A generalization of Kummer theory to Hopf-Galois extensions

Daniel Gil Muñoz

Charles University in Prague
Department of Algebra

Hopf Algebras & Galois Module Theory
June 2023

University of Nebraska at Omaha (online)

Let $n \in \mathbb{Z}_{>0}$ and let K be a field with $\mathrm{char}(K) \nmid n$.

Let $n \in \mathbb{Z}_{>0}$ and let K be a field with $\mathrm{char}(K) \nmid n$.

Definition

A field Galois extension L/K is Kummer if $\zeta_n \in K$ and the Galois group G is abelian of exponent dividing n.

Let $n \in \mathbb{Z}_{>0}$ and let K be a field with $\mathrm{char}(K) \nmid n$.

Definition

A field Galois extension L/K is Kummer if $\zeta_n \in K$ and the Galois group G is abelian of exponent dividing n.

The Kummer extensions of K are the radical ones

$$L = K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_k}), \quad \zeta_n \in K.$$

Let $n \in \mathbb{Z}_{>0}$ and let K be a field with $\mathrm{char}(K) \nmid n$.

Definition

A field Galois extension L/K is Kummer if $\zeta_n \in K$ and the Galois group G is abelian of exponent dividing n.

The Kummer extensions of K are the radical ones

$$L = K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_k}), \quad \zeta_n \in K.$$

We can rewrite the Kummer condition in terms of the Galois group and its action on L.

Let $n \in \mathbb{Z}_{>0}$ and let K be a field with $\mathrm{char}(K) \nmid n$.

Definition

A field Galois extension L/K is Kummer if $\zeta_n \in K$ and the Galois group G is abelian of exponent dividing n.

The Kummer extensions of K are the radical ones

$$L = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}), \quad \zeta_n \in K.$$

We can rewrite the Kummer condition in terms of the Galois group and its action on L.

Now, if L/K is an H-Galois extension, one can follow the style of that definition to define an H-Kummer condition.

Let $n \in \mathbb{Z}_{>0}$ and let K be a field with $\mathrm{char}(K) \nmid n$.

Definition

A field Galois extension L/K is Kummer if $\zeta_n \in K$ and the Galois group G is abelian of exponent dividing n.

The Kummer extensions of K are the radical ones

$$L = K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_k}), \quad \zeta_n \in K.$$

We can rewrite the Kummer condition in terms of the Galois group and its action on L.

Now, if L/K is an H-Galois extension, one can follow the style of that definition to define an H-Kummer condition.

From this new perspective, we can study many extensions for which $\zeta_n \notin K$ and translate results as the one above to this new setting.

Table of contents

Table of contents

Let $n \in \mathbb{Z}_{>0}$ and let K be a field with $\mathrm{char}(K) \nmid n$ and $\zeta_n \in K$.

Let $n \in \mathbb{Z}_{>0}$ and let K be a field with $\mathrm{char}(K) \nmid n$ and $\zeta_n \in K$.

Proposition

The cyclic extensions of K are the simple radical ones:

$$L = K(\sqrt[n]{a}), \quad a \in K^\times/(K^\times)^n.$$

Let $n \in \mathbb{Z}_{>0}$ and let K be a field with $\mathrm{char}(K) \nmid n$ and $\zeta_n \in K$.

Proposition

The cyclic extensions of K are the simple radical ones:

$$L = K(\sqrt[n]{a}), \quad a \in K^\times/(K^\times)^n.$$

Let L/K be a cyclic degree n extension with group G.

Let $n \in \mathbb{Z}_{>0}$ and let K be a field with $\mathrm{char}(K) \nmid n$ and $\zeta_n \in K$.

Proposition

The cyclic extensions of K are the simple radical ones:

$$L = K(\sqrt[n]{a}), \quad a \in K^\times/(K^\times)^n.$$

Let L/K be a cyclic degree n extension with group G.

Let $\alpha = \sqrt[n]{a}$ (in particular $L = K(\alpha)$).
The conjugates of α are $\alpha, \zeta_n\alpha, \ldots, \zeta_n^{n-1}\alpha$.

Let $n \in \mathbb{Z}_{>0}$ and let K be a field with $\mathrm{char}(K) \nmid n$ and $\zeta_n \in K$.

Proposition

The cyclic extensions of K are the simple radical ones:

$$L = K(\sqrt[n]{a}), \quad a \in K^\times/(K^\times)^n.$$

Let L/K be a cyclic degree n extension with group G.

Let $\alpha = \sqrt[n]{a}$ (in particular $L = K(\alpha)$).
The conjugates of α are $\alpha, \zeta_n\alpha, \ldots, \zeta_n^{n-1}\alpha$.

Then for each $\sigma \in G$ there is a unique $0 \leq i_\sigma \leq n-1$ such that

$$\sigma(\alpha) = \zeta_n^{i_\sigma}\alpha.$$

Let $n \in \mathbb{Z}_{>0}$ and let K be a field with $\mathrm{char}(K) \nmid n$ and $\zeta_n \in K$.

Proposition

The cyclic extensions of K are the simple radical ones:

$$L = K(\sqrt[n]{a}), \quad a \in K^\times/(K^\times)^n.$$

Let L/K be a cyclic degree n extension with group G.

Let $\alpha = \sqrt[n]{a}$ (in particular $L = K(\alpha)$).
The conjugates of α are $\alpha, \zeta_n\alpha, \ldots, \zeta_n^{n-1}\alpha$.

Then for each $\sigma \in G$ there is a unique $0 \leq i_\sigma \leq n-1$ such that

$$\sigma(\alpha) = \zeta_n^{i_\sigma}\alpha.$$

The element α is an eigenvector of all the automorphisms in G. We call it a G-**eigenvector**.

Proposition

Let L/K be a Galois extension with group G. Then L/K admits some primitive element which is a G-eigenvector if and only if $\zeta_n \in K$ and L/K is cyclic.

Proposition

Let L/K be a Galois extension with group G. Then L/K admits some primitive element which is a G-eigenvector if and only if $\zeta_n \in K$ and L/K is cyclic.

If $L = K(\sqrt[n]{a})$ is such an extension, a primitive element which is a G-eigenvector is $\alpha = \sqrt[n]{a}$.

Proposition

Let L/K be a Galois extension with group G. Then L/K admits some primitive element which is a G-eigenvector if and only if $\zeta_n \in K$ and L/K is cyclic.

If $L = K(\sqrt[n]{a})$ is such an extension, a primitive element which is a G-eigenvector is $\alpha = \sqrt[n]{a}$.

This characterization can be extended to arbitrary Kummer extensions.

Proposition

Let L/K be a Galois extension with group G. Then L/K admits some primitive element which is a G-eigenvector if and only if $\zeta_n \in K$ and L/K is cyclic.

If $L = K(\sqrt[n]{a})$ is such an extension, a primitive element which is a G-eigenvector is $\alpha = \sqrt[n]{a}$.

This characterization can be extended to arbitrary Kummer extensions.

Idea: Any Kummer extension can be described as a compositum of cyclic extensions and the eigenvectors property *lifts* in compositums.

Let L_i/K be a Galois extension with group G_i, $i \in \{1, 2\}$. Then L_1L_2/K is a Galois extension with group $G \hookrightarrow G_1 \times G_2$.

Let L_i/K be a Galois extension with group G_i, $i \in \{1, 2\}$. Then $L_1 L_2/K$ is a Galois extension with group $G \hookrightarrow G_1 \times G_2$.

Proposition

If α_i is a G_i-eigenvector for $i \in \{1, 2\}$, then $\alpha_1\alpha_2$ is a G-eigenvector.

Let L_i/K be a Galois extension with group G_i, $i \in \{1, 2\}$. Then L_1L_2/K is a Galois extension with group $G \hookrightarrow G_1 \times G_2$.

Proposition

If α_i is a G_i-eigenvector for $i \in \{1, 2\}$, then $\alpha_1\alpha_2$ is a G-eigenvector.

Theorem

Let L/K be a Galois extension of K with group G. Then, L/K admits some finite generating set of G-eigenvectors if and only if $\zeta_n \in K$ and L/K is Kummer.

Let L_i/K be a Galois extension with group G_i, $i \in \{1,2\}$. Then L_1L_2/K is a Galois extension with group $G \hookrightarrow G_1 \times G_2$.

Proposition

If α_i is a G_i-eigenvector for $i \in \{1,2\}$, then $\alpha_1\alpha_2$ is a G-eigenvector.

Theorem

Let L/K be a Galois extension of K with group G. Then, L/K admits some finite generating set of G-eigenvectors if and only if $\zeta_n \in K$ and L/K is Kummer.

If $L = K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_k})$ is such an extension, a finite generating set of G-eigenvectors is $\{\sqrt[n]{a_1}, \dots, \sqrt[n]{a_k}\}$.

Definition

Let L/K be an H-Galois extension. We say that $\alpha \in L$ is an H-eigenvector if for every $h \in H$ there is some $\lambda(h) \in K$ such that

$$h \cdot \alpha = \lambda(h)\alpha.$$

Definition

Let L/K be an H-Galois extension. We say that $\alpha \in L$ is an H-eigenvector if for every $h \in H$ there is some $\lambda(h) \in K$ such that

$$h \cdot \alpha = \lambda(h)\alpha.$$

The previous result says that a Galois extension L/K with $\zeta_n \in K$ is Kummer if and only if it admits some finite generating set of H_c-eigenvectors, where H_c is the classical Galois structure on L/K.

Definition

Let L/K be an H-Galois extension. We say that $\alpha \in L$ is an H-eigenvector if for every $h \in H$ there is some $\lambda(h) \in K$ such that

$$h \cdot \alpha = \lambda(h)\alpha.$$

The previous result says that a Galois extension L/K with $\zeta_n \in K$ is Kummer if and only if it admits some finite generating set of H_c-eigenvectors, where H_c is the classical Galois structure on L/K.

Definition

We say that an H-Galois extension L/K is H-Kummer if it admits some finite generating set of H-eigenvectors.

INTRODUCTION

It is well known that adjoining $\omega = \sqrt[3]{2}$ to $\mathbb{Q}$ does not give a Galois extension of $\mathbb{Q}$, i.e., there is no set of automorphisms of $\mathbb{Q}(\omega)$ whose set of common fixed elements is precisely $\mathbb{Q}$. However, one can define the following linear maps s, c from $\mathbb{Q}(\omega)$ to itself by

$$c(1) = 1, \qquad c(\omega) = -\tfrac{1}{2}\omega, \qquad c(\omega^2) = -\tfrac{1}{2}\omega^2,$$
$$s(1) = 0, \qquad s(\omega) = \tfrac{1}{2}\omega, \qquad s(\omega^2) = -\tfrac{1}{2}\omega^2,$$

Figure: C. Greither, B. Pareigis (1986)

INTRODUCTION

It is well known that adjoining $\omega = \sqrt[3]{2}$ to $\mathbb{Q}$ does not give a Galois extension of $\mathbb{Q}$, i.e., there is no set of automorphisms of $\mathbb{Q}(\omega)$ whose set of common fixed elements is precisely $\mathbb{Q}$. However, one can define the following linear maps s, c from $\mathbb{Q}(\omega)$ to itself by

$$c(1) = 1, \qquad c(\omega) = -\tfrac{1}{2}\omega, \qquad c(\omega^2) = -\tfrac{1}{2}\omega^2,$$
$$s(1) = 0, \qquad s(\omega) = \tfrac{1}{2}\omega, \qquad s(\omega^2) = -\tfrac{1}{2}\omega^2,$$

Figure: C. Greither, B. Pareigis (1986)

The extension $L = \mathbb{Q}(\omega)$ admits a unique Hopf-Galois structure H. A basis of the underlying Hopf algebra can be written as $\{\mathrm{Id}, c, s\}$.

INTRODUCTION

It is well known that adjoining $\omega = \sqrt[3]{2}$ to $\mathbb{Q}$ does not give a Galois extension of $\mathbb{Q}$, i.e., there is no set of automorphisms of $\mathbb{Q}(\omega)$ whose set of common fixed elements is precisely $\mathbb{Q}$. However, one can define the following linear maps s, c from $\mathbb{Q}(\omega)$ to itself by

$$c(1) = 1, \qquad c(\omega) = -\tfrac{1}{2}\omega, \qquad c(\omega^2) = -\tfrac{1}{2}\omega^2,$$
$$s(1) = 0, \qquad s(\omega) = \tfrac{1}{2}\omega, \qquad s(\omega^2) = -\tfrac{1}{2}\omega^2,$$

Figure: C. Greither, B. Pareigis (1986)

The extension $L = \mathbb{Q}(\omega)$ admits a unique Hopf-Galois structure H. A basis of the underlying Hopf algebra can be written as $\{\mathrm{Id}, c, s\}$.

If an element is an eigenvector with respect to a K-basis of H, then it is an H-eigenvector.

INTRODUCTION

It is well known that adjoining $\omega = \sqrt[3]{2}$ to $\mathbb{Q}$ does not give a Galois extension of $\mathbb{Q}$, i.e., there is no set of automorphisms of $\mathbb{Q}(\omega)$ whose set of common fixed elements is precisely $\mathbb{Q}$. However, one can define the following linear maps s, c from $\mathbb{Q}(\omega)$ to itself by

$$c(1)=1, \qquad c(\omega) = -\tfrac{1}{2}\omega, \qquad c(\omega^2) = -\tfrac{1}{2}\omega^2,$$
$$s(1)=0, \qquad s(\omega) = \tfrac{1}{2}\omega, \qquad s(\omega^2) = -\tfrac{1}{2}\omega^2,$$

Figure: C. Greither, B. Pareigis (1986)

The extension $L = \mathbb{Q}(\omega)$ admits a unique Hopf-Galois structure H. A basis of the underlying Hopf algebra can be written as $\{\mathrm{Id}, c, s\}$.

If an element is an eigenvector with respect to a K-basis of H, then it is an H-eigenvector.

Therefore, ω is an H-eigenvector and $L/\mathbb{Q}$ is H-Kummer.

Let L/K be a separable extension with normal closure $\widetilde{L}$, $G = \mathrm{Gal}(\widetilde{L}/K)$ and $G' = \mathrm{Gal}(\widetilde{L}/L)$.

Let L/K be a separable extension with normal closure $\widetilde{L}$, $G = \mathrm{Gal}(\widetilde{L}/K)$ and $G' = \mathrm{Gal}(\widetilde{L}/L)$.

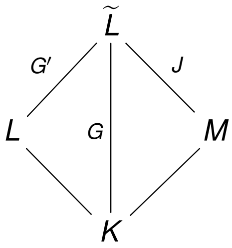
Definition

L/K is almost classically Galois (a.c.G.) if there is $J \triangleleft G$ such that $G = J \rtimes G'$. We will say that $M = \widetilde{L}^J$ is the complement of L.

Let L/K be a separable extension with normal closure $\widetilde{L}$, $G = \mathrm{Gal}(\widetilde{L}/K)$ and $G' = \mathrm{Gal}(\widetilde{L}/L)$.

Definition

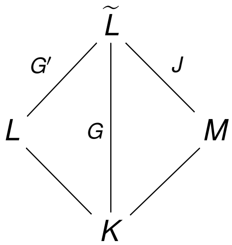
L/K is almost classically Galois (a.c.G.) if there is $J \triangleleft G$ such that $G = J \rtimes G'$. We will say that $M = \widetilde{L}^J$ is the complement of L.



Let L/K be a separable extension with normal closure $\widetilde{L}$, $G = \mathrm{Gal}(\widetilde{L}/K)$ and $G' = \mathrm{Gal}(\widetilde{L}/L)$.

Definition

L/K is almost classically Galois (a.c.G.) if there is $J \lhd G$ such that $G = J \rtimes G'$. We will say that $M = \widetilde{L}^J$ is the complement of L.

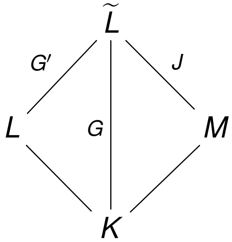


Hopf-Galois structures on L/K correspond bijectively to regular G-stable subgroups of $\mathrm{Perm}(G/G')$.

Let L/K be a separable extension with normal closure $\widetilde{L}$, $G = \mathrm{Gal}(\widetilde{L}/K)$ and $G' = \mathrm{Gal}(\widetilde{L}/L)$.

Definition

L/K is almost classically Galois (a.c.G.) if there is $J \lhd G$ such that $G = J \rtimes G'$. We will say that $M = \widetilde{L}^J$ is the complement of L.



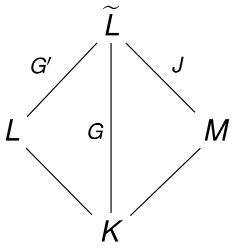
Hopf-Galois structures on L/K correspond bijectively to regular G-stable subgroups of $\mathrm{Perm}(G/G')$.

$\lambda \colon G \longrightarrow \mathrm{Perm}(G/G')$ left translation.

Let L/K be a separable extension with normal closure $\widetilde{L}$, $G = \mathrm{Gal}(\widetilde{L}/K)$ and $G' = \mathrm{Gal}(\widetilde{L}/L)$.

Definition

L/K is almost classically Galois (a.c.G.) if there is $J \lhd G$ such that $G = J \rtimes G'$. We will say that $M = \widetilde{L}^J$ is the complement of L.



Hopf-Galois structures on L/K correspond bijectively to regular G-stable subgroups of $\mathrm{Perm}(G/G')$.

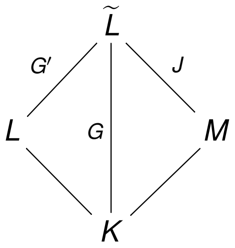
$\lambda \colon G \longrightarrow \mathrm{Perm}(G/G')$ left translation.

$N = \lambda(J)$ is such a subgroup.

Let L/K be a separable extension with normal closure $\widetilde{L}$, $G = \mathrm{Gal}(\widetilde{L}/K)$ and $G' = \mathrm{Gal}(\widetilde{L}/L)$.

Definition

L/K is almost classically Galois (a.c.G.) if there is $J \triangleleft G$ such that $G = J \rtimes G'$. We will say that $M = \widetilde{L}^J$ is the complement of L.



Hopf-Galois structures on L/K correspond bijectively to regular G-stable subgroups of $\mathrm{Perm}(G/G')$.

$\lambda\colon G \longrightarrow \mathrm{Perm}(G/G')$ left translation.

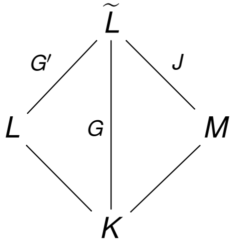
$N = \lambda(J)$ is such a subgroup.

If J is abelian, the corresponding Hopf-Galois structure will be called **the a.c.G. structure corresponding to M.**

Let L/K be a separable extension with normal closure $\widetilde{L}$, $G = \mathrm{Gal}(\widetilde{L}/K)$ and $G' = \mathrm{Gal}(\widetilde{L}/L)$.

Definition

L/K is almost classically Galois (a.c.G.) if there is $J \lhd G$ such that $G = J \rtimes G'$. We will say that $M = \widetilde{L}^J$ is the complement of L.



Hopf-Galois structures on L/K correspond bijectively to regular G-stable subgroups of $\mathrm{Perm}(G/G')$.

$\lambda\colon G \longrightarrow \mathrm{Perm}(G/G')$ left translation.

$N = \lambda(J)$ is such a subgroup.

If J is abelian, the corresponding Hopf-Galois structure will be called **the a.c.G. structure corresponding to *M*.**

Identifying $J \cong \lambda(J)$, the underlying Hopf algebra is $H = M[J]^{G'}$.

If $L = K(\sqrt[n]{a})$ is such that $L \cap K(\zeta_n) = K$, then L/K is a.c.G. with complement $M = K(\zeta_n)$.

If $L = K(\sqrt[n]{a})$ is such that $L \cap K(\zeta_n) = K$, then L/K is a.c.G. with complement $M = K(\zeta_n)$.

Proposition

Let H be the a.c.G. structure on L/K corresponding to M. Then $\alpha = \sqrt[n]{a}$ is an H-eigenvector.

If $L = K(\sqrt[n]{a})$ is such that $L \cap K(\zeta_n) = K$, then L/K is a.c.G. with complement $M = K(\zeta_n)$.

Proposition

Let H be the a.c.G. structure on L/K corresponding to M. Then $\alpha = \sqrt[n]{a}$ is an H-eigenvector.

Sketch of proof: $\widetilde{L}/M$ is a Kummer extension and α is a J-eigenvector.

If $L = K(\sqrt[n]{a})$ is such that $L \cap K(\zeta_n) = K$, then L/K is a.c.G. with complement $M = K(\zeta_n)$.

Proposition

Let H be the a.c.G. structure on L/K corresponding to M. Then $\alpha = \sqrt[n]{a}$ is an H-eigenvector.

Sketch of proof: $\widetilde{L}/M$ is a Kummer extension and α is a J-eigenvector. Since $H = M[J]^{G'}$, elements of H are M-linear combinations of elements in J.

If $L = K(\sqrt[n]{a})$ is such that $L \cap K(\zeta_n) = K$, then L/K is a.c.G. with complement $M = K(\zeta_n)$.

Proposition

Let H be the a.c.G. structure on L/K corresponding to M. Then $\alpha = \sqrt[n]{a}$ is an H-eigenvector.

Sketch of proof: $\widetilde{L}/M$ is a Kummer extension and α is a J-eigenvector. Since $H = M[J]^{G'}$, elements of H are M-linear combinations of elements in J.

Then, given $h = \sum_i m_i(h) w_i \in H$,

$$h \cdot \alpha = \sum_i m_i(h) w_i \cdot \alpha = \sum_i m_i(h) \lambda_i \alpha = \lambda(h) \alpha,$$

where $\lambda(h) = \sum_i m_i(h) \lambda_i \in M$.

If $L = K(\sqrt[n]{a})$ is such that $L \cap K(\zeta_n) = K$, then L/K is a.c.G. with complement $M = K(\zeta_n)$.

Proposition

Let H be the a.c.G. structure on L/K corresponding to M. Then $\alpha = \sqrt[n]{a}$ is an H-eigenvector.

Sketch of proof: $\widetilde{L}/M$ is a Kummer extension and α is a J-eigenvector. Since $H = M[J]^{G'}$, elements of H are M-linear combinations of elements in J.

Then, given $h = \sum_i m_i(h)w_i \in H$,

$$h \cdot \alpha = \sum_i m_i(h)w_i \cdot \alpha = \sum_i m_i(h)\lambda_i\alpha = \lambda(h)\alpha,$$

where $\lambda(h) = \sum_i m_i(h)\lambda_i \in M$. But $\lambda(h) = \frac{h\cdot\alpha}{\alpha} \in L \cap M = K$.

Theorem

Let L/K be an H-Galois extension. The following statements are equivalent:

- $L \cap K(\zeta_n) = K$ *and* L/K *is simple radical.*
- L/K *is an a.c.G. extension with complement* $K(\zeta_n)$ *and admits some primitive element which is an* H*-eigenvector, where* H *is the a.c.G. structure on* L/K *corresponding to* $K(\zeta_n)$.

Theorem

Let L/K be an H-Galois extension. The following statements are equivalent:

- $L \cap K(\zeta_n) = K$ *and* L/K *is simple radical.*
- L/K *is an a.c.G. extension with complement* $K(\zeta_n)$ *and admits some primitive element which is an* H*-eigenvector, where* H *is the a.c.G. structure on* L/K *corresponding to* $K(\zeta_n)$.

If $L = K(\sqrt[n]{a})$ is such an extension, a primitive element which is an H-eigenvector is $\alpha = \sqrt[n]{a}$.

Let $L = K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_k})$ with $L \cap K(\zeta_n) = K$.

Let $L = K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_k})$ with $L \cap K(\zeta_n) = K$.

L/K is a.c.G. with complement $M = K(\zeta_n)$ and we can consider the a.c.G. structure H corresponding to $K(\zeta_n)$.

Let $L = K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_k})$ with $L \cap K(\zeta_n) = K$.

L/K is a.c.G. with complement $M = K(\zeta_n)$ and we can consider the a.c.G. structure H corresponding to $K(\zeta_n)$.

Natural question: Is L/K H-Kummer?

Let $L = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$ with $L \cap K(\zeta_n) = K$.

L/K is a.c.G. with complement $M = K(\zeta_n)$ and we can consider the a.c.G. structure H corresponding to $K(\zeta_n)$.

Natural question: Is L/K H-Kummer?

Natural strategy: Work with the simple radical extensions $L_i = K(\sqrt[n]{a_i})$ and *lift* the information to their compositums.

Let $L = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$ with $L \cap K(\zeta_n) = K$.

L/K is a.c.G. with complement $M = K(\zeta_n)$ and we can consider the a.c.G. structure H corresponding to $K(\zeta_n)$.

Natural question: Is L/K H-Kummer?

Natural strategy: Work with the simple radical extensions $L_i = K(\sqrt[n]{a_i})$ and *lift* the information to their compositums.

Set $k = 2$, so that $L = L_1 L_2$, $L_i = K(\sqrt[n]{a_i})$.

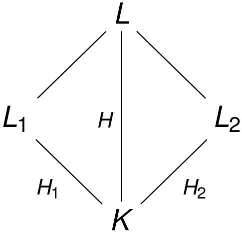
Let $L = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$ with $L \cap K(\zeta_n) = K$.

L/K is a.c.G. with complement $M = K(\zeta_n)$ and we can consider the a.c.G. structure H corresponding to $K(\zeta_n)$.

Natural question: Is L/K H-Kummer?

Natural strategy: Work with the simple radical extensions $L_i = K(\sqrt[n]{a_i})$ and *lift* the information to their compositums.

Set $k = 2$, so that $L = L_1 L_2$, $L_i = K(\sqrt[n]{a_i})$.



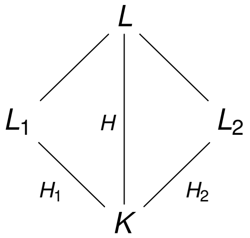
Let $L = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$ with $L \cap K(\zeta_n) = K$.

L/K is a.c.G. with complement $M = K(\zeta_n)$ and we can consider the a.c.G. structure H corresponding to $K(\zeta_n)$.

Natural question: Is L/K H-Kummer?

Natural strategy: Work with the simple radical extensions $L_i = K(\sqrt[n]{a_i})$ and *lift* the information to their compositums.

Set $k = 2$, so that $L = L_1 L_2$, $L_i = K(\sqrt[n]{a_i})$.



Let H_i be the a.c.G. structure corresponding to $K(\zeta_{n_i})$, $i \in \{1, 2\}$.

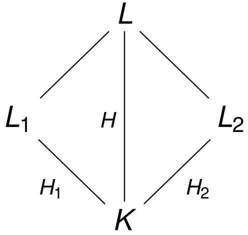
Let $L = K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_k})$ with $L \cap K(\zeta_n) = K$.

L/K is a.c.G. with complement $M = K(\zeta_n)$ and we can consider the a.c.G. structure H corresponding to $K(\zeta_n)$.

Natural question: Is L/K H-Kummer?

Natural strategy: Work with the simple radical extensions $L_i = K(\sqrt[n]{a_i})$ and *lift* the information to their compositums.

Set $k = 2$, so that $L = L_1 L_2$, $L_i = K(\sqrt[n]{a_i})$.



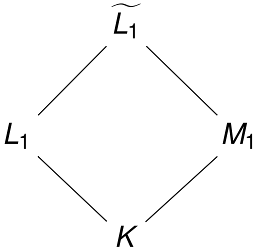
Let H_i be the a.c.G. structure corresponding to $K(\zeta_{n_i})$, $i \in \{1, 2\}$.

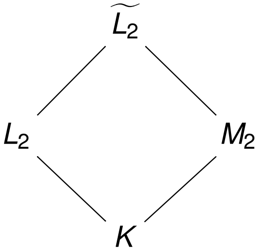
If α_i is an H_i-eigenvector, is $\alpha_1\alpha_2$ an H-eigenvector?

Table of contents

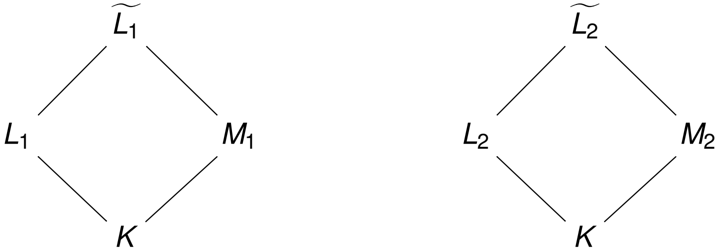
Let L_1/K, L_2/K be a.c.G. extensions.

Let L_1/K, L_2/K be a.c.G. extensions.



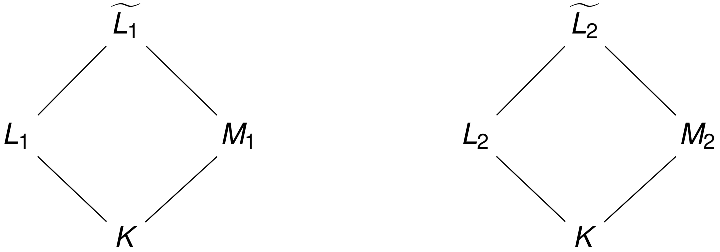


Let L_1/K, L_2/K be a.c.G. extensions.



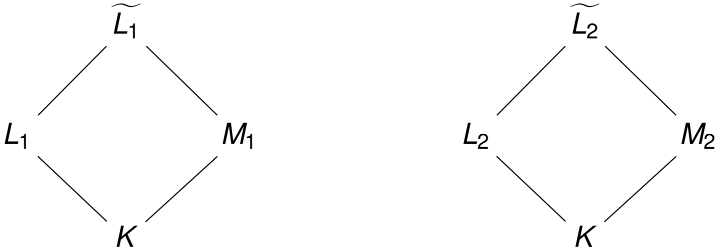
Is $L = L_1L_2$ an a.c.G. extension?

Let L_1/K, L_2/K be a.c.G. extensions.



Is $L = L_1L_2$ an a.c.G. extension?
It is easy to see that $\widetilde{L} = \widetilde{L_1}\widetilde{L_2}$.

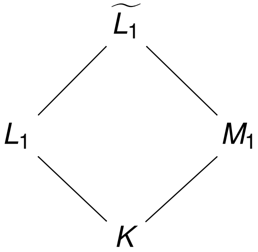
Let L_1/K, L_2/K be a.c.G. extensions.

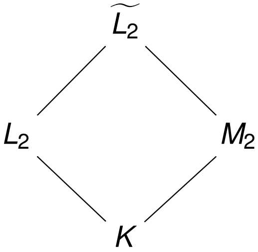


Is $L = L_1 L_2$ an a.c.G. extension?
It is easy to see that $\widetilde{L} = \widetilde{L_1}\widetilde{L_2}$.

We need to assume that L_1 and L_2 are K-linearly disjoint.

Let L_1/K, L_2/K be a.c.G. extensions.





Is $L = L_1L_2$ an a.c.G. extension?
It is easy to see that $\widetilde{L} = \widetilde{L_1}\widetilde{L_2}$.

We need to assume that L_1 and L_2 are K-linearly disjoint.

This is the condition that the epimorphism

$$L_1 \otimes_K L_2 \longrightarrow L_1L_2$$

is an isomorphism.

Definition

Two linearly disjoint a.c.G. extensions L_1/K, L_2/K with complements M_1, M_2 are said to be ***strongly disjoint*** *if*

$$L_1 \cap M_2 = L_2 \cap M_1 = K.$$

Definition

Two linearly disjoint a.c.G. extensions L_1/K, L_2/K with complements M_1, M_2 are said to be ***strongly disjoint*** *if*

$$L_1 \cap M_2 = L_2 \cap M_1 = K.$$

Proposition

If L_1/K and L_2/K are strongly disjoint a.c.G. extensions with complements M_1, M_2, then $L = L_1 L_2$ is an a.c.G. extension of K with complement $M = M_1 M_2$.

Definition

Two linearly disjoint a.c.G. extensions L_1/K, L_2/K with complements M_1, M_2 are said to be ***strongly disjoint*** *if*

$$L_1 \cap M_2 = L_2 \cap M_1 = K.$$

Proposition

If L_1/K and L_2/K are strongly disjoint a.c.G. extensions with complements M_1, M_2, then $L = L_1L_2$ is an a.c.G. extension of K with complement $M = M_1M_2$.

$$\begin{aligned} L \otimes_K M &= (L_1 \otimes_K M_1)(L_1 \otimes_K M_2)(L_2 \otimes_K M_1)(L_2 \otimes_K M_2) \\ &\cong \widetilde{L}(L_1 \otimes_K M_2)(L_2 \otimes_K M_1) \end{aligned}$$

Definition

*Two linearly disjoint a.c.G. extensions L_1/K, L_2/K with complements M_1, M_2 are said to be **strongly disjoint** if*

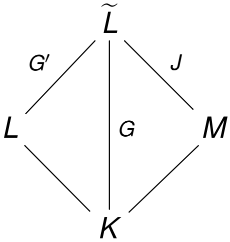
$$L_1 \cap M_2 = L_2 \cap M_1 = K.$$

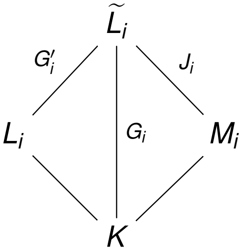
Proposition

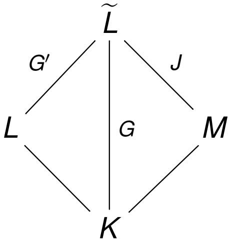
If L_1/K and L_2/K are strongly disjoint a.c.G. extensions with complements M_1, M_2, then $L = L_1 L_2$ is an a.c.G. extension of K with complement $M = M_1 M_2$.

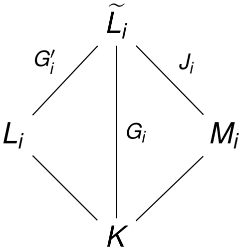
$$\begin{aligned} L \otimes_K M &= (L_1 \otimes_K M_1)(L_1 \otimes_K M_2)(L_2 \otimes_K M_1)(L_2 \otimes_K M_2) \\ &\cong \widetilde{L}(L_1 \otimes_K M_2)(L_2 \otimes_K M_1) \end{aligned}$$

Since $M_1, M_2/K$ are Galois, strong disjointness gives $L_i \otimes_K M_j \hookrightarrow \widetilde{L}$.


$\widetilde{L}$
G'
J
L
G
M
K


$\widetilde{L}_i$
G'_i
J_i
L_i
G_i
M_i
K

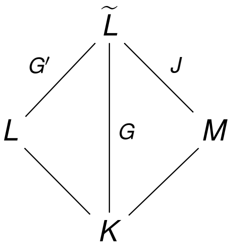


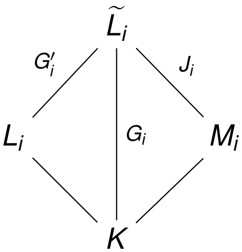


There is an embedding $G \hookrightarrow G_1 \times G_2$, by which

$$G' \hookrightarrow G'_1 \times G'_2, \quad J \hookrightarrow J_1 \times J_2.$$

Since L_1/K and L_2/K are linearly disjoint, $J \cong J_1 \times J_2$.



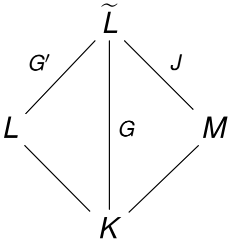


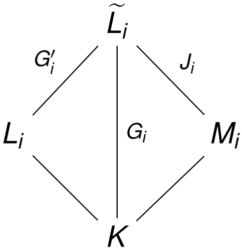
There is an embedding $G \hookrightarrow G_1 \times G_2$, by which

$$G' \hookrightarrow G_1' \times G_2', \quad J \hookrightarrow J_1 \times J_2.$$

Since L_1/K and L_2/K are linearly disjoint, $J \cong J_1 \times J_2$.

Hopf-Galois structures on L/K: Regular subgroups of $\mathrm{Perm}(G/G')$ normalized by $\lambda \colon G \longrightarrow \mathrm{Perm}(G/G')$.





There is an embedding $G \hookrightarrow G_1 \times G_2$, by which

$$G' \hookrightarrow G_1' \times G_2', \quad J \hookrightarrow J_1 \times J_2.$$

Since L_1/K and L_2/K are linearly disjoint, $J \cong J_1 \times J_2$.

Hopf-Galois structures on L/K: Regular subgroups of $\mathrm{Perm}(G/G')$ normalized by $\lambda\colon G \longrightarrow \mathrm{Perm}(G/G')$.

Hopf-Galois structures on L_i/K: Regular subgroups of $\mathrm{Perm}(G_i/G_i')$ normalized by $\lambda_i\colon G_i \longrightarrow \mathrm{Perm}(G_i/G_i')$.

Strategy: To factorize λ through $\mathrm{Perm}(G_1/G_1') \times \mathrm{Perm}(G_2/G_2')$.

Strategy: To factorize λ through $\mathrm{Perm}(G_1/G_1') \times \mathrm{Perm}(G_2/G_2')$.

$$\begin{array}{cccccc} G & \longrightarrow & \mathrm{Perm}(G_1/G_1') \times \mathrm{Perm}(G_2/G_2') & \longrightarrow & \mathrm{Perm}(G/G') \\ g & \longmapsto & (\lambda_1(g_1), \lambda_2(g_2)) & & \\ & & (\varphi_1, \varphi_2) & \longmapsto & ? \end{array}$$

Strategy: To factorize λ through $\mathrm{Perm}(G_1/G_1') \times \mathrm{Perm}(G_2/G_2')$.

$$\begin{array}{ccccc} G & \longrightarrow & \mathrm{Perm}(G_1/G_1') \times \mathrm{Perm}(G_2/G_2') & \longrightarrow & \mathrm{Perm}(G/G') \\ g & \longmapsto & (\lambda_1(g_1), \lambda_2(g_2)) & & \\ & & (\varphi_1, \varphi_2) & \longmapsto & ? \end{array}$$

Lemma

There is a bijection

$$\begin{array}{rccc} \psi \colon & G/G' & \longrightarrow & G_1/G_1' \times G_2/G_2' \\ & g_1 g_2 G' & \longmapsto & (g_1 G_1', g_2 G_2') \end{array}$$

Strategy: To factorize λ through $\mathrm{Perm}(G_1/G_1') \times \mathrm{Perm}(G_2/G_2')$.

$$\begin{array}{ccccc} G & \longrightarrow & \mathrm{Perm}(G_1/G_1') \times \mathrm{Perm}(G_2/G_2') & \longrightarrow & \mathrm{Perm}(G/G') \\ g & \longmapsto & (\lambda_1(g_1), \lambda_2(g_2)) & & \\ & & (\varphi_1, \varphi_2) & \longmapsto & ? \end{array}$$

Lemma

There is a bijection

$$\begin{array}{cccc} \psi\colon & G/G' & \longrightarrow & G_1/G_1' \times G_2/G_2' \\ & g_1 g_2 G' & \longmapsto & (g_1 G_1', g_2 G_2') \end{array}$$

Then there is a well defined map

$$\iota\colon \mathrm{Perm}(G_1/G_1') \times \mathrm{Perm}(G_2/G_2') \longrightarrow \mathrm{Perm}(G/G').$$

It is easy to check that ι is a monomorphism.

Proposition

If N_i is a regular subgroup of $\mathrm{Perm}(G_i/G_i')$ normalized by $\lambda_i(G_i)$ for every $i \in \{1,2\}$, then $N = \iota(N_1 \times N_2)$ is a regular subgroup of $\mathrm{Perm}(G/G')$ normalized by $\lambda(G)$.

Proposition

If N_i is a regular subgroup of $\mathrm{Perm}(G_i/G_i')$ normalized by $\lambda_i(G_i)$ for every $i \in \{1,2\}$, then $N = \iota(N_1 \times N_2)$ is a regular subgroup of $\mathrm{Perm}(G/G')$ normalized by $\lambda(G)$.

Definition

Let $H_i = \widetilde{L_i}[N_i]^{G_i}$ be a Hopf-Galois structure on L_i/K, $i \in \{1,2\}$. The Hopf-Galois structure $H = \widetilde{L}[N]^G$ on L/K will be called the ***product Hopf-Galois structure*** *of H_1 and H_2.*

The name of this new object is justified by the following.

The name of this new object is justified by the following.

Proposition

Let H be the product Hopf-Galois structure of H_1 and H_2. Then:

1. $H \cong H_1 \otimes_K H_2$ *as* K*-algebras.*
2. *If* $h_i \in H_i$ *and* $\alpha_i \in L_i$ *for* $i \in \{1, 2\}$, *then*

$$(h_1 h_2) \cdot (\alpha_1 \alpha_2) = (h_1 \cdot \alpha_1)(h_2 \cdot \alpha_2).$$

The name of this new object is justified by the following.

Proposition

Let H be the product Hopf-Galois structure of H_1 and H_2. Then:

1. $H \cong H_1 \otimes_K H_2$ *as* K*-algebras.*
2. *If* $h_i \in H_i$ *and* $\alpha_i \in L_i$ *for* $i \in \{1, 2\}$*, then*

$$(h_1 h_2) \cdot (\alpha_1 \alpha_2) = (h_1 \cdot \alpha_1)(h_2 \cdot \alpha_2).$$

Let $\rho_{H_i} \colon H_i \longrightarrow \mathrm{End}_K(L_i)$ and $\rho_H \colon H \longrightarrow \mathrm{End}_K(L)$ be the actions of H_i on L_i for $i \in \{1, 2\}$ and of H on L, respectively. Then

$$\rho_H = \rho_{H_1} \otimes_K \rho_{H_2}.$$

Let H be the product Hopf-Galois structure of H_1 and H_2.

Let H be the product Hopf-Galois structure of H_1 and H_2.

Proposition

If α_i is an H_i-eigenvector for $i \in \{1, 2\}$, then $\alpha_1\alpha_2$ is an H-eigenvector.

Let H be the product Hopf-Galois structure of H_1 and H_2.

Proposition

If α_i is an H_i-eigenvector for $i \in \{1,2\}$, then $\alpha_1\alpha_2$ is an H-eigenvector.

Proposition

Let M_i be the complement of L_i/K and let $M = M_1M_2$. If H_i is the a.c.G. structure on L_i/K corresponding to M_i, then H is the a.c.G. structure on L/K corresponding to M.

We will call an extension strongly decomposable if it is a compositum of strongly disjoint extensions.

We will call an extension strongly decomposable if it is a compositum of strongly disjoint extensions.

Theorem

Let L/K be a strongly decomposable H-Galois extension. The following statements are equivalent:

- $L \cap K(\zeta_n) = K$ *and* L/K *is radical.*
- L/K *is an a.c.G. extension with complement* $K(\zeta_n)$ *and* L/K *is* H*-Kummer, where* H *is the a.c.G. extension on* L/K *corresponding to* $K(\zeta_n)$*.*

We will call an extension strongly decomposable if it is a compositum of strongly disjoint extensions.

Theorem

Let L/K be a strongly decomposable H-Galois extension. The following statements are equivalent:

- *$L \cap K(\zeta_n) = K$ and L/K is radical.*
- *L/K is an a.c.G. extension with complement $K(\zeta_n)$ and L/K is H-Kummer, where H is the a.c.G. extension on L/K corresponding to $K(\zeta_n)$.*

If $L = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k})$ is such an extension, a finite generating set of H-eigenvectors is $\{\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_k}\}$.

Table of contents

Let L/K be an H-Galois extension of number or p-adic fields.

Let L/K be an H-Galois extension of number or p-adic fields.

$$\begin{array}{ccc} L & \text{———} & \mathcal{O}_L \\ H \Big| & & \Big| \\ K & \text{———} & \mathcal{O}_K \end{array}$$

Let L/K be an H-Galois extension of number or p-adic fields.

$$\begin{array}{ccc} L & \text{———} & \mathcal{O}_L \\ {\scriptstyle H}\Big| & & \Big| \\ K & \text{———} & \mathcal{O}_K \end{array}$$

Associated order of $\mathcal{O}_L$ in H:
$\mathfrak{A}_H = \{h \in H \mid h \cdot \mathcal{O}_L \subset \mathcal{O}_L\}$.

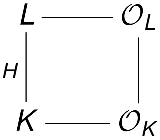
Let L/K be an H-Galois extension of number or p-adic fields.

$$\begin{array}{ccc} L & \text{——} & \mathcal{O}_L \\ H \Big| & & \Big| \\ K & \text{——} & \mathcal{O}_K \end{array}$$

Associated order of $\mathcal{O}_L$ in H:
$\mathfrak{A}_H = \{h \in H \mid h \cdot \mathcal{O}_L \subset \mathcal{O}_L\}$.

Is $\mathcal{O}_L$ free as $\mathfrak{A}_H$-module?

Let L/K be an H-Galois extension of number or p-adic fields.



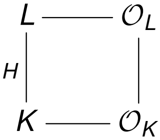
Associated order of $\mathcal{O}_L$ in H:
$\mathfrak{A}_H = \{h \in H \mid h \cdot \mathcal{O}_L \subset \mathcal{O}_L\}$.

Is $\mathcal{O}_L$ free as $\mathfrak{A}_H$-module?

Theorem

Assume that there is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$ which in addition is a K-basis of H-eigenvectors for L. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.

Let L/K be an H-Galois extension of number or p-adic fields.



Associated order of $\mathcal{O}_L$ in H:
$\mathfrak{A}_H = \{h \in H \mid h \cdot \mathcal{O}_L \subset \mathcal{O}_L\}$.

Is $\mathcal{O}_L$ free as $\mathfrak{A}_H$-module?

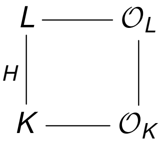
Theorem

Assume that there is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$ which in addition is a K-basis of H-eigenvectors for L. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.

Example

Let $L = \mathbb{Q}(\omega)$, $\omega = \sqrt[3]{2}$. We have seen that $\{1, \omega, \omega^2\}$ are H-eigenvectors of L.

Let L/K be an H-Galois extension of number or p-adic fields.



Associated order of $\mathcal{O}_L$ in H:
$\mathfrak{A}_H = \{h \in H \mid h \cdot \mathcal{O}_L \subset \mathcal{O}_L\}$.

Is $\mathcal{O}_L$ free as $\mathfrak{A}_H$-module?

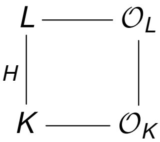
Theorem

Assume that there is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$ which in addition is a K-basis of H-eigenvectors for L. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.

Example

Let $L = \mathbb{Q}(\omega)$, $\omega = \sqrt[3]{2}$. We have seen that $\{1, \omega, \omega^2\}$ are H-eigenvectors of L. In addition, it is an integral basis of L.

Let L/K be an H-Galois extension of number or p-adic fields.



Associated order of $\mathcal{O}_L$ in H:
$\mathfrak{A}_H = \{h \in H \mid h \cdot \mathcal{O}_L \subset \mathcal{O}_L\}$.

Is $\mathcal{O}_L$ free as $\mathfrak{A}_H$-module?

Theorem

Assume that there is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$ which in addition is a K-basis of H-eigenvectors for L. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.

Example

Let $L = \mathbb{Q}(\omega)$, $\omega = \sqrt[3]{2}$. We have seen that $\{1, \omega, \omega^2\}$ are H-eigenvectors of L. In addition, it is an integral basis of L. Then, $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.

Proposition

Let $L = K(\sqrt[n]{a})$ be a simple radical extension such that $L \cap K(\zeta_n) = K$ and $\mathcal{O}_L = \mathcal{O}_K[\sqrt[n]{a}]$. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free, where H is the a.c.G. structure corresponding to $K(\zeta_n)$.

Proposition

Let $L = K(\sqrt[n]{a})$ be a simple radical extension such that $L \cap K(\zeta_n) = K$ and $\mathcal{O}_L = \mathcal{O}_K[\sqrt[n]{a}]$. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free, where H is the a.c.G. structure corresponding to $K(\zeta_n)$.

If $K = \mathbb{Q}$, a sufficient condition is that $a^p \not\equiv a \pmod{p^2}$ for every prime $p \mid n$ (Gassert).

Proposition

Let $L = K(\sqrt[n]{a})$ be a simple radical extension such that $L \cap K(\zeta_n) = K$ and $\mathcal{O}_L = \mathcal{O}_K[\sqrt[n]{a}]$. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free, where H is the a.c.G. structure corresponding to $K(\zeta_n)$.

If $K = \mathbb{Q}$, a sufficient condition is that $a^p \not\equiv a \pmod{p^2}$ for every prime $p \mid n$ (Gassert).

Corollary

Let $L = \mathbb{Q}(\sqrt[n]{a})$ be such that $L \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ and $a^p \not\equiv a \pmod{p^2}$ for every prime divisor p of n. Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.

Module structure over the product Hopf-Galois structure:

Module structure over the product Hopf-Galois structure:

Proposition

Let L_1/K and L_2/K be strongly and arithmetically disjoint a.c.G. extensions. Let H be the product Hopf-Galois structure on L/K from Hopf-Galois structures H_i on L_i/K.
If $\mathcal{O}_{L_i}$ is $\mathfrak{A}_{H_i}$-free for all $i \in \{1,2\}$, then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.

Module structure over the product Hopf-Galois structure:

Proposition

Let L_1/K and L_2/K be strongly and arithmetically disjoint a.c.G. extensions. Let H be the product Hopf-Galois structure on L/K from Hopf-Galois structures H_i on L_i/K.
If $\mathcal{O}_{L_i}$ is $\mathfrak{A}_{H_i}$-free for all $i \in \{1,2\}$, then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.

Proposition

Let $L = K(\sqrt[n_1]{a_1}, \dots, \sqrt[n_k]{a_k})$ and call $L_i = K(\sqrt[n_i]{a_i})$. Assume:

- *$L_i \cap K(\zeta_{n_i}) = K$ for every $1 \leq i \leq k$.*
- *L_i/K and L_j/K are strongly and arithmetically disjoint.*
- *$\mathcal{O}_{L_i} = \mathcal{O}_K[\sqrt[n_i]{a_i}]$ for every $1 \leq i \leq k$.*

Then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.

L.N. Childs; *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory,* Mathematical Surveys and Monographs 80, American Mathematical Society, 2000.

T. A. Gassert; *A note on the monogenity of power maps*, Albanian Journal of Mathematics **11** (2017), 3-12.

D. Gil-Muñoz; *A generalization of Kummer theory to Hopf-Galois extensions*, Preprint (2023).

C. Greither, B. Pareigis; *Hopf-Galois theory for separable field extensions*, Journal of Algebra **106** (1987), 239-258.

Thank you for your attention