On the algebra structure of Hopf algebras occurring in Hopf-Galois theory

Cornelius Greither

June 24, 2021

Universität der Bundeswehr München

We fix a Galois extension L/K of fields, with group G, assuming $\mathrm{char}(K) = 0$ throughout.

We fix a Galois extension L/K of fields, with group G, assuming $\mathrm{char}(K) = 0$ throughout. We consider "structures" over K; these may be, for example, K-algebras, K-Hopf algebras, or just K-vector spaces ...

We fix a Galois extension L/K of fields, with group G, assuming $\mathrm{char}(K) = 0$ throughout. We consider "structures" over K; these may be, for example, K-algebras, K-Hopf algebras, or just K-vector spaces ...

To avoid repetition, we do things generally, for any kind of structure; morphisms are tacitly assumed to be in the appropriate category. We now explain the notion of "form" .

We fix a Galois extension L/K of fields, with group G, assuming $\mathrm{char}(K) = 0$ throughout. We consider "structures" over K; these may be, for example, K-algebras, K-Hopf algebras, or just K-vector spaces ...

To avoid repetition, we do things generally, for any kind of structure; morphisms are tacitly assumed to be in the appropriate category. We now explain the notion of "form" .

Let A be a structure over K. A second structure B is called an *L-form of A* if

We fix a Galois extension L/K of fields, with group G, assuming $\mathrm{char}(K) = 0$ throughout. We consider "structures" over K; these may be, for example, K-algebras, K-Hopf algebras, or just K-vector spaces ...

To avoid repetition, we do things generally, for any kind of structure; morphisms are tacitly assumed to be in the appropriate category. We now explain the notion of "form" .

Let A be a structure over K. A second structure B is called an *L-form of A* if

$$L \otimes_K A \cong L \otimes_K B.$$

Examples:

We start with the simplest structure, **vector spaces.** If A is an n-dimensional space over K, then so is any L-form B of A

Examples:

We start with the simplest structure, **vector spaces.** If A is an n-dimensional space over K, then so is any L-form B of A (because of the invariance of dimension under base change).

Consequence: Vector spaces do not have nontrivial forms.

Examples:

We start with the simplest structure, **vector spaces.** If A is an n-dimensional space over K, then so is any L-form B of A (because of the invariance of dimension under base change).

Consequence: Vector spaces do not have nontrivial forms.

Hopf Galois theory: If H is a K-Hopf algebra and M/K is H-Galois, then

Examples:

We start with the simplest structure, **vector spaces.** If A is an n-dimensional space over K, then so is any L-form B of A (because of the invariance of dimension under base change).

Consequence: Vector spaces do not have nontrivial forms.

Hopf Galois theory: If H is a K-Hopf algebra and M/K is H-Galois, then

$$M \otimes_K M \cong M \otimes_K H^*.$$

Examples:

We start with the simplest structure, **vector spaces.** If A is an n-dimensional space over K, then so is any L-form B of A (because of the invariance of dimension under base change).

Consequence: Vector spaces do not have nontrivial forms.

Hopf Galois theory: If H is a K-Hopf algebra and M/K is H-Galois, then

$$M \otimes_K M \cong M \otimes_K H^*.$$

In other words, the algebra M is an M-form of the algebra H^*. Note M occurs twice! Once in the place of formerly L.

Examples:

We start with the simplest structure, **vector spaces.** If A is an n-dimensional space over K, then so is any L-form B of A (because of the invariance of dimension under base change).

Consequence: Vector spaces do not have nontrivial forms.

Hopf Galois theory: If H is a K-Hopf algebra and M/K is H-Galois, then

$$M \otimes_K M \cong M \otimes_K H^*.$$

In other words, the algebra M is an M-form of the algebra H^*. Note M occurs twice! Once in the place of formerly L.

Simple special case: the classical Hopf-Galois structure, $H = K[N]$. Then $H^* = K^{|N|} = K \times \cdots \times K$ (indexed by N),

Examples:

We start with the simplest structure, **vector spaces.** If A is an n-dimensional space over K, then so is any L-form B of A (because of the invariance of dimension under base change).

Consequence: Vector spaces do not have nontrivial forms.

Hopf Galois theory: If H is a K-Hopf algebra and M/K is H-Galois, then

$$M \otimes_K M \cong M \otimes_K H^*.$$

In other words, the algebra M is an M-form of the algebra H^*. Note M occurs twice! Once in the place of formerly L.

Simple special case: the classical Hopf-Galois structure, $H = K[N]$. Then $H^* = K^{|N|} = K \times \cdots \times K$ (indexed by N), and any N-Galois extension M/K is a form of the "trivial N-Galois extension" $K^{|N|}$.

Before we say more about Hopf-Galois extensions, we describe the general mechanism of determining the set of all L-forms, modulo K-isomorphism. This uses a little group cohomology; we will only use $\mathrm{H}^1(G, X)$, Before we say more about Hopf-Galois extensions, we describe the general mechanism of determining the set of all L-forms, modulo K-isomorphism. This uses a little group cohomology; we will only use $\mathrm{H}^1(G, X)$, which means the set of 1-cocycles (= crossed homomorphisms) $G \to X$, modulo a suitable equivalence relation.

Before we say more about Hopf-Galois extensions, we describe the general mechanism of determining the set of all L-forms, modulo K-isomorphism. This uses a little group cohomology; we will only use $\mathrm{H}^1(G, X)$, which means the set of 1-cocycles (= crossed homomorphisms) $G \to X$, modulo a suitable equivalence relation. Here X is any group acted upon by G, the Galois group of a given extension L/K.

Before we say more about Hopf-Galois extensions, we describe the general mechanism of determining the set of all L-forms, modulo K-isomorphism. This uses a little group cohomology; we will only use $\mathrm{H}^1(G, X)$, which means the set of 1-cocycles (= crossed homomorphisms) $G \to X$, modulo a suitable equivalence relation. Here X is any group acted upon by G, the Galois group of a given extension L/K.

Unless X is abelian, $\mathrm{H}^1(G, X)$ will only be a pointed set, not a group.

Before we say more about Hopf-Galois extensions, we describe the general mechanism of determining the set of all L-forms, modulo K-isomorphism. This uses a little group cohomology; we will only use $\mathrm{H}^1(G, X)$, which means the set of 1-cocycles (= crossed homomorphisms) $G \to X$, modulo a suitable equivalence relation. Here X is any group acted upon by G, the Galois group of a given extension L/K.

Unless X is abelian, $\mathrm{H}^1(G, X)$ will only be a pointed set, not a group.

Theorem

Let $\mathrm{Forms}_{L/K}(A)$ denote the set of L-forms of A, modulo K-isomorphism. Then there is a bijection as follows, in which the trivial form A corresponds to the distinguished element:

Before we say more about Hopf-Galois extensions, we describe the general mechanism of determining the set of all L-forms, modulo K-isomorphism. This uses a little group cohomology; we will only use $\mathrm{H}^1(G, X)$, which means the set of 1-cocycles (= crossed homomorphisms) $G \to X$, modulo a suitable equivalence relation. Here X is any group acted upon by G, the Galois group of a given extension L/K.

Unless X is abelian, $\mathrm{H}^1(G, X)$ will only be a pointed set, not a group.

Theorem

Let $\mathrm{Forms}_{L/K}(A)$ denote the set of L-forms of A, modulo K-isomorphism. Then there is a bijection as follows, in which the trivial form A corresponds to the distinguished element:

$$\mathrm{Forms}_{L/K}(A) \to \mathrm{H}^1(G, \mathrm{Aut}_L(L \otimes_K A)).$$

We explain how the forms arise from a given cocycle, and how our decription connects to that of Childs.

We explain how the forms arise from a given cocycle, and how our decription connects to that of Childs.

Assume $(\vartheta_g)_{g\in G}$ is a 1-cocycle of automorphisms of $L \otimes_K A$. Consider

We explain how the forms arise from a given cocycle, and how our decription connects to that of Childs.

Assume $(\vartheta_g)_{g \in G}$ is a 1-cocycle of automorphisms of $L \otimes_K A$. Consider

$$\beta_g = \vartheta_g \circ (g \otimes id_A).$$

We explain how the forms arise from a given cocycle, and how our decription connects to that of Childs.

Assume $(\vartheta_g)_{g\in G}$ is a 1-cocycle of automorphisms of $L \otimes_K A$. Consider

$$\beta_g = \vartheta_g \circ (g \otimes id_A).$$

Then the cocycle condition on the ϑ_g translates into $\beta_{gh} = \beta_g\beta_h$, so G acts semilinearly on $L \otimes_K A$.

We explain how the forms arise from a given cocycle, and how our decription connects to that of Childs.

Assume $(\vartheta_g)_{g\in G}$ is a 1-cocycle of automorphisms of $L \otimes_K A$. Consider

$$\beta_g = \vartheta_g \circ (g \otimes id_A).$$

Then the cocycle condition on the ϑ_g translates into $\beta_{gh} = \beta_g\beta_h$, so G acts semilinearly on $L \otimes_K A$. The form B is the common fixed set of all β_g.

We explain how the forms arise from a given cocycle, and how our decription connects to that of Childs.

Assume $(\vartheta_g)_{g\in G}$ is a 1-cocycle of automorphisms of $L \otimes_K A$. Consider

$$\beta_g = \vartheta_g \circ (g \otimes id_A).$$

Then the cocycle condition on the ϑ_g translates into $\beta_{gh} = \beta_g \beta_h$, so G acts semilinearly on $L \otimes_K A$. The form B is the common fixed set of all β_g.

This agrees with Childs' decription, where the semilinear automorphisms are extracted from an action of the entire endomorphism ring $End_K(L)$.

Example: Forms of vector spaces. Let V be n-dimensional over K.

Example: Forms of vector spaces. Let V be n-dimensional over K. So w.l.o.g. $V = K^n$. Hence

Example: Forms of vector spaces. Let V be n-dimensional over K. So w.l.o.g. $V = K^n$. Hence

$$\mathrm{Aut}_L(L \otimes_K V) = GL_n(L).$$

Example: Forms of vector spaces. Let V be n-dimensional over K. So w.l.o.g. $V = K^n$. Hence

$$\mathrm{Aut}_L(L \otimes_K V) = GL_n(L).$$

A generalization of Hilbert's Thm. 90 states: $\mathrm{H}^1\left(G, GL_n(L)\right)$ is trivial.

Example: Forms of vector spaces. Let V be n-dimensional over K. So w.l.o.g. $V = K^n$. Hence

$$\mathrm{Aut}_L(L \otimes_K V) = GL_n(L).$$

A generalization of Hilbert's Thm. 90 states: $\mathrm{H}^1\left(G, GL_n(L)\right)$ is trivial.

This confirms our observation: In the category of finite-dimensional vector spaces, all forms are trivial.

Example involving Hopf algebras: Let $L = K(i)$ (with $i = \sqrt{-1}$) and assume $L \neq K$. We write $G = \mathrm{Gal}(L/K) = \{1, \tau\}$.

Example involving Hopf algebras: Let $L = K(i)$ (with $i = \sqrt{-1}$) and assume $L \neq K$. We write $G = \mathrm{Gal}(L/K) = \{1, \tau\}$.

For A we take $K[N]$ where $N = \{1, e, e^2, e^3\}$ is the cyclic group of order 4. Then

Example involving Hopf algebras: Let $L = K(i)$ (with $i = \sqrt{-1}$) and assume $L \neq K$. We write $G = \mathrm{Gal}(L/K) = \{1, \tau\}$.

For A we take $K[N]$ where $N = \{1, e, e^2, e^3\}$ is the cyclic group of order 4. Then $\vartheta_1 = id$, $\vartheta_\tau : e \mapsto e^{-1} = e^3$ defines a 1-cocycle of automorphisms of $L[N]$. What is the associated form?

Example involving Hopf algebras: Let $L = K(i)$ (with $i = \sqrt{-1}$) and assume $L \neq K$. We write $G = \mathrm{Gal}(L/K) = \{1, \tau\}$.

For A we take $K[N]$ where $N = \{1, e, e^2, e^3\}$ is the cyclic group of order 4. Then $\vartheta_1 = id, \ \vartheta_\tau : e \mapsto e^{-1} = e^3$ defines a 1-cocycle of automorphisms of $L[N]$. What is the associated form?

We are looking for elements $x \in L \oplus Le \oplus Le^2 \oplus Le^3$ such that applying ϑ_τ, followed by τ on coefficients, leaves x intact.

Example involving Hopf algebras: Let $L = K(i)$ (with $i = \sqrt{-1}$) and assume $L \neq K$. We write $G = \mathrm{Gal}(L/K) = \{1, \tau\}$.

For A we take $K[N]$ where $N = \{1, e, e^2, e^3\}$ is the cyclic group of order 4. Then $\vartheta_1 = id$, $\vartheta_\tau : e \mapsto e^{-1} = e^3$ defines a 1-cocycle of automorphisms of $L[N]$. What is the associated form?

We are looking for elements $x \in L \oplus Le \oplus Le^2 \oplus Le^3$ such that applying ϑ_τ, followed by τ on coefficients, leaves x intact. Just by guessing one finds two such elements:

$$c = (e + e^3)/2; \quad s = (e - e^3)/(2i).$$

Example involving Hopf algebras: Let $L = K(i)$ (with $i = \sqrt{-1}$) and assume $L \neq K$. We write $G = \mathrm{Gal}(L/K) = \{1, \tau\}$.

For A we take $K[N]$ where $N = \{1, e, e^2, e^3\}$ is the cyclic group of order 4. Then $\vartheta_1 = id$, $\vartheta_\tau : e \mapsto e^{-1} = e^3$ defines a 1-cocycle of automorphisms of $L[N]$. What is the associated form?

We are looking for elements $x \in L \oplus Le \oplus Le^2 \oplus Le^3$ such that applying ϑ_τ, followed by τ on coefficients, leaves x intact. Just by guessing one finds two such elements:

$$c = (e + e^3)/2; \quad s = (e - e^3)/(2i).$$

The are reminiscent of cosine and sine. Indeed they satisfy $c^2 + s^2 = 1$, and one can check $B = K[c, s]$.

Recall $c = (e + e^{-1})/2$; $s = (e - e^{-1})/(2i)$; $\quad B = K[c, s]$.

Recall $c = (e + e^{-1})/2$; $s = (e - e^{-1})/(2i)$; $\quad B = K[c, s]$.

This Hopf algebra B does show up in a Hopf-Galois situation: $M = K(w)$ with $w^4 = u \in K^\times$. (We assume $[M : K] = 4$.)

Recall $c = (e + e^{-1})/2;\ s = (e - e^{-1})/(2i); \quad B = K[c, s].$

This Hopf algebra B does show up in a Hopf-Galois situation:
$M = K(w)$ with $w^4 = u \in K^\times$. (We assume $[M : K] = 4$.)

Then there is an action, making M into a B-Hopf Galois extension.
We have for example: $cw = 0, sw = w, cw^2 = -w^2, sw^2 = 0$.

Another example with Hopf algebras: Here we begin with the Hopf Galois context. Let M/K be a given N-Galois extension, where N is any finite group.

Another example with Hopf algebras: Here we begin with the Hopf Galois context. Let M/K be a given N-Galois extension, where N is any finite group. Consequently, M/K is Hopf Galois for the Hopf algebra $A = K[N]$ (the classical case).

Another example with Hopf algebras: Here we begin with the Hopf Galois context. Let M/K be a given N-Galois extension, where N is any finite group. Consequently, M/K is Hopf Galois for the Hopf algebra $A = K[N]$ (the classical case).

Then there exist a Hopf algebra B such that M/K is also B-Hopf Galois; but such that the resulting correspondence only sees the normal intermediate fields, not all fields as for the classical case.

Another example with Hopf algebras: Here we begin with the Hopf Galois context. Let M/K be a given N-Galois extension, where N is any finite group. Consequently, M/K is Hopf Galois for the Hopf algebra $A = K[N]$ (the classical case).

Then there exist a Hopf algebra B such that M/K is also B-Hopf Galois; but such that the resulting correspondence only sees the normal intermediate fields, not all fields as for the classical case.

We describe how B is obtained as a form of A.

Another example with Hopf algebras: Here we begin with the Hopf Galois context. Let M/K be a given N-Galois extension, where N is any finite group. Consequently, M/K is Hopf Galois for the Hopf algebra $A = K[N]$ (the classical case).

Then there exist a Hopf algebra B such that M/K is also B-Hopf Galois; but such that the resulting correspondence only sees the normal intermediate fields, not all fields as for the classical case.

We describe how B is obtained as a form of A.

We put $L = M$; $G := N$ acts on N and hence on $L[N]$ by inner automorphisms: $\vartheta_g(\nu) = g\nu g^{-1}$. This defines the form B.

Another example with Hopf algebras: Here we begin with the Hopf Galois context. Let M/K be a given N-Galois extension, where N is any finite group. Consequently, M/K is Hopf Galois for the Hopf algebra $A = K[N]$ (the classical case).

Then there exist a Hopf algebra B such that M/K is also B-Hopf Galois; but such that the resulting correspondence only sees the normal intermediate fields, not all fields as for the classical case.

We describe how B is obtained as a form of A.

We put $L = M$; $G := N$ acts on N and hence on $L[N]$ by inner automorphisms: $\vartheta_g(\nu) = g\nu g^{-1}$. This defines the form B. As soon as N is not abelian, this form is nontrivial as we will see. We call it the anti-classical Hopf form.

Underwood's observation (at a conference in 2016):

Underwood's observation (at a conference in 2016):

Take $K = \mathbb{Q}$ and $M/\mathbb{Q}$ any Galois extension with group $N = S_3$. Then, as remarked above, the M-form B of the group ring $\mathbb{Q}[S_3]$ is nontrivial, as a form in the category of Hopf algebras, but ...

Underwood's observation (at a conference in 2016):

Take $K = \mathbb{Q}$ and $M/\mathbb{Q}$ any Galois extension with group $N = S_3$. Then, as remarked above, the M-form B of the group ring $\mathbb{Q}[S_3]$ is nontrivial, as a form in the category of Hopf algebras, but ...

it is trivial in the category of $\mathbb{Q}$-algebras!

Underwood's observation (at a conference in 2016):

Take $K = \mathbb{Q}$ and $M/\mathbb{Q}$ any Galois extension with group $N = S_3$. Then, as remarked above, the M-form B of the group ring $\mathbb{Q}[S_3]$ is nontrivial, as a form in the category of Hopf algebras, but ...

it is trivial in the category of $\mathbb{Q}$-algebras!

We elaborate a little. From representation theory we easily get that

$$\mathbb{Q}[S_3] \cong \mathbb{Q} \times \mathbb{Q} \times M_2(\mathbb{Q}) \quad \text{as algebras.}$$

Underwood's observation (at a conference in 2016):

Take $K = \mathbb{Q}$ and $M/\mathbb{Q}$ any Galois extension with group $N = S_3$. Then, as remarked above, the M-form B of the group ring $\mathbb{Q}[S_3]$ is nontrivial, as a form in the category of Hopf algebras, but . . .

it is trivial in the category of $\mathbb{Q}$-algebras!

We elaborate a little. From representation theory we easily get that

$$\mathbb{Q}[S_3] \cong \mathbb{Q} \times \mathbb{Q} \times M_2(\mathbb{Q}) \quad \text{as algebras.}$$

Underwood's observation (proved by direct calculation) is then: B is also isomorphic to $\mathbb{Q} \times \mathbb{Q} \times M_2(\mathbb{Q})$.

Underwood's observation (at a conference in 2016):

Take $K = \mathbb{Q}$ and $M/\mathbb{Q}$ any Galois extension with group $N = S_3$. Then, as remarked above, the M-form B of the group ring $\mathbb{Q}[S_3]$ is nontrivial, as a form in the category of Hopf algebras, but ...

it is trivial in the category of $\mathbb{Q}$-algebras!

We elaborate a little. From representation theory we easily get that

$$\mathbb{Q}[S_3] \cong \mathbb{Q} \times \mathbb{Q} \times M_2(\mathbb{Q}) \quad \text{as algebras.}$$

Underwood's observation (proved by direct calculation) is then: B is also isomorphic to $\mathbb{Q} \times \mathbb{Q} \times M_2(\mathbb{Q})$. In the rest of this talk we try to explain the reason why this isomorphism happens in many other situations, and generalize things still further.

We recall a few things and make some general remarks.

We recall a few things and make some general remarks.

Fix any field L and any finite group N. Then every group automorphism ν of N induces an automorphism of the L-Hopf algebra $A_L = L[N]$.

Fact (easy to prove):

We recall a few things and make some general remarks.

Fix any field L and any finite group N. Then every group automorphism ν of N induces an automorphism of the L-Hopf algebra $A_L = L[N]$.

Fact (easy to prove): All L-Hopf automorphisms of the group ring $L[N]$ are of this kind.

We recall a few things and make some general remarks.

Fix any field L and any finite group N. Then every group automorphism ν of N induces an automorphism of the L-Hopf algebra $A_L = L[N]$.

Fact (easy to prove): All L-Hopf automorphisms of the group ring $L[N]$ are of this kind.

The equivalence relation "cohomologous" for two 1-cocycles $G \to \mathrm{Aut}_L(A_L) = \mathrm{Aut}(N)$ is as follows:

We recall a few things and make some general remarks.

Fix any field L and any finite group N. Then every group automorphism ν of N induces an automorphism of the L-Hopf algebra $A_L = L[N]$.

Fact (easy to prove): All L-Hopf automorphisms of the group ring $L[N]$ are of this kind.

The equivalence relation "cohomologous" for two 1-cocycles $G \to \mathrm{Aut}_L(A_L) = \mathrm{Aut}(N)$ is as follows:

$$(\vartheta_g)_{g\in G} \sim (\vartheta'_g)_{g\in G} \iff \exists\ \nu \in \mathrm{Aut}(N) : \vartheta'_g = \nu\vartheta_g\nu^{-1}\ \forall g \in G.$$

We recall a few things and make some general remarks.

Fix any field L and any finite group N. Then every group automorphism ν of N induces an automorphism of the L-Hopf algebra $A_L = L[N]$.

Fact (easy to prove): All L-Hopf automorphisms of the group ring $L[N]$ are of this kind.

The equivalence relation "cohomologous" for two 1-cocycles $G \to \mathrm{Aut}_L(A_L) = \mathrm{Aut}(N)$ is as follows:

$$(\vartheta_g)_{g\in G} \sim (\vartheta'_g)_{g\in G} \iff \exists\ \nu \in \mathrm{Aut}(N) : \vartheta'_g = \nu\vartheta_g\nu^{-1}\ \forall g \in G.$$

In particular the trivial cocycle $\vartheta_g = id_N$ is only cohomologous to itself!

The trivial cocycle $\vartheta_g = id_N$ is only cohomologous to itself;

The trivial cocycle $\vartheta_g = id_N$ is only cohomologous to itself;

so every nontrivial cocycle defines a nontrivial Hopf form. This applies in particular to the anticlassical Hopf form of $K[N]$, as soon as N is not abelian.

The trivial cocycle $\vartheta_g = id_N$ is only cohomologous to itself;

so every nontrivial cocycle defines a nontrivial Hopf form. This applies in particular to the anticlassical Hopf form of $K[N]$, as soon as N is not abelian. Remember that in this case the cocycle ϑ_g is given as conjugation by $g \in G = N$.

The trivial cocycle $\vartheta_g = id_N$ is only cohomologous to itself;

so every nontrivial cocycle defines a nontrivial Hopf form. This applies in particular to the anticlassical Hopf form of $K[N]$, as soon as N is not abelian. Remember that in this case the cocycle ϑ_g is given as conjugation by $g \in G = N$.

Our main result, to be stated below (we will even sketch a proof) will imply:

The trivial cocycle $\vartheta_g = id_N$ is only cohomologous to itself;

so every nontrivial cocycle defines a nontrivial Hopf form. This applies in particular to the anticlassical Hopf form of $K[N]$, as soon as N is not abelian. Remember that in this case the cocycle ϑ_g is given as conjugation by $g \in G = N$.

Our main result, to be stated below (we will even sketch a proof) will imply:

For every finite group N and every N-extension L/K, the anti-classical Hopf form $B = B_N(L/K)$ of $A = K[N]$ is isomorphic to A as a K-algebra.

Recall: An automorphism ν of a group N is inner, if it is given as conjugation $C(\sigma)$ by some element $\sigma \in N$. The inner automorphisms form a group $\mathrm{Inn}(N)$;

Recall: An automorphism ν of a group N is inner, if it is given as conjugation $C(\sigma)$ by some element $\sigma \in N$. The inner automorphisms form a group $\mathrm{Inn}(N)$; sending σ to $C(\sigma)$ identifies $\mathrm{Inn}(N)$ with N modulo its center.

Recall: An automorphism ν of a group N is inner, if it is given as conjugation $C(\sigma)$ by some element $\sigma \in N$. The inner automorphisms form a group $\mathrm{Inn}(N)$; sending σ to $C(\sigma)$ identifies $\mathrm{Inn}(N)$ with N modulo its center.

Many non-abelian groups, e.g. S_n for $n \neq 6$, have only inner automorphisms. On the other hand, any inner automorphism of an abelian group is trivial.

Recall: An automorphism ν of a group N is inner, if it is given as conjugation $C(\sigma)$ by some element $\sigma \in N$. The inner automorphisms form a group $\mathrm{Inn}(N)$; sending σ to $C(\sigma)$ identifies $\mathrm{Inn}(N)$ with N modulo its center.

Many non-abelian groups, e.g. S_n for $n \neq 6$, have only inner automorphisms. On the other hand, any inner automorphism of an abelian group is trivial.

We will consider, as before, cocycles $\vartheta : G \to \mathrm{Aut}(N) = \mathrm{Aut}_L(L[N])$, where L/K is a G-Galois extension.

Recall: An automorphism ν of a group N is inner, if it is given as conjugation $C(\sigma)$ by some element $\sigma \in N$. The inner automorphisms form a group $\mathrm{Inn}(N)$; sending σ to $C(\sigma)$ identifies $\mathrm{Inn}(N)$ with N modulo its center.

Many non-abelian groups, e.g. S_n for $n \neq 6$, have only inner automorphisms. On the other hand, any inner automorphism of an abelian group is trivial.

We will consider, as before, cocycles $\vartheta : G \to \mathrm{Aut}(N) = \mathrm{Aut}_L(L[N])$, where L/K is a G-Galois extension.

Definition: (1) ϑ is inner, if all ϑ_g are in Inn(N).

Recall: An automorphism ν of a group N is inner, if it is given as conjugation $C(\sigma)$ by some element $\sigma \in N$. The inner automorphisms form a group $\mathrm{Inn}(N)$; sending σ to $C(\sigma)$ identifies $\mathrm{Inn}(N)$ with N modulo its center.

Many non-abelian groups, e.g. S_n for $n \neq 6$, have only inner automorphisms. On the other hand, any inner automorphism of an abelian group is trivial.

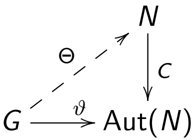
We will consider, as before, cocycles $\vartheta : G \to \mathrm{Aut}(N) = \mathrm{Aut}_L(L[N])$, where L/K is a G-Galois extension.

Definition: (1) ϑ is inner, if all ϑ_g are in Inn(N).

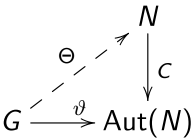
(2) ϑ is liftable, if there is a homomorphism $\Theta : G \to N$ with $\vartheta_g = C(\Theta(g))$, all $g \in G$.

ϑ is inner $\iff$ $\vartheta : G \to \mathrm{Inn}(N)$.

ϑ is inner $\iff$ $\vartheta : G \to \mathrm{Inn}(N)$.

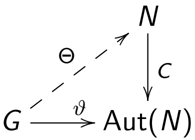


ϑ is inner $\iff$ $\vartheta : G \to \mathrm{Inn}(N)$.



Obviously, liftable cocycles are inner. Moreover, both notions "inner" and "liftable" make also sense for cohomology classes (behave well with respect to equivalence of cocycles).

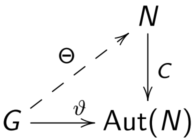
ϑ is inner $\iff$ $\vartheta : G \to \mathrm{Inn}(N)$.



Obviously, liftable cocycles are inner. Moreover, both notions "inner" and "liftable" make also sense for cohomology classes (behave well with respect to equivalence of cocycles).

Hence, it is legitimate to talk about inner forms, and liftable forms.

ϑ is inner $\iff \vartheta : G \to \mathrm{Inn}(N)$.



Obviously, liftable cocycles are inner. Moreover, both notions "inner" and "liftable" make also sense for cohomology classes (behave well with respect to equivalence of cocycles).

Hence, it is legitimate to talk about inner forms, and liftable forms.

We remark in passing: If N is centerless, then $\mathrm{Inn}(N)$ identifies with N (via C), and then "inner" and "liftable" are the same.

Theorem

Every liftable form of the K-Hopf algebra $K[N]$ is isomorphic to $K[N]$ as an algebra.

Theorem

Every liftable form of the K-Hopf algebra $K[N]$ is isomorphic to $K[N]$ as an algebra.

Let us note that the anticlassical form is a liftable form: Indeed, the cocycle $(\vartheta_g)_g$ is by definition $\vartheta_g = C(g)$, so we can put $\Theta =$ identity in the triangle.

Theorem

Every liftable form of the K-Hopf algebra $K[N]$ is isomorphic to $K[N]$ as an algebra.

Let us note that the anticlassical form is a liftable form: Indeed, the cocycle $(\vartheta_g)_g$ is by definition $\vartheta_g = C(g)$, so we can put $\Theta =$ identity in the triangle.

In a way, the anticlassical cocycle is the "universal liftable" cocycle!

Theorem

Every liftable form of the K-Hopf algebra $K[N]$ is isomorphic to $K[N]$ as an algebra.

Let us note that the anticlassical form is a liftable form: Indeed, the cocycle $(\vartheta_g)_g$ is by definition $\vartheta_g = C(g)$, so we can put $\Theta =$ identity in the triangle.

In a way, the anticlassical cocycle is the “universal liftable” cocycle!

The proof will use a bit of cohomology (this will be explained, cheating just a little ...), plus a straightforward generalization of Hilbert 90, which will be stated but not proved.

So assume we have a liftable 1-cocycle $\vartheta = C \circ \Theta$, with C being a group homomorphism $G \to N$.

So assume we have a liftable 1-cocycle $\vartheta = C \circ \Theta$, with C being a group homomorphism $G \to N$. (Recall: $C(\sigma)$ is conjugation with σ, $\sigma \in N$; $A = K[N]$; $A_L = L[N]$.)

So assume we have a liftable 1-cocycle $\vartheta = C \circ \Theta$, with C being a group homomorphism $G \to N$. (Recall: $C(\sigma)$ is conjugation with σ, $\sigma \in N$; $A = K[N]$; $A_L = L[N]$.)

Preparation: A decomposes (via Wedderburn's theorem) as a finite product of simple algebras

So assume we have a liftable 1-cocycle $\vartheta = C \circ \Theta$, with C being a group homomorphism $G \to N$. (Recall: $C(\sigma)$ is conjugation with σ, $\sigma \in N$; $A = K[N]$; $A_L = L[N]$.)

Preparation: A decomposes (via Wedderburn's theorem) as a finite product of simple algebras (matrix rings over skew fields, which all are finite-dimensional over K). One *can* show that every automorphism ϑ_g respects this decomposition.

So assume we have a liftable 1-cocycle $\vartheta = C \circ \Theta$, with C being a group homomorphism $G \to N$. (Recall: $C(\sigma)$ is conjugation with σ, $\sigma \in N$; $A = K[N]$; $A_L = L[N]$.)

Preparation: A decomposes (via Wedderburn's theorem) as a finite product of simple algebras (matrix rings over skew fields, which all are finite-dimensional over K). One *can* show that every automorphism ϑ_g respects this decomposition.

So we will pretend that A is already a simple algebra (which is never literally true!)

So assume we have a liftable 1-cocycle $\vartheta = C \circ \Theta$, with C being a group homomorphism $G \to N$. (Recall: $C(\sigma)$ is conjugation with σ, $\sigma \in N$; $A = K[N]$; $A_L = L[N]$.)

Preparation: A decomposes (via Wedderburn's theorem) as a finite product of simple algebras (matrix rings over skew fields, which all are finite-dimensional over K). One *can* show that every automorphism ϑ_g respects this decomposition.

So we will pretend that A is already a simple algebra (which is never literally true!) It will suffice that the form B defined by the given cocycle is isomorphic as an algebra to A.

We consider the homomorphism $c : A_L^\times \to \mathrm{Aut}_L(A_L)$ which sends x to conjugation with x.

We consider the homomorphism $c : A_L^\times \to \mathrm{Aut}_L(A_L)$ which sends x to conjugation with x.

Then we have for all $\sigma \in G$: $\vartheta_\sigma = c(\Theta(\sigma))$.

We consider the homomorphism $c : A_L^\times \to \mathrm{Aut}_L(A_L)$ which sends x to conjugation with x.

Then we have for all $\sigma \in G$: $\vartheta_\sigma = c(\Theta(\sigma))$.

Now $\Theta : G \to A_L^\times$ is a 1-cocycle again. There is the following generalization of Hilbert 90:

We consider the homomorphism $c : A_L^\times \to \mathrm{Aut}_L(A_L)$ which sends x to conjugation with x.

Then we have for all $\sigma \in G$: $\vartheta_\sigma = c(\Theta(\sigma))$.

Now $\Theta : G \to A_L^\times$ is a 1-cocycle again. There is the following generalization of Hilbert 90:

Proposition

If A is any simple finite-dimensional K-algebra, then $\mathrm{H}^1(G, A_L^\times)$ is trivial.

We consider the homomorphism $c : A_L^\times \to \mathrm{Aut}_L(A_L)$ which sends x to conjugation with x.

Then we have for all $\sigma \in G$: $\vartheta_\sigma = c(\Theta(\sigma))$.

Now $\Theta : G \to A_L^\times$ is a 1-cocycle again. There is the following generalization of Hilbert 90:

Proposition

If A is any simple finite-dimensional K-algebra, then $\mathrm{H}^1(G, A_L^\times)$ is trivial.

So Θ is equivalent to the trivial cocycle $G \to A_L^\times$;

We consider the homomorphism $c : A_L^\times \to \mathrm{Aut}_L(A_L)$ which sends x to conjugation with x.

Then we have for all $\sigma \in G$: $\vartheta_\sigma = c(\Theta(\sigma))$.

Now $\Theta : G \to A_L^\times$ is a 1-cocycle again. There is the following generalization of Hilbert 90:

Proposition

If A is any simple finite-dimensional K-algebra, then $\mathrm{H}^1(G, A_L^\times)$ is trivial.

So Θ is equivalent to the trivial cocycle $G \to A_L^\times$; applying c gives that ϑ is equivalent to the trivial cocycle $G \to \mathrm{Aut}_L(A_L)$.

We consider the homomorphism $c : A_L^\times \to \mathrm{Aut}_L(A_L)$ which sends x to conjugation with x.

Then we have for all $\sigma \in G$: $\vartheta_\sigma = c(\Theta(\sigma))$.

Now $\Theta : G \to A_L^\times$ is a 1-cocycle again. There is the following generalization of Hilbert 90:

Proposition

If A is any simple finite-dimensional K-algebra, then $\mathrm{H}^1(G, A_L^\times)$ is trivial.

So Θ is equivalent to the trivial cocycle $G \to A_L^\times$; applying c gives that ϑ is equivalent to the trivial cocycle $G \to \mathrm{Aut}_L(A_L)$. Looks like cheating, but it works! — q.e.d.

We now turn to cases which are not covered by the main result on liftable forms.

We now turn to cases which are not covered by the main result on liftable forms.

There are two obvious situations to consider: cocycles which are not inner to begin with (this will happen if N is abelian),

We now turn to cases which are not covered by the main result on liftable forms.

There are two obvious situations to consider: cocycles which are not inner to begin with (this will happen if N is abelian), and cocycles which are inner but not liftable. The latter is more subtle and appears to be more interesting.

We now turn to cases which are not covered by the main result on liftable forms.

There are two obvious situations to consider: cocycles which are not inner to begin with (this will happen if N is abelian), and cocycles which are inner but not liftable. The latter is more subtle and appears to be more interesting.

Recall an earlier example: N cyclic of order 4, $G = \mathrm{Gal}(K(i)/K)$ of order 2; the nontrivial element $\tau \in G$ gives the automorphism ϑ_τ $=$ inversion on N.

We now turn to cases which are not covered by the main result on liftable forms.

There are two obvious situations to consider: cocycles which are not inner to begin with (this will happen if N is abelian), and cocycles which are inner but not liftable. The latter is more subtle and appears to be more interesting.

Recall an earlier example: N cyclic of order 4, $G = \mathrm{Gal}(K(i)/K)$ of order 2; the nontrivial element $\tau \in G$ gives the automorphism ϑ_τ $=$ inversion on N.

One can show $K[N] \cong K \times K \times K[i]$ and

We now turn to cases which are not covered by the main result on liftable forms.

There are two obvious situations to consider: cocycles which are not inner to begin with (this will happen if N is abelian), and cocycles which are inner but not liftable. The latter is more subtle and appears to be more interesting.

Recall an earlier example: N cyclic of order 4, $G = \mathrm{Gal}(K(i)/K)$ of order 2; the nontrivial element $\tau \in G$ gives the automorphism ϑ_τ $=$ inversion on N.

One can show $K[N] \cong K \times K \times K[i]$ and the form B is a product of four copies of K.

We now turn to cases which are not covered by the main result on liftable forms.

There are two obvious situations to consider: cocycles which are not inner to begin with (this will happen if N is abelian), and cocycles which are inner but not liftable. The latter is more subtle and appears to be more interesting.

Recall an earlier example: N cyclic of order 4, $G = \mathrm{Gal}(K(i)/K)$ of order 2; the nontrivial element $\tau \in G$ gives the automorphism ϑ_τ $=$ inversion on N.

One can show $K[N] \cong K \times K \times K[i]$ and the form B is a product of four copies of K.

So the conclusion of the main theorem does not hold; of course ϑ is not inner.

As our final topic, we look at cocycles which are inner but not liftable.

As our final topic, we look at cocycles which are inner but not liftable.

As said before, we then need a group N that has a nontrivial center; so $N = S_3$ is out.

As our final topic, we look at cocycles which are inner but not liftable.

As said before, we then need a group N that has a nontrivial center; so $N = S_3$ is out. We will take the dihedral group $N = D_4$; this does have a center of order 2, and has the extra advantage that Taylor and Truman have studied Hopf Galois situations where forms of $K[D_4]$ occur.

As our final topic, we look at cocycles which are inner but not liftable.

As said before, we then need a group N that has a nontrivial center; so $N = S_3$ is out. We will take the dihedral group $N = D_4$; this does have a center of order 2, and has the extra advantage that Taylor and Truman have studied Hopf Galois situations where forms of $K[D_4]$ occur.

Let us give the elementary facts on D_4 and its group ring.

As our final topic, we look at cocycles which are inner but not liftable.

As said before, we then need a group N that has a nontrivial center; so $N = S_3$ is out. We will take the dihedral group $N = D_4$; this does have a center of order 2, and has the extra advantage that Taylor and Truman have studied Hopf Galois situations where forms of $K[D_4]$ occur.

Let us give the elementary facts on D_4 and its group ring.

D_4 has two generators s and t, of order 4 and 2 respectively,

As our final topic, we look at cocycles which are inner but not liftable.

As said before, we then need a group N that has a nontrivial center; so $N = S_3$ is out. We will take the dihedral group $N = D_4$; this does have a center of order 2, and has the extra advantage that Taylor and Truman have studied Hopf Galois situations where forms of $K[D_4]$ occur.

Let us give the elementary facts on D_4 and its group ring.

D_4 has two generators s and t, of order 4 and 2 respectively, and we have the rule

$$tst = s^3 (= s^{-1}).$$

The Wedderburn decomposition of $K[D_4]$ is

$$K \times K \times K \times K \times M_2(K),$$

The Wedderburn decomposition of $K[D_4]$ is

$$K \times K \times K \times K \times M_2(K),$$

where $K \times K \times K \times K$ can be identified with $K[D_4^{ab}] = K[C_2 \times C_2]$;

The Wedderburn decomposition of $K[D_4]$ is

$$K \times K \times K \times K \times M_2(K),$$

where $K \times K \times K \times K$ can be identified with $K[D_4^{ab}] = K[C_2 \times C_2]$; this is, so to speak, the abelian part of this group ring.

The Wedderburn decomposition of $K[D_4]$ is

$$K \times K \times K \times K \times M_2(K),$$

where $K \times K \times K \times K$ can be identified with $K[D_4^{ab}] = K[C_2 \times C_2]$; this is, so to speak, the abelian part of this group ring.

One can easily show that every inner cocycle leads to a form B whose "abelian part" is again K^4; in fact, then the cocycle defining the form of the abelian part is trivial.

The Wedderburn decomposition of $K[D_4]$ is

$$K \times K \times K \times K \times M_2(K),$$

where $K \times K \times K \times K$ can be identified with $K[D_4^{ab}] = K[C_2 \times C_2]$; this is, so to speak, the abelian part of this group ring.

One can easily show that every inner cocycle leads to a form B whose "abelian part" is again K^4; in fact, then the cocycle defining the form of the abelian part is trivial.

So what really matters is what happens to the non-abelian part $M_2(K)$; the corresponding factor B' of B will also be a central simple K-algebra of dimension 4,

The Wedderburn decomposition of $K[D_4]$ is

$$K \times K \times K \times K \times M_2(K),$$

where $K \times K \times K \times K$ can be identified with $K[D_4^{ab}] = K[C_2 \times C_2]$; this is, so to speak, the abelian part of this group ring.

One can easily show that every inner cocycle leads to a form B whose "abelian part" is again K^4; in fact, then the cocycle defining the form of the abelian part is trivial.

So what really matters is what happens to the non-abelian part $M_2(K)$; the corresponding factor B' of B will also be a central simple K-algebra of dimension 4, and the question is whether it is a matrix algebra or a skew field.

Recall: $B = B^{ab} \times B'$; and B^{ab} is not interesting.

Recall: $B = B^{ab} \times B'$; and B^{ab} is not interesting.

Do there exist inner cocycles that are not liftable?

Recall: $B = B^{ab} \times B'$; and B^{ab} is not interesting.

Do there exist inner cocycles that are not liftable?

Yes, if L/K and G are suitably chosen. Take G to be the quaternion group of order 8.

Recall: $B = B^{ab} \times B'$; and B^{ab} is not interesting.

Do there exist inner cocycles that are not liftable?

Yes, if L/K and G are suitably chosen. Take G to be the quaternion group of order 8. Explicitly:

$$Q_8 = \langle \sigma, \tau | \sigma^4 = 1, \tau^2 = \sigma^2, \tau\sigma\tau^{-1} = \sigma^3 \rangle.$$

Recall: $B = B^{ab} \times B'$; and B^{ab} is not interesting.

Do there exist inner cocycles that are not liftable?

Yes, if L/K and G are suitably chosen. Take G to be the quaternion group of order 8. Explicitly:

$$Q_8 = \langle \sigma, \tau | \sigma^4 = 1, \tau^2 = \sigma^2, \tau\sigma\tau^{-1} = \sigma^3 \rangle.$$

We define $\vartheta : Q_8 \to \mathrm{Inn}(D_4)$ by: $\vartheta_\sigma = C(s)$ and $\vartheta_\tau = C(t)$.

Recall: $B = B^{ab} \times B'$; and B^{ab} is not interesting.

Do there exist inner cocycles that are not liftable?

Yes, if L/K and G are suitably chosen. Take G to be the quaternion group of order 8. Explicitly:

$$Q_8 = \langle \sigma, \tau | \sigma^4 = 1, \tau^2 = \sigma^2, \tau\sigma\tau^{-1} = \sigma^3 \rangle.$$

We define $\vartheta : Q_8 \to \mathrm{Inn}(D_4)$ by: $\vartheta_\sigma = C(s)$ and $\vartheta_\tau = C(t)$.

Then Q_8 and D_4 are in a way similar enough for ϑ to be a group homomorphism but not similar enough for ϑ to be liftable through $C : N \to \mathrm{Inn}(N)$.

To describe the final result, we take a closer look at the Q_8-extension L/K.

To describe the final result, we take a closer look at the Q_8-extension L/K. The fixed fields of σ and τ, respectively, are quadratic over K; we write them in the form $K(\sqrt{a})$ and $K(\sqrt{b})$ respectively.

To describe the final result, we take a closer look at the Q_8-extension L/K. The fixed fields of σ and τ, respectively, are quadratic over K; we write them in the form $K(\sqrt{a})$ and $K(\sqrt{b})$ respectively.

Theorem

The L-form B' of $M_2(K)$ given by the cocycle ϑ described above is the quaternion algebra

$$B' = (-a, b)_K.$$

To describe the final result, we take a closer look at the Q_8-extension L/K. The fixed fields of σ and τ, respectively, are quadratic over K; we write them in the form $K(\sqrt{a})$ and $K(\sqrt{b})$ respectively.

Theorem

The L-form B' of $M_2(K)$ given by the cocycle ϑ described above is the quaternion algebra

$$B' = (-a, b)_K.$$

Using this, one can produce examples of both phenomena: B' can be a matrix algebra (that is, the form B is trivial in the category of K-algebras),

To describe the final result, we take a closer look at the Q_8-extension L/K. The fixed fields of σ and τ, respectively, are quadratic over K; we write them in the form $K(\sqrt{a})$ and $K(\sqrt{b})$ respectively.

Theorem

The L-form B' of $M_2(K)$ given by the cocycle ϑ described above is the quaternion algebra

$$B' = (-a, b)_K.$$

Using this, one can produce examples of both phenomena: B' can be a matrix algebra (that is, the form B is trivial in the category of K-algebras), or it can be a skew-field, and this means the form B is nontrivial even as an algebra.

To describe the final result, we take a closer look at the Q_8-extension L/K. The fixed fields of σ and τ, respectively, are quadratic over K; we write them in the form $K(\sqrt{a})$ and $K(\sqrt{b})$ respectively.

Theorem

The L-form B' of $M_2(K)$ given by the cocycle ϑ described above is the quaternion algebra

$$B' = (-a, b)_K.$$

Using this, one can produce examples of both phenomena: B' can be a matrix algebra (that is, the form B is trivial in the category of K-algebras), or it can be a skew-field, and this means the form B is nontrivial even as an algebra. (Can take $K = \mathbb{Q}$, $a = 3$, $b = 2$.)