0 \). Denote by \( \tilde{T} \) the map from \( \text{C}^1(H, M) \) to the set \( \text{twist}(S/R, N_0) \) defined by
\[
\tilde{T}(F) = (N_F, \varphi_F).
\]
The map \( \tilde{T} \) obviously sends the distinguished point \( \Delta_M \) of \( \text{C}^1(H, M) \) to the distinguished point \((N_0, \text{id}_{N_0 \otimes_R S})\) of \( \text{twist}(S/R, N_0) \).

Suppose that \( F \) and \( F' \) are cohomologous in \( \text{C}^1(H, M) \). We claim that the corresponding descended modules \( N_F \) and \( N_{F'} \) are isomorphic in \( \mathcal{M}_R \). Indeed, let \( f \in \text{Aut}_S(M) \) such that \((f \otimes \text{id}_H) \circ F = F' \circ f \). For any \( n \in N_F \), the image \( f(n) \) belongs to \( N_{F'} \), since
\[
F'(f(n)) = (f \otimes \text{id}_H)(F(n)) = (f \otimes \text{id}_H)(n \otimes 1) = f(n) \otimes 1.
\]
So the automorphism \( f \) induces an isomorphism from \( N_F \) to \( N_{F'} \). From this fact we deduce a quotient map
\[
\mathcal{T} : \text{D}^1(H, M) \longrightarrow \text{Twist}(S/R, N_0).
\]
We now prove that $\mathcal{T}$ is an isomorphism of pointed sets. In order to do this, we introduce the map $\tilde{D} : \text{twist}(S/R, N_0) \to C^1(H, M)$ which associates to any twisted form $(N, \varphi)$ of $M$ the map $F_N : M \to M \otimes H$ defined by

$$F_N = (\varphi^{-1})^* (\text{id}_N \otimes \Delta_S) = (\varphi \otimes \text{id}_H) \circ (\text{id}_N \otimes \Delta_S) \circ \varphi^{-1}.$$ 

Since $(\text{id}_N \otimes \Delta_S)$ is the canonical $(H, S)$-Hopf module structure on $N \otimes RS$, by Lemma 2.2, the map $F_N$ belongs to $C^1(H, M)$.

Suppose that $(N, \varphi)$ and $(N', \varphi')$ are two equivalent twisted forms of $M$ via $\vartheta \in \text{Aut}_S(M)$. Set $f = \varphi' \circ (\vartheta \otimes \text{id}_S) \circ \varphi^{-1}$. Observe that the following diagram commutes:

So $F_{N'}$ equals $f^* F_N$ and therefore $\tilde{D}$ induces a quotient map

$$\mathcal{D} : \text{Twist}(S/R, N_0) \to D^1(H, M).$$

It remains to prove that $\mathcal{T} \circ \mathcal{D}$ and $\mathcal{D} \circ \mathcal{T}$ are the identity maps.

The composition $\mathcal{T} \circ \mathcal{D}$ is the identity. Let $(N, \varphi)$ be a twisted form of $N_0$. Since $N_{F_N} \otimes RS$ is isomorphic to $N \otimes RS$ (Lemma 2.7), we deduce from Hopf-Galois descent theory [11, Theorem 3.7] the existence of an isomorphism $\vartheta : N \to N_{F_N}$. So the twisted form $\mathcal{T}(\mathcal{D}(N, \varphi))$ is equivalent to $(N, \varphi)$. In concrete terms, $\vartheta$ fits into the following commutative diagram of $R$-modules with exact rows:

Hence one gets $\mathcal{T} \circ \mathcal{D} = \text{id}$.

The composition $\mathcal{D} \circ \mathcal{T}$ is the identity. Let $F$ be an element of $C^1(M, H)$. Consider the following diagram:
The left and right triangles are trivially commutative. The upper trapezium commutes by the definition of $F_{N_F}$. Let us show the commutativity of the lower trapezium. Pick an indecomposable tensor $m \otimes s$ in $N_F \otimes_R S$. Setting $\Delta_S(s) = s_0 \otimes s_1$, we have

$$ (\varphi_F \otimes \text{id}_H) \circ (\text{id}_{N_F} \otimes \Delta_S)(m \otimes s) = \varphi_F(m \otimes s_0) \otimes s_1 = ms_0 \otimes s_1. $$

The latter equality comes from Lemma 2.7. On the other hand, using the $(H, S)$-linearity of $F$, one has

$$ (F \circ \varphi_F)(m \otimes s) = F(ms) = F(m)\Delta_S(s) = ms_0 \otimes s_1. $$

So the whole diagram is commutative. Hence we obtain $F = F_{N_F}$, which means $\tilde{D} \circ \tilde{T} = \text{id}$. Therefore we conclude $\tilde{D} \circ \tilde{T} = \text{id}$. \hfill \Box

2.4. The 1-descent cohomology set and torsors.

Let $G$ be a finite group and $A$ be a $G$-group. Recall that an $A$-torsor (or $A$-principal homogeneous space) is a non-empty $G$-set $P$ on which $A$ acts on the right in a compatible way with the $G$-action and such that $P$ is an affine space over $A$ (see [13]). Pursuing our analogy between non-abelian group- and Hopf-cohomology theories, we are led to state the following definition.

Let $H$ be a Hopf algebra and $M$ be an $(H, S)$-Hopf module. An $M$-torsor is a triple $(X, \Delta_X, \beta)$, where $\Delta_X : X \rightarrow X \otimes H$ is a map conferring $X$ a structure of $(H, S)$-Hopf module and $\beta : M \rightarrow X$ is an $S$-linear isomorphism. Denote by $\text{tors}(M)$ the set of $M$-torsors. It is pointed with distinguished point $(M, \Delta_M, \text{id}_M)$. We say that two $M$-torsors $(X, \Delta_X, \beta)$ and $(X', \Delta_{X'}, \beta')$ are equivalent if there exists $f \in \text{Aut}_S(M)$ such that the composition $\beta' \circ f \circ \beta'^{-1} : X' \rightarrow X$ is a morphism of $(H, S)$-Hopf modules. Denote by $\text{Tors}(M)$ the set of equivalence classes of $M$-torsors; it is pointed with distinguished point the class of $(M, \Delta_M, \text{id}_M)$. We have the following result:

**Proposition 2.8.** Let $H$ be a Hopf algebra and $M$ be an $(H, S)$-Hopf module. There is an isomorphism of pointed sets

$$ D^1(H, M) \cong \text{Tors}(M). $$

*Proof.* Define $\tilde{U} : C^1(H, M) \rightarrow \text{tors}(M)$ and $\tilde{V} : \text{tors}(M) \rightarrow C^1(H, M)$ by

$$ \tilde{U} : F \mapsto (M, F, \text{id}_M) \quad \text{and} \quad \tilde{V} : (X, \Delta_X, \beta) \mapsto \beta^* \Delta_X. $$

We set here $\beta^* \Delta_X = (\beta^{-1} \otimes \text{id}_H) \circ \Delta_X \circ \beta$, which, following Lemma 2.2, is an element of $C^1(H, M)$ since $\Delta_X$ belongs to $C^1(H, X)$. Using again Lemma 2.2, it is easy to check that $\tilde{U}$ and $\tilde{V}$ define maps $U : D^1(H, M) \rightarrow \text{Tors}(M)$ and $V : \text{Tors}(M) \rightarrow D^1(H, M)$ on the quotients.

It is straightforward to prove $\tilde{V} \circ \tilde{U} = \text{id}_{C^1(H, M)}$. Moreover, the torsor $(\tilde{U} \circ \tilde{V})(X, \Delta_X, \beta)$ equals $(M, \beta^* \Delta_X, \text{id}_M)$, which, via $f = \text{id}_M$, is equivalent to $(X, \Delta_X, \beta)$ in $\text{Tors}(M)$. \hfill \Box

3. The isomorphism between Hopf cohomology sets and descent cohomology sets.

In this paragraph, we interpret the noncommutative Hopf cohomology sets in terms of the descent cohomology sets.

Let $H$ be a Hopf-algebra and $(M, \Delta_M : M \rightarrow M \otimes H)$ be an $H$-comodule. We define a map $\bar{k}$ from $W^1_k(M)$ to itself by the formula

$$ \bar{k}(\Phi) = \Phi \circ \Delta_M, $$

for any $\Phi \in W^1_k(M)$. The map $\bar{k}$ is a bijection. Indeed, denote by $\Delta'_M$ the map $(\text{id}_M \otimes \sigma_H) \circ \Delta_M$, which is easily seen to be the $\circ$-inverse of $\Delta_M$ in $W^1_k(M)$. The inverse map of $\bar{k}$ is therefore given by

$$ \bar{k}^{-1}(\Phi) = \Phi \circ \Delta'_M. $$
**Theorem 3.1.** Let $H$ be a Hopf-algebra, $S$ be an $H$-comodule algebra, and $M$ be an $(H,S)$-Hopf module with coaction $\Delta_M : M \rightarrow M \otimes H$. The identity map $\text{id}_{\text{Aut}_S(M)}$ realizes the equality of groups
\[
H^0(H, M) = D^0(H, M).
\]
The translation map $\kappa$ induces an isomorphism of pointed sets
\[
\kappa : H^1(H, M) \rightarrow D^1(H, M).
\]

As a consequence of this result and of Proposition 2.5, one immediately gets the following corollary which relates non-abelian Hopf-cohomology objects to non-abelian group-cohomology objects:

**Corollary 3.2.** Let $G$ be a finite group, $\psi : R \rightarrow S$ be a $G$-Galois extension, and $M = N_0 \otimes_R S$ be the extended $S$-module of an $R$-module $N_0$. There is the equality of groups
\[
H^0(k^G, M) = H^0(G, \text{Aut}_S(M))
\]
and an isomorphism of pointed sets
\[
H^1(k^G, M) \cong H^1(G, \text{Aut}_S(M)).
\]

**Proof of Theorem 3.1.**

0-level. Let $\varphi$ be an element of $H^0(H, M)$. Then, by definition we have $d^0 \varphi = d^1 \varphi$. This equality implies
\[
(id_M \otimes \mu_H)(d^0 \varphi \otimes \text{id}_H) \Delta_M = (id_M \otimes \mu_H)(d^1 \varphi \otimes \text{id}_H) \Delta_M.
\]
Let us compute the left-hand side on an element $m \in M$. We get
\[
(id_M \otimes \mu_H)(d^0 \varphi \otimes \text{id}_H) \Delta_M(m) = \varphi(m_0) \otimes \varphi(m_0) \sigma_H(m_1) m_2 = \varphi(m_0) \otimes \varphi(m_0) \varepsilon_H(m_1)
\]
\[
= (\Delta_M \circ \varphi)(m_0 \varepsilon_H(m_1)) = (\Delta_M \circ \varphi)(m).
\]
The right-hand side applied to $m \in M$ is equal to
\[
(id_M \otimes \mu_H)(d^1 \varphi \otimes \text{id}_H) \Delta_M(m) = \varphi(m_0) \otimes 1_H m_1 = \varphi(m_0) \otimes m_1 = (\varphi \otimes \text{id}_H) \Delta_M(m).
\]
Thus, one has $\Delta_M \circ \varphi = (\varphi \otimes \text{id}_H) \circ \Delta_M$, and therefore $f$ belongs to $D^0(H, M)$.

Conversely, let $f$ be an element of $D^0(H, M)$. It satisfies the relation $(f \otimes \text{id}_H) \circ \Delta_M = \Delta_M \circ f$. Compose each term of this equality on the left with $(id_M \otimes \mu_H) \circ (\Delta_M \otimes \sigma_H)$. The left-hand side becomes then exactly $d^0 f$. Apply the right-hand side on $m \in M$. Setting $m' = f(m)$, we get
\[
m_0' \otimes m_1' \sigma_H(m_2') = m_0' \otimes \varepsilon_H(m_1') 1_H = m_0' \otimes 1_H = f(m) \otimes 1_H = d^1 f(m).
\]
Therefore $d^0 f$ equals $d^1 f$, hence $f$ belongs to $H^0(H, M)$.

1-level. We begin to prove that $\tilde{\kappa}$ restricts to a bijection, still denoted by $\tilde{\kappa}$, from $Z^1(H, M)$ to $C^1(H, M)$. With the aim to do that, we shall show that via $\tilde{\kappa}$, for any $i = 1, 2, 3$, Condition CC$_i$ of §1.1 is equivalent to Condition CC$_i$ of §2.1. We then prove that the bijection $\kappa$ induces a quotient map $\kappa : H^1(H, M) \rightarrow D^1(H, M)$ which is an isomorphism. Adopt the following notations. For $\Phi \in Z^1(H, M)$ and $m \in M$, we denote the tensor $\Phi(m) \in M \otimes H$ by $m_{[0]} \otimes m_{[1]}$. Similarly, for $F \in C^1(H, M)$ and $m \in M$, we set $F(m) = m_{(0)} \otimes m_{(1)}$. 

...
– **Equivalence of Condition ZC₁ and Condition CC₁.** Fix \( \Phi \in Z^1(\mathcal{H}, M) \) and set \( F = \tilde{\kappa}(\Phi) = \Phi \circ \Delta_M \). So, for any \( m \in M \), we have \( F(m) = (m_0)_{[0]} \otimes (m_0)_{[1]} m_1 \). Pick now \( s \in S \). Condition ZC₁ on \( \Phi \) means \((ms)_{[0]} \otimes (ms)_{[1]} = m_{[0]} s \otimes m_{[1]} \). Let us compute \( F(ms) \):

\[
F(ms) = ((ms)_0)_{[0]} \otimes ((ms)_0)_{[1]} (ms)_1 \\
= (m_0 s_0)_{[0]} \otimes (m_0 s_0)_{[1]} m_1 s_1 \\
= (m_0)_{[0]} s_0 \otimes (m_0)_{[1]} m_1 s_1 \\
= F(m) \Delta_S(s).
\]

We use here the fact that \( \Delta_M \) is twisted \( S \)-linear (second equality). Hence \( F \) verifies Condition CC₁.

Conversely, fix \( F \in C^1(\mathcal{H}, M) \). Condition CC₁ on \( F \) means \((ms)_{[0]} \otimes (ms)_{[1]} = m_{[0]} s \otimes m_{[1]} \), for any \( s \) in \( S \). Set \( \Phi = \tilde{\kappa}^{-1}(F) = F \circ \Delta'_M \), so \( \Phi(m) = (m_0)_{[0]} \otimes (m_0)_{[1]} \sigma_H(m_1) \). Compute \( \Phi(ms) \):

\[
\Phi(ms) = ((ms)_0)_{[0]} \otimes ((ms)_0)_{[1]} \sigma_H((ms)_1) \\
= (m_0 s_0)_{[0]} \otimes (m_0 s_0)_{[1]} \sigma_H(s_1) \sigma_H(m_1) \\
= (m_0)_{[0]} s_0 \otimes (m_0)_{[1]} s_1 \sigma_H(s_2) \sigma_H(m_1) \\
= (m_0)_{[0]} s_0 \otimes (m_0)_{[1]} \varepsilon_H(s_1) \sigma_H(m_1) \\
= (m_0)_{[0]} s \otimes (m_0)_{[1]} \sigma_H(m_1) \\
= \Phi(m)(s \otimes 1).
\]

Thus \( \Phi \) verifies Condition ZC₁.

– **Equivalence of Condition ZC₂ and Condition CC₂.** We still take \( \Phi \in Z^1(\mathcal{H}, M) \) and set \( F = \tilde{\kappa}(\Phi) = \Phi \circ \Delta_M \), so \( F(m) = (m_0)_{[0]} \otimes (m_0)_{[1]} m_1 \), for any \( m \in M \). Pick \( s \in S \). Condition ZC₂ on \( \Phi \) is given by the relation \( m_{[0]} \varepsilon_H(m_{[1]}) = m \). Let us verify Condition CC₂ for \( F \):

\[
(id_M \otimes \varepsilon_H) F(m) = (m_0)_{[0]} \varepsilon_H((m_0)_{[1]} \varepsilon_H(m_1) \\
= (m_0) \varepsilon_H(m_1) \\
= (id_M \otimes \varepsilon_H) \Delta_M(m) \\
= m.
\]

Conversely, if \( F \) verifies Condition CC₂, an easy computation shows that \( \Phi = F \circ \Delta'_M \) fulfils Condition ZC₂.

– **Equivalence of Condition ZC₃ and Condition CC₃.** We introduce the deformed differential map \( \delta : W^1_\mathcal{S}(M) \longrightarrow W^2_\mathcal{S}(M) \) defined on \( \Phi \in W^1_\mathcal{S}(M) \) by the formula

\[
\delta \Phi = (id_M \otimes T) \circ d^2 \Phi
\]

(recall that \( T \) is the flip of \( H \otimes H \), see §1.1). We prove now that Condition CC₃ on \( F \in W^1_\mathcal{S}(M) \) may be translated into the equality

\[
d^2 F \circ \delta F = d^1 F. \tag{4}
\]

Indeed, as a consequence of the definitions of \( \circ \) and of \( d^2 \), one gets

\[
d^2 F \circ \delta F = (id_M \otimes \mu_H^{\otimes 2})(id_M \otimes \chi_2)(d^2 F \otimes id_H^{\otimes 2}) \delta F = (id_M \otimes \mu_H^{\otimes 2})(id_M \otimes \chi_2)(F \otimes \eta_H \otimes id_H^{\otimes 2}) \delta F.
\]
Take $m \in M$ and observe that we have $\delta F(m) = m_{(0)} \otimes 1 \otimes m_{(1)}$. Let us compute $(d^2 F \circ \delta F)(m)$:

$$
(d^2 F \circ \delta F)(m) = (\text{id}_M \otimes \mu_H^{\otimes 2}) (\text{id}_M \otimes \chi_2)(F \otimes H \otimes \text{id}_H^{\otimes 2}) \delta F(m)
$$

$$
= (\text{id}_M \otimes \mu_H^{\otimes 2}) (\text{id}_M \otimes \chi_2)(F \otimes H \otimes \text{id}_H^{\otimes 2})(m_{(0)} \otimes 1 \otimes m_{(1)})
$$

$$
= F(m_{(0)}) \otimes m_{(1)}
$$

$$
= \left( (F \otimes \text{id}_H) \circ F \right)(m).
$$

Since $d^1 F = (\text{id}_M \otimes \Delta_H) \circ F$, Condition $CC_3$ is equivalent to Equality (4).

Let $\Phi$ be an element of $W^1_S(M)$. Set $F = \tilde{\kappa}(\Phi) = \Phi \circ \Delta_M$. We write down a sequence of equivalent assertions which begins with Condition $ZC_3$ on $\Phi$ and ends with an avatar of (4).

$$
(d^2 \Delta'_M \circ d^0 F)(m) = x_0 \otimes \sigma_H(x_1) x_2 \sigma_H(m_{(1)}) \otimes 1 y = x \otimes \sigma_H(m_{(1)}) \otimes y.
$$

Combining (5) and (6), one obtains

$$
((d^2 \Delta'_M \circ d^0 F) \circ (d^0 \Delta'_M \circ d^1 \Delta_M))(m) = x \otimes \varepsilon_H(m_{(1)}) m_{2} \otimes y 1
$$

$$
= \text{id}_M \otimes T)(x \otimes y \otimes \varepsilon_H(m_{(1)}) 1)
$$

$$
= (\text{id}_M \otimes T)(F \otimes \text{id}_H)(m_{0} \otimes \varepsilon_H(m_{(1)}) 1)
$$

$$
= (\text{id}_M \otimes T)(F(m) \otimes 1)
$$

$$
= (d^2 F)(m)
$$

$$
= (\delta F)(m).
$$

- **Factorization of $\tilde{\kappa}$.** We claim that the bijection $\tilde{\kappa}$ factorizes through an isomorphism from $H^1(H, M)$ to $D^1(H, M)$. Indeed, take $\Phi$ and $\Phi'$ two cohomologous 1-Hopf cocycles and $f \in \text{Aut}_S(M)$ satisfying the equality $d^1 f^{-1} \circ \Phi \circ d^0 f = \Phi'$. Set $F = \tilde{\kappa}(\Phi)$ and $F' = \tilde{\kappa}(\Phi')$. One has then the equivalences

$$
d^1 f^{-1} \circ \Phi \circ d^0 f = \Phi' \iff d^1 f^{-1} \circ (F \circ \Delta'_M) \circ d^0 f = F' \circ \Delta'_M
$$

$$
\iff F \circ \Delta'_M \circ d^0 f \circ \Delta_M = d^1 f \circ F'
$$

$$
\iff F \circ d^1 f = d^1 f \circ F'
$$

$$
\iff F \circ f = (F \circ \text{id}_H) \circ F'.
$$
The last equality means that $F$ and $F'$ are descent-cohomologous. Observe that the third equivalence is a consequence of the equality $d^0 f = \Delta_M \circ d^1 f \circ \Delta'_M$, which may be easily checked by the reader.

\textit{Post-scriptum.} The present work in its first preprint version led T. Brzeziński to generalize the descent cohomology to the coring framework \cite{2}. For any coring $C$ and any $C$-comodule $M$, this author defines two descent cohomology sets $D^0(C,M)$ and $D^1(C,M)$, which coincide respectively with $D^0(H,M)$ and $D^1(H,M)$ (notations of \S 2) when $C$ is the coring $S \otimes H$.

\textbf{REFERENCES}

[1] A. BLANCO FERRO, Hopf algebras and Galois descent, \textit{Publ. Sec. Mat. Universitat Autònoma Barcelona} \textbf{30} (1986), no. 1, 65 – 80.

[2] T. BRZEZIŃSKI, Descent cohomology and corings, Preprint arXiv: \texttt{math.RA/0601491} (2006).

[3] M. CIPOLLA, Discesa fedelmente piatta dei moduli, \textit{Rendiconti del Circolo Matemàtico di Palermo}, Serie II - tomo XXV (1976).

[4] P. DELIGNE, Catégories tannakiennes, \textit{The Grothendieck Festschrift}, Vol. II, 111 – 195, Progr. Math., 87, Birkhäuser Boston, Boston, MA (1990).

[5] Y. DOI, M. TAKEUCHI, Hopf-Galois extensions of algebras, the Miyashita-Ulbrich action, and Azumaya algebras, \textit{J. Algebra} \textbf{121} (1989), no. 2, 488 – 516.

[6] M.A. KNUS, \textit{Quadratic and hermitian forms over rings}, Grundlehren der mathematischen Wissenschaften 294, Springer-Verlag, Berlin - Heidelberg - New York (21991).

[7] H. F. KREIMER, M. TAKEUCHI, Hopf algebras and Galois extensions of an algebra, \textit{Indiana Univ. Math. J.} \textbf{30} (1981), no. 5, 675 – 692.

[8] S. LANG, J. TATE, Principal homogeneous spaces over abelian varieties, \textit{Amer. J. Maths.} \textbf{80} (1958), 659 – 684.

[9] L. LE BRUYN, M. VAN DEN BERGH, F. VAN OYSTAEYEN, \textit{Graded orders}, Birkhäuser, Boston – Basel (1988).

[10] P. NUSS, Noncommutative descent and non-abelian cohomology, \textit{K-Theory} \textbf{12} (1997), no. 1, 23 – 74.

[11] H.-J. SCHNEIDER, Principal homogeneous spaces for arbitrary Hopf algebras, \textit{Israel J. Math.} \textbf{72} (1990), no. 1 – 2, 167 – 195.

[12] J.-P. SERRE, \textit{Corps locaux}, Troisième édition corrigée, Hermann, Paris (1968).

[13] J.-P. SERRE, \textit{Galois cohomology}, Springer-Verlag, Berlin – Heidelberg (1997). Translated from \textit{Cohomologie galoisienne}, Lecture Notes in Mathematics 5, Springer-Verlag, Berlin – Heidelberg – New York (1973).

[14] M. E. SWEEDLER, Cohomology of algebras over Hopf algebras, \textit{Trans. Amer. Math. Soc.} \textbf{133} (1968), 205 – 239.