Greither-Pareigis theory, through the lens of algebraic geometry

Alan Koch

Agnes Scott College

May 21, 2018

Outline

Overview

Let L/K be a separable extension of fields, normal closure E.

1986. Greither and Pareigis showed how one can classify/construct Hopf-Galois structures on L/K.

Let $G = \mathrm{Gal}(E/K),\ G' = \mathrm{Gal}(E/L)$. Then one can classify Hopf-Galois structures by finding all regular subgroups $N \leq \mathrm{Perm}(G/G')$ normalized by the action of conjugation by $\lambda(G) \leq \mathrm{Perm}(G/G')$, where $\lambda(g)(xG') = (gx)G'$.

The beauty of their work is that it is entirely group theoretic.

Isomorphism Problems: Motivation I

Given $N \leq \mathrm{Perm}(G/G')$, the Hopf algebra is $E[N]^G$, where G acts on E via Galois action and on N by $\lambda(G)$.

Suppose N_1, N_2 give Hopf-Galois structures.

- Under what conditions are the two Hopf algebras isomorphic?
  TARP has a very satisfying answer.

- Under what conditions are the two Hopf algebras isomorphic as K-algebras?
  In general, much harder.
  Results are known in certain cases, e.g., N abelian.

Purely Inseparable Analogue: Motivation II

At this conference...

Childs, 2013: Is there a Greither-Pareigis theory for purely inseparable extensions?

K., 2014: No.

There exist purely inseparable extensions with an infinite number of Hopf-Galois structures.

K., 2018: Maybe.

It is possible that the theory which begat Greither-Pareigis can generate a similar, but different, purely inseparable theory as well.

Using simple algebraic geometry.

Outline

An *affine scheme* (over K) is a representable functor $\mathcal{X}$ from K-algebras to sets.

There exists a (commutative) K-algebra A such that $\mathcal{X}(B) = \mathrm{Alg}_K(A, B)$ for all K-algebras B. We say A *represents* $\mathcal{X}$ and write $\mathcal{X} = \mathrm{Spec}(A)$.

The category of affine schemes is anti-equivalent to the category of K-algebras.

Example

$A = \mathbb{Q}[x]/(x^3 + x)$, $\mathcal{X} = \mathrm{Spec}(A)$

$$\mathcal{X}(B) = \mathrm{Alg}_{\mathbb{Q}}(\mathbb{Q}[x]/(x^3 + x), B) \leftrightarrow \{b \in B : b^3 + b = 0\}.$$

So, e.g., $\mathcal{X}(\mathbb{Q}) = \{0\}$, $\mathcal{X}(\mathbb{Q}(i)) = \{0, i, -i\}$, and $\mathcal{X}(\mathbb{C}^2) = \{(0,0),(0,i),(0,-i),(i,0),(i,i),(i,-i),(-i,0),(-i,i),(-i,-i)\}$.

An *affine group scheme* (over K) is a representable functor $\mathcal{G}$ from K-algebras to groups.

If $\mathcal{G} = \mathrm{Spec}(H)$ then H is a K-Hopf algebra whose coalgebra structure provides the group operation.

$f, g \in \mathcal{G}(B) = \mathrm{Alg}_K(H, B) \Rightarrow (f *_{\mathcal{G}} g)(h) = \mathrm{mult}(f \otimes g)\Delta(h),\ h \in H.$

Example

$\mathcal{G} = \mathrm{Spec}(H),\ H = \mathbb{Q}[x]/(x^3 - 1),\ \Delta(x) = x \otimes x.$

$$\mathcal{G}(B) = \mathrm{Alg}_{\mathbb{Q}}(\mathbb{Q}[x]/(x^3 - 1), B) \leftrightarrow \{b \in B : b^3 - 1 = 0\}.$$

If $f(x) = a,\ g(x) = b,\ a, b \in B$ then

$$(f *_{\mathcal{G}} g)(x) = \mathrm{mult}(f \otimes g)\Delta(x) = f(x)g(x) = ab.$$

Thus the group operation is the usual multiplication in B.

Group Scheme Actions

We say a group scheme $\mathcal{G}$ *acts* on a scheme $\mathcal{X}$ if there is a morphism of schemes

$$\mathcal{G} \times \mathcal{X} \to \mathcal{X}.$$

That is, for each K-algebra B there is a group action

$$\mathcal{G}(B) \times \mathcal{X}(B) \to \mathcal{X}(B),\ (g, x) \mapsto g * x.$$

If $\mathcal{G} = \mathsf{Spec}(H)$ and $\mathcal{X} = \mathsf{Spec}(A)$ this corresponds to a K-algebra map

$$A \to A \otimes_K H$$

which provides an H-comodule structure on A.

A Small Example of Everything

Let $K = \mathbb{Q}$.

Let $\mathcal{G} = \text{Spec}(\mathbb{Q}[t]/(t^3 + 3t)),\ \Delta(t) = t \otimes 1 + 1 \otimes t + \frac{1}{2}t^2 \otimes t + \frac{1}{2}t \otimes t^2$.

Then, for a $\mathbb{Q}$-algebra B, $\mathcal{G}(B) = \{b \in B : b^3 + 3b = 0\}$ and

$$a +_{\mathcal{G}} b = a + b + \frac{1}{2}a^2 b + \frac{1}{2}ab^2.$$

Let $\mathcal{X} = \text{Spec}(\mathbb{Q}(\sqrt[3]{2}))$.

Then $\mathcal{G}$ acts on $\mathcal{X}$ via

$$g * x = x + \frac{1}{2}gx + \frac{1}{2}g^2 x,\ g \in \mathcal{G}(B), x \in \mathcal{X}(B)$$

after identifying $\mathcal{G}(B), \mathcal{X}(B)$ as subsets of B.

Example

Let $B = \mathbb{Q}(\sqrt[3]{2})$. Then

$$\mathcal{G}(B) = \{b \in \mathbb{Q}(B) : b^3 + 3b = 0\} = \{0\}$$
$$\mathcal{X}(B) = \mathrm{Alg}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), B) = \{1\}$$

and the action is trivial.

$\mathcal{G} = \text{Spec}(\mathbb{Q}[t]/(t^3+3t)), \mathcal{X} = \text{Spec}(\mathbb{Q}(\sqrt[3]{2}))$

$$g +_{\mathcal{G}} h = g + h + \frac{1}{2}g^2h + \frac{1}{2}gh^2, \; g * x = x + \frac{1}{2}gx + \frac{1}{2}g^2x$$

Example

Let E be the splitting field of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$.

$$\mathcal{G}(E) = \{0, i\sqrt{3}, -i\sqrt{3}\}$$
$$\mathcal{X}(E) = \text{Alg}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), E) \leftrightarrow \{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\}$$

where $\zeta \in E$ is a primitive cube root of unity. Then, e.g.,

$$i\sqrt{3} * \sqrt[3]{2} = \sqrt[3]{2} + \frac{1}{2}(i\sqrt{3})(\sqrt[3]{2}) + \frac{1}{2}(i\sqrt{3})^2(\sqrt[3]{2})$$
$$= \sqrt[3]{2}\left(\frac{-1 - i\sqrt{3}}{2}\right) = \zeta^2\sqrt[3]{2}.$$

Principal Homogeneous Space

Suppose $\mathcal{G}$ acts on $\mathcal{X}$. We say $\mathcal{X}$ is a *principal homogenous space* if $\mathcal{X}(B) \neq \emptyset$ for some B and the map

$$\begin{aligned} \mathcal{G} \times \mathcal{X} &\to \mathcal{X} \times \mathcal{X} \\ (g, x) &\mapsto (g * x, x),\ g \in \mathcal{G}(B),\ x \in \mathcal{X}(B) \end{aligned}$$

is a bijection for all K-algebras B.

If $\mathcal{G} = \mathrm{Spec}(H)$ and $\mathcal{X} = \mathrm{Spec}(A)$ the corresponding isomorphism of K-algebras is the map $A \otimes A \to A \otimes H$ found in the definition of H-Galois object.

The action on the previous example makes $\mathcal{X}$ a *PHS* for $\mathcal{G}$.

$\mathcal{G} \times \mathcal{X} \to \mathcal{X} \times \mathcal{X},\ (g, x) \to (g * x, x)$

Suppose $\mathcal{X}$ is a PHS for $\mathcal{G}$, and $f : \mathcal{G} \times \mathcal{X} \to \mathcal{X} \times \mathcal{X}$ be the bijection above.

Fix a K-algebra B, and write $G = \mathcal{G}(B),\ X = \mathcal{X}(B)$.

f is injective. Suppose $g * x = x$ for some $g \in G, x \in X$. Then $f((g, x)) = (x, x) = f((1_G, x))$, so $g = 1_G$ and the stabilizer of any element of X is trivial.

f is surjective. Pick $x, y \in X$. There exists a $(g, z) \in G \times X$ such that $f((g, z)) = (y, x)$. Clearly, $z = x$ and $g * x = y$. Thus the action of G on X is transitive.

f is bijective. $|G| = {}^{\#}X$.

This looks a lot like Greither-Pareigis theory.

Outline

The Extension

Let K be a field of characteristic 2.

Let $L = K(x)$ where $x^4 = x + 1$ and $[L : K] = 4$.

Then L/K is Galois with $G = \mathrm{Gal}(L/K) = \langle g \rangle \cong C_4,\ g(x) = x^2 + 1$.

$L = K(x),\ x^4 = x+1,\ G = \langle g \rangle$, Regular Subgroup I

Let $N = \rho(G) \leq \mathrm{Perm}(G)$ (here $\rho(g^i)[g^j] = g^{j-i}$ is right regular representation).

Then $H = L[\rho(G)]^G = K[\rho(G)] \cong K[G]$ since $\lambda(g^i)\rho(g^j) = \rho(g^j)\lambda(g^i)$.

Let $\mathcal{N} = \mathrm{Spec}(H^*) = \mathrm{Spec}(K[G]^*),\ \mathcal{X} = \mathrm{Spec}(L)$.

$$\mathcal{N}(L) = \mathrm{Alg}_K(K[N]^*, L) \cong \mathrm{Alg}_L(L[N]^*, L) \cong N \text{ via } (f \mapsto f(\eta)) \leftarrow\!\shortmid \eta$$
$$\mathcal{X}(L) = \mathrm{Alg}_K(L, L) = \mathrm{Gal}(L/K) = G.$$

So N and G arise "organically" as the L-valued points of $\mathcal{N}$ and $\mathcal{X}$ respectively.

L is an H-comodule via:

$$x \mapsto \sum_{k=0}^{3} (\rho(g^k))^{-1}[1_G] \cdot x \otimes \varepsilon_k = \sum_{k=0}^{3} g^k(x) \otimes \varepsilon_k$$

where $\varepsilon_k \in H^*$ is defined by $\varepsilon_k(\rho(g^j)) = \delta_{k,j}$.

The induced action on group schemes is

$$(\rho(g^i) * g^j)(x) = \sum_{k=0}^{3} g^j(g^k(x)) \otimes \varepsilon_k(\rho(g^i)) = g^{j+i}(x),$$

and so $\rho(g^i) * g^j = g^{j+i}$, which differs from the original action of $N \leq \mathrm{Perm}(G)$ on G: $\rho(g^i)[g^j] = g^{j-i}$.

Therefore, $\rho(g^i) * g^j = (\rho(g^i)^{-1})[g^j]$.

$L = K(x),\ x^4 = x + 1,\ G = \langle g \rangle$, Regular Subgroup II

Let

$$\begin{array}{cccc} \eta(1_G) = g & \eta(g) = 1_G & \eta(g^2) = g^3 & \eta(g^3) = g^2 \\ \pi(1_G) = g^2 & \pi(g) = g^3 & \pi(g^2) = 1_G & \pi(g^3) = g \\ \eta\pi(1_G) = g^3 & \eta\pi(g) = g^2 & \eta\pi(g^2) = g & \eta\pi(g^3) = 1_G \end{array}$$

and let $N = \langle \eta, \pi \rangle \leq \mathrm{Perm}(G)$. Then N is regular, and G acts on N via

$$^g\eta = \eta\pi \qquad ^g\pi = \pi \qquad ^g(\eta\pi) = \eta.$$

$\eta = (1\ g)(g^2\ g^3), \pi = (1\ g^2)(g\ g^3),\ \eta\pi = (1\ g^3)(g\ g^2)$

Let $h_0, h_1, h_2, h_3 \in H = L[N]^G$ be given by

$$h_0 = 1 \qquad h_1 = \eta + \eta\pi$$
$$h_2 = \pi \qquad h_3 = (x + x^2) + (1 + x + x^2)\eta\pi.$$

Then H has basis $\{h_0, h_1, h_2, h_3\}$. Furthermore,

$$h_0 \cdot x = x \qquad h_1 \cdot x = 1 \qquad h_2 \cdot x = x + 1 \qquad h_3 \cdot x = x.$$

Let $\varepsilon_i \in H^*, 0 \le i \le 3$ be given by $\varepsilon_i(h_j) = \delta_{i,j}$.

$h_0 = 1, h_1 = \eta + \eta\pi, h_2 = \pi, h_3 = (x + x^2) + (1 + x + x^2)\eta\pi$

Let $\mathcal{N} = \mathrm{Spec}(H^*)$ and $\mathcal{X} = \mathrm{Spec}(L)$. Recall $\mathcal{X}(L) = G$; furthermore,

$$\mathcal{N}(L) = \mathrm{Alg}_K(H^*, L) \cong \mathrm{Alg}_L(L \otimes H^*, L) \cong \mathrm{Alg}_L(L[N]^*, L) \cong N,$$

analogous to the classical case.

The nature of the isomorphism $L \otimes H^* \cong L[N]^*$ (or $L \otimes H \cong L[N]$) is important when considering the group scheme action of $\mathcal{N}$ on $\mathcal{X}$.

$h_0 = 1, h_1 = \eta + \eta\pi, h_2 = \pi, h_3 = (x + x^2) + (1 + x + x^2)\eta\pi$

In $L \otimes H = LH$ we have:

$$\begin{aligned} 1_N &= h_0 \\ \eta &= (1 + x + x^2)h_1 + h_3 \\ \pi &= h_2 \\ \eta\pi &= (x + x^2)h_1 + h_3. \end{aligned}$$

Thus $\varepsilon_i(1_N) = \delta_{i,0},\ \varepsilon_i(\pi) = \delta_{i,2}$, and

$$\varepsilon_i(\eta) = \begin{cases} 0 & i = 0, 2 \\ 1 + x + x^2 & i = 1 \\ 1 & i = 3 \end{cases}, \quad \varepsilon_i(\eta\pi) = \begin{cases} 0 & i = 0, 2 \\ x + x^2 & i = 1 \\ 1 & i = 3 \end{cases}.$$

$\varepsilon_1(\eta) = 1 + x + x^2, \ \varepsilon_3(\eta) = 1, \ \varepsilon_0(\eta) = \varepsilon_2(\eta) = 0$

L is an H-Galois object via

$$\begin{aligned} x \mapsto (h_0 \cdot x) \otimes \varepsilon_0 + (h_1 \cdot x) \otimes \varepsilon_1 + (h_2 \cdot x) \otimes \varepsilon_2 + (h_3 \cdot x) \otimes \varepsilon_3 \\ = x \otimes \varepsilon_0 + 1 \otimes \varepsilon_1 + (x+1) \otimes \varepsilon_2 + x \otimes \varepsilon_3, \end{aligned}$$

and the action of $\mathcal{N}(L)$ on $\mathcal{X}(L)$ satisfies

$$\begin{aligned} (\eta * 1_G)(x) &= x\varepsilon_0(\eta) + \varepsilon_1(\eta) + (x+1)\varepsilon_2(\eta) + x\varepsilon_3(\eta) \\ &= \varepsilon_1(\eta) + x\varepsilon_3(\eta) \\ &= (1 + x + x^2) + x \\ &= x^2 + 1 = g(x). \end{aligned}$$

Thus, $\eta * 1_G = g$. More generally, the action of $\mathcal{N}(L)$ on $\mathcal{X}(L)$ is precisely the same action we find in $N \leq \mathrm{Perm}(G)$.
Since every element of N is self-inverse, this action is consistent with the previous example.

Outline

As before, let L/K be separable, $G = \mathrm{Gal}(E/K),\ G' = \mathrm{Gal}(E/L)$.

Let $N \leq \mathrm{Perm}(G/G')$ regular, normalized by G, and $H = E[N]^G$.

Let $\{h_0, h_1, \dots h_{n-1}\}$ be a K-basis for H, dual basis $\{\varepsilon_0, \dots, \varepsilon_{n-1}\}$.

For each $\eta_j \in N$, write $\eta_j = \sum_{i=0}^{n-1} a_{i,j} h_i,\ a_{i,j} \in E$.

Let $\mathcal{N} = \mathrm{Spec}(H^*),\ \mathcal{X} = \mathrm{Spec}(E)$.

Then $\mathcal{N}(E) = N$ and $\mathcal{X}(E) = G$.

The (regular) action of $\mathcal{N}(E)$ on $\mathcal{X}(E)$ is

$$(\eta * g)(x) = \sum_{i=0}^{n-1} g(h_i \cdot x)\varepsilon_i(\eta) = \sum_{i=0}^{n-1} g(h_i \cdot x) a_{i,j}.$$

Claim. $\eta * g = \eta^{-1}[g]$.

Claim. $\eta * g = \eta^{-1}[g]$.

Keep $\eta_j = \sum_{i=0}^{n-1} a_{i,j} h_i,\ a_{i,j} \in E$, and write $h_i = \sum_{j=0}^{n-1} b_{i,j}\eta_j,\ b_{i,j} \in E$. Let $A = [a_{i,j}],\ B = [b_{i,j}]$. Then $A^T B = I$, so

$$a_{1,j}b_{1,k} + a_{2,j}b_{2,k} + \cdots + a_{n,j}b_{n,k} = \delta_{j,k}.$$

Now for $x \in L$ we have

$$\begin{aligned}
(\eta_j * 1_G)(x) &= \sum_{i=0}^{n-1} (h_i \cdot x)\varepsilon_i(\eta_j) \\
&= \sum_{i=0}^{n-1}\sum_{k=0}^{n-1} b_{i,k}\eta_k^{-1}[1_G](x)\varepsilon_i(\eta_j) \\
&= \left(\sum_{i=0}^{n-1}\sum_{k=0}^{n-1} a_{i,j}b_{i,k}\right)\eta_k^{-1}[1_G](x) \\
&= \eta_j^{-1}[1_G](x).
\end{aligned}$$

Outline

Question

Let $N_1, N_2 \leq \mathrm{Perm}(G/G')$ be regular subgroups normalized by G.

Are $E[N_1]^G \cong E[N_2]^G$ as K-algebras?

We have answers to these types of questions, particularly when N_1, N_2 abelian (esp. cyclic); as well as when $N_1 = \rho(G), N_2 = \lambda(G)$.

Problem. In its full generality, this seems like a fairly difficult problem.

Separable Algebras, char $K = 0$

There exists a way to classify all separable algebras.

Let A be a separable algebra, and let $\mathcal{X} = \mathrm{Spec}(A)$.

Let $X_A = \mathcal{X}(K^{\mathrm{sep}}) = \mathrm{Alg}_K(A, K^{\mathrm{sep}})$, where K^{sep} is the separable closure of K.

Let $\Gamma = \mathrm{Gal}(K^{\mathrm{sep}}/K)$. Then Γ acts on X_A via $({}^{\gamma}f)(a) = \gamma(f(a))$.

Furthermore, this action is continuous (the action factors through finite Galois extensions of K).

There is a one-to-one correspondence

$$\begin{array}{ccc} \{\text{Separable } K\text{-algebras}\} & \leftrightarrow & \{\text{finite sets on which } \Gamma \text{ acts continuously}\} \\ A & \mapsto & X_A \\ F^{\mathrm{Sta}\, x_0} & \leftarrow\!\shortmid & X = \Gamma x_0 \text{ (single orbit case)} \end{array}$$

with F a finite extension of K such that the action of Γ factors through $\mathrm{Gal}(F/K)$.

Given $N \leq \mathrm{Perm}(G)$ as usual, let $H = E[N]^G$.

If N is not abelian, then H may not be a separable K-algebra.

But H^* is separable since H is cocommutative.

Thus, H^* corresponds to a finite Γ-set, namely $\mathcal{N}(K^{\mathrm{sep}})$ where $\mathcal{N} = \mathrm{Spec}(H^*)$ as before.

Note $\mathcal{N}(K^{\mathrm{sep}}) = \mathcal{N}(E) \cong N$, and the action of Γ on $\mathcal{N}(E)$ factors through G.

So N_1, N_2 give isomorphic K-coalgebras (i.e., the dual to their Hopf algebras are isomorphic as K-algebras) if and only if $\mathcal{N}_1$ and $\mathcal{N}_2$ are isomorphic as Γ-sets, or simply as G-sets.

$$\mathcal{N}(E) = \mathrm{Alg}_K(H^*, E) \cong \mathrm{Alg}_E(E \otimes H^*, E) \cong \mathrm{Alg}_E(E[N]^*, E) \cong N$$

Let $N = \{\eta_i\}$. Let $\{h_i\}$ be a K-basis for H, and $\{\varepsilon_i\}$ the dual basis for H^* (as well as $(E \otimes H)^*$).
Under the isomorphism above $\eta \in N$ corresponds to the algebra map $(E \otimes H)^* \to E$ obtained by evaluating at η. Set

$$\eta_j = \sum_{i=0}^{n-1} a_{i,j} h_i, \text{ so } \varepsilon_i(\eta_j) = a_{i,j} \in E.$$

Then $\mathcal{N}(E) = \mathrm{Alg}_K(H^*, E) = \{f_j\}$ where $f_j(\varepsilon_i) = a_{i,j}$.

However,

$$^g\eta_j = {}^g\left(\sum_{i=0}^{n-1} a_{i,j} h_i\right) = \sum_{i=0}^{n-1} g(a_{i,j}) h_i.$$

Thus, if $^g\eta_j = \eta_k$ we have $a_{i,k} = g(a_{i,j})$ for all i.

Then G acts on $\mathcal{N}(E)$ by $(g \cdot f_j)(\varepsilon_i) = g(a_{i,j}) = a_{i,k} = f_k(\varepsilon_i)$, i.e., $g \cdot f_j = f_k$ iff $^g\eta_j = \eta_k$.

And I'm sure that this makes sense.

Outline

Question

Let L/K be purely inseparable, $\mathcal{X} = \text{Spec}(L)$.
Given a PHS $\mathcal{X}$ for $\mathcal{G}$, can we "evaluate" both functors at some field and look for regular subgroups?

Problem. K^{sep} doesn't work.

Example

Let $K = \mathbb{F}_p((T)),\ L = K(x),\ x^p = T$.
Let $\alpha_p = \text{Spec}(H)$, where $H = K[t]/(t^p),\ \Delta(t) = t \otimes 1 + 1 \otimes t$.
Then $\mathcal{X} := \text{Spec}(L)$ is a PHS for α_p via

$$g * x = g + x$$

for $g \in \alpha_p(B) = \{b \in B : b^p = 0\},\ x \in \mathcal{X} = \{b \in B : b^p = T\}$.
But $\alpha(F) = \text{Alg}_K(H, F)$ is trivial for F a field extension of K.

However...

... perhaps $\mathcal{G}$ and $\mathcal{X}$ can be evaluated for some other K-algebra.

Example

Let $K = \mathbb{F}_p((T)),\ L = K(x),\ x^p = T,\ \alpha_p = \text{Spec}(H),\ H = K[t]/(t^p)$. Let

$$B = L[y]/(y^p) = K[x,y]/(x^p - T, y^p).$$

$$\alpha_p(B) = \{b \in B : b^p = 0\} = yB \text{ (group under } +_B)$$
$$\mathcal{X}(B) = \{b \in B : b^p = T\} = x + yB$$

The action is addition in B, and one can view yB as a regular subgroup of $\text{Perm}(x + yB)$.

Let L/K be a finite normal modular extension of exponent e.

Let $B = L[y]/(y^{p^e+1})$.

The *Heerema-Galois group* is defined to be

$$HG(L/K) = \mathrm{Aut}_{K[y]}(L[y]).$$

Battiston (Proc. AMS, 2017) gives a theory of Galois descent for finite inseparable extensions using $HG(L/K)$.

Perhaps $L[y]/(y^{p^e+1})$ (or $L[y]/(y^{p^e})$) is a useful analogue for K^{sep}.

Thank you.