THE GROUP OF GALOIS EXTENSIONS OVER ORDERS IN $KC_{p^2}$

ROBERT UNDERWOOD

Abstract. In this paper we characterize all Galois extensions over $H$ where $H$ is an arbitrary $R$-Hopf order in $KC_{p^2}$. We conclude that the abelian group of $H$-Galois extensions is isomorphic to a certain quotient of units groups in $R \times R$. This result generalizes the classification of $H$-Galois extensions, where $H \subset KC_p$, due to Roberts, and also to Hurley and Greither.

Introduction

Let $K$ be a finite extension of the $p$-adic rationals $\mathbb{Q}_p$ endowed with the $p$-adic valuation $\nu$ with $\nu(p) = 1$. Let $R$ be the integral closure of $\mathbb{Z}_p$ in $K$ and let $H$ be an arbitrary $R$-Hopf algebra order in $KC_{p^2}$. We assume that $R$ contains $\zeta$, a primitive $p^2$nd root of unity; thus the linear dual $H^* = Hom_R(H, R)$ is an $R$-Hopf algebra order in $KC_{p^2}$. In this paper we characterize all Galois extensions over $H$, and hence, all Galois algebras over $H^*$. We conclude that the abelian group of $H$-Galois extensions is isomorphic to a certain quotient of units groups in $R \times R$. This result generalizes the classification of $H$-Galois extensions, where $H \subset KC_p$, due to Roberts [R, Thm. 1], and also found in [H, Thm 4.9] and [G, Prop. II.2.1].

1. Definitions and preliminaries

Let $C_{p^2}$ denote the cyclic group of order $p^2$ with generator $g$. Then the group ring $KC_{p^2}$ can be endowed with the structure of a $K$-Hopf algebra, with $\Delta$, $\epsilon$, and $\sigma$ denoting the co-multiplication, co-unit, and antipode maps. An $R$-Hopf algebra order in $KC_{p^2}$ is an $R$-Hopf algebra $H$ which is a finitely generated projective $R$ module satisfying

$H \otimes_R K \cong KC_{p^2}$

as $K$-Hopf algebras. Note that as a finitely generated module over a local ring $R$, a Hopf algebra order in $KC_{p^2}$ is free over $R$ of rank $p^2$.

The structure of $R$-Hopf algebra orders in $KC_{p^2}$ has been determined by C. Greither in [G, Cor. 3.6], and this author in [U2, Main Theorem]. For an arbitrary $R$-Hopf algebra order $H$ in $KC_{p^2}$, we have that

$H = A_v(s, r) = R \left[ \frac{g^p - 1}{x_s}, \frac{g - a_v}{x_r} \right], \quad \langle g \rangle = C_{p^2}$.
Here \( x_s, x_r \) denote elements in \( R \) of value \( s, r \) respectively. The quantity \( a_v \) is an element in \( R \left[ \frac{g^{p-1}}{x_s} \right] \) of the form \( a_v = \sum_{i=0}^{p-1} v^i e_i \), where \( v \) is a certain unit in \( R \) and the \( e_i \) are the idempotents for the maximal integral order in \( KC_p \) \( \left( \text{for details see [G, Cor. 3.6], [U2, §1.2], [U3, §3.1]} \right) \). Moreover, it is not difficult to show that the algebra generator \( \frac{g^{p-1}}{x_s} \) is a root of the monic polynomial

\[
p(X) = x_{-ps}(1 + x_sX)^p - 1
\]

of degree \( p \) with coefficients in \( R \), and that the generator \( \frac{g - a_v}{x_r} \) is a root of the monic polynomial

\[
q(Y) = x_{-pr} \left( (a_v + x_rY)^p - g^p \right)
\]

of degree \( p \) with coefficients in \( R \left[ \frac{g^{p-1}}{x_s} \right] \). Hence an \( R \) basis for \( H \) consists of

\[
\left\{ \left( \frac{g^{p-1}}{x_s} \right)^i \left( \frac{g - a_v}{x_r} \right)^j \right\},
\]

for \( i, j = 0, \ldots, p - 1 \).

For \( \nu(1 - v) \) sufficiently large we can assume that \( v = 1 \); thus \( a_v = 1 \). In this case the \( R \)-Hopf order \( A_1(s, r) \) can be written as the Larson order

\[
H(s, r) = R \left[ \frac{g^{p-1}}{x_s}, \frac{g - 1}{x_r} \right].
\]

Necessarily, we must have \( pr \leq s \) \( \left( \text{cf. [U2, §1.2]} \right) \). As before, the algebra generator \( \frac{g^{p-1}}{x_s} \) is a root of the monic polynomial

\[
p(X) = x_{-ps}(1 + x_sX)^p - 1
\]

of degree \( p \) with coefficients in \( R \), and the generator \( \frac{g - 1}{x_r} \) is a root of the monic polynomial

\[
q(Y) = x_{-pr} (1 + x_rY)^p - g^p
\]

of degree \( p \) with coefficients in \( R \left[ \frac{g^{p-1}}{x_s} \right] \). It follows that an \( R \) basis for the Larson order \( H(s, r) \) consists of

\[
\left\{ \left( \frac{g^{p-1}}{x_s} \right)^i \left( \frac{g - 1}{x_r} \right)^j \right\},
\]

for \( i, j = 0, \ldots, p - 1 \).

Let \( H = A_v(s, r) \) be an arbitrary order in \( KC_p^2 \). Since we supposed that \( \zeta \in R \), the linear dual \( H^* = Hom_R(H, R) \) inherits the structure of a Hopf algebra order in \( KC_p^2 \) of the form

\[
H^* = A_{v'}(r', s') \cong R \left[ \frac{g^{p-1}}{x_{r'}}, \frac{g - a_{v'}}{x_{s'}} \right]
\]

where \( r' = \frac{1}{p} r, s' = \frac{1}{p} s - s \), and \( v' = 1 + \zeta - v \) \( \left( \text{cf. [G, Remark 3.12], [U3, Thm 3.1.0]} \right) \). We note that for the dual pair \( A_v(s, r) \) and \( A_{v'}(r', s') \) we have either \( pr \leq s \) or \( ps' \leq r' \) \( \left( \text{cf. [U2, Thms. 2.4, 2.5]} \right) \).
In general, an arbitrary order in $KC_{p^2}$ is either a Larson order $H(s, r)$, or a non-Larson order of the form $A_v(s, r)$.

Again, let $H$ denote an arbitrary $R$-Hopf order in $KC_{p^2}$.

**Definition 1.0.** An $H$-Galois extension of $R$ is a finitely generated projective $R$-algebra $S$ together with an $R$-algebra map $$\alpha : S \to S \otimes H$$ satisfying the conditions $$\alpha \otimes 1 \alpha = (1 \otimes \Delta) \alpha,$$ $$1 \otimes \epsilon \alpha = \text{Id}_S,$$ with the map $$\gamma : S \otimes S \to S \otimes H,$$ given by $$\gamma(s \otimes t) = \sum_{(t)} st(1) \otimes t(2)$$ an isomorphism. Here we employ the Sweedler-like notation $$\alpha(t) = \sum_{(t)} t(1) \otimes t(2),$$ where $t(1) \in S$, $t(2) \in H$.

**Definition 1.1.** A finitely generated projective $R$-algebra $S$ is an $H$-Galois algebra if there exists an $H$-module map $$\beta : H \otimes S \to S,$$ satisfying $$\beta(h \otimes 1) = \epsilon(h),$$ $$\beta(h \otimes xy) = \sum_{(h)} \beta(h(1) \otimes x) \cdot \beta(h(2) \otimes y),$$ with the map $$H \otimes S \to \text{End}_R(S), \ h \otimes x \mapsto (y \mapsto x \cdot \beta(h \otimes y)),$$ an isomorphism.

We note that $S$ is an $H$-Galois extension if and only if $S$ is an $H^*$-Galois algebra (cf. [C, §1]).

Our goal in this paper is to characterize all $H$-Galois extensions $S$, where $H$ is an arbitrary $R$-Hopf algebra order in $KC_{p^2}$. Note that S. Hurley, [H], C. Greither, [G], and L. Roberts [R] all provide classifications of $H$-Galois extensions when $H$ is an arbitrary “Tate-Oort” order in $KC_p$. Our methods here generalize those of [G] and [R]. We realize that every $R$-Hopf order $H$ in $KC_{p^2}$ will give rise to a finite group scheme $Sp_R H = \text{Hom}_{R-alg}(H, )$ of order $p^2$. Moreover, the cohomology group $H^1(R, Sp_R H)$ can be identified with the collection of $H$-Galois extensions, up to $H$-comodule isomorphism. In other parlance, the group $H^1(R, Sp_R H)$ corresponds to isomorphism classes of principal homogeneous spaces for $Sp_R H$ over the base scheme $Sp_R R$, and the affine algebras of these principal homogeneous spaces give rise to our $H$-Galois extensions. (Cf. [G, Intro.] and [M1, Ch.III, § 4].)
Our plan is to calculate $H^1(R, SpR H)$ and then give the algebraic structure of the corresponding $H$-Galois extensions. Our first step is to involve $SpR H$ in a short exact sequence of group schemes. Specializing to the case where $H$ is a Larson order $H(s, r)$, we first resolve $SpH(s, r)$ and then compute $H^1(R, SpH(s, r))$. Next we consider the class of non-Larson orders in $KC_{pr}$, of the form $A_v(s, r)$. We then give a resolution of $SpA_v(s, r)$, and compute $H^1(R, SpA_v(s, r))$.

2. A resolution of $SpR(H(s, r))$

To resolve $SpR(H(s, r))$, we first need to define certain abelian group functors $E_{s, r}$ and $E_{ps, pr}$. We first define $E_{s, r}$. Let $A$ be a commutative $R$-algebra, and let $G_{s, r}(A)$ be the subset of $U(A) \times U(A)$ defined

$$G_{s, r}(A) = \{(u_0, u_1) \in U(A) \times U(A) | u_0 \equiv 1 (mod \ x_s) \ and \ u_1 \equiv 1 (mod \ x_r)\}.$$

Here $a \equiv b (mod \ x_s)$ if and only if $a - b \in x_s A$. One easily checks that $G_{s, r}(A)$ forms a subgroup of $U(A) \times U(A)$ under coordinatewise multiplication. Moreover, for each element $(u_0, u_1) \in G_{s, r}(A)$ there is a pair $(w_{u_0}, w_{u_1}) \in A \times A$ with $u_0 = 1 + x_s w_{u_0}$ and $u_1 = 1 + x_r w_{u_1}$. With this in mind, we define a subset $E_{s, r}(A)$ of $A \times A$ as follows:

$$E_{s, r}(A) = \{(w_{u_0}, w_{u_1}) \in A \times A | w_{u_0} = \frac{u_0 - 1}{x_s} \ and \ w_{u_1} = \frac{u_1 - 1}{x_r}\},$$

for some $(u_0, u_1) \in G_{s, r}(A)$.

By construction, we have a bijection of sets

$$\rho : E_{s, r}(A) \rightarrow G_{s, r}(A), \quad \rho(w_{u_0}, w_{u_1}) = (u_0, u_1).$$

In fact, we can put a group structure on $E_{s, r}(A)$ so that $\rho$ is an isomorphism of abelian groups. For two elements $(w_{u_0}, w_{u_1}), (w_{v_0}, w_{v_1}) \in A \times A$ we simply define an operation

$$(w_{u_0}, w_{u_1}) * (w_{v_0}, w_{v_1}) = (w_{u_0 v_0}, w_{u_1 v_1}),$$

induced from the group structure of $G_{s, r}(A)$. We realize that $E_{s, r}$ is a group functor from the category of commutative $R$-algebras to the category of abelian groups and is representable by the $R$-Hopf algebra

$$B = R \left[ T_0, T_1, (1 + x_s T_0)^{-1}, (1 + x_r T_1)^{-1} \right],$$

where $T_0, T_1$ are indeterminates. Comultiplication in $B$ is the unique $R$-algebra map $\Delta : B \rightarrow B \otimes B$ which makes the elements $1 + x_s T_0, 1 + x_r T_1$ grouplike.

In a similar manner we define the abelian group functor $E_{ps, pr}$. Let $A$ be any commutative $R$-algebra, and let

$$E_{ps, pr}(A) = \{(w_{u_0}, w_{u_1}) \in A \times A | w_{u_0} = \frac{u_0 - 1}{x_{ps}}, w_{u_1} = \frac{u_1 - 1}{x_{pr}}\},$$

for some $(u_0, u_1) \in G_{ps, pr}(A)$ with

$$G_{ps, pr}(A) = \{(u_0, u_1) \in U(A) \times U(A) | u_0 \equiv 1 (mod \ x_{ps}), u_1 \equiv 1 (mod \ x_{pr})\}.$$

We see that $E_{ps, pr}$ is a group functor from the category of commutative $R$-algebras to the category of abelian groups, and is represented by the $R$-Hopf algebra

$$R \left[ T_0, T_1, (1 + x_{ps} T_0)^{-1}, (1 + x_{pr} T_1)^{-1} \right],$$

with indeterminates $T_0, T_1$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Theorem 2.0. There is an epimorphism of flat sheaves $\Theta : E_{s,r} \to E_{ps,pr}$ whose kernel is the group scheme represented by the $R$-Hopf algebra $H(s,r)$.

Proof. Let $\Theta$ be the morphism on $E_{s,r}$ defined

$$\Theta(A)((w_{u_0}, w_{u_1})) = (p(w_{u_0}), (1 + x_s w_{u_0})^{-1} q(w_{u_0}, w_{u_1})),$$

with

$$p(T_0) = x_{-ps}((1 + x_s T_0)^p - 1),$$

$$q(T_0, T_1) = x_{-pr}((1 + x_r T_1)^p - (1 + x_s T_0)).$$

We first show that for an $R$-algebras $A$,

$$\Theta(A)(E_{s,r}(A)) \subseteq E_{ps,pr}(A).$$

Let $(w_{u_0}, w_{u_1}) \in E_{s,r}(A)$. Then

$$\Theta(A)(w_{u_0}, w_{u_1}) = \Theta(A) \left( \frac{u_0 - 1}{x_s}, \frac{u_1 - 1}{x_r} \right) = \left( \frac{u_0^p - 1}{x_{ps}}, \frac{u_1^p - 1}{x_{pr}} \right).$$

Now since $s \leq \frac{1}{p-1}$ and $pr \leq s$,

$$\frac{u_0 - 1}{x_s} \in A \implies \frac{u_0^p - 1}{x_{ps}} \in A,$$

and

$$\frac{u_1 - 1}{x_r} \in A \implies \frac{u_1^p - 1}{x_{pr}} \in A \implies \frac{u_0^{-1} u_1^p - 1}{x_{pr}} \in A.$$

We next show that $\Theta$ is an epimorphism of $R$-group schemes in the flat topology. For an $R$-algebra $A$, let $(A \to A_i)$ be any flat covering of $A$. (We have identified affine open sets with their representing algebras, cf. [U1, Ch.2], [M1, pp. 46-66].) For $(a, b) \in E_{ps,pr}(A)$, let $(a_i, b_i)$ be the image of $(a, b)$ under the induced maps

$$E_{ps,pr}(A) \to E_{ps,pr}(A_i).$$

Now form the $A_i$-algebras

$$A'_i = A_i[T_0, T_1, (1 + x_s T_0)^{-1}, (1 + x_r T_1)^{-1}] / \langle p(T_0) - a_i, (1 + x_s T_0)^{-1} q(T_0, T_1) - b_i \rangle.$$

By §1, $p(T_0) - a_i$ is monic of degree $p$ with coefficients in $A_i$ and $q(T_0, T_1)$ is monic, degree $p$ in $T_1$ with coefficients in $A_i[T_0, (1 + x_s T_0)^{-1}]$. It follows that the ideal generated by the coefficients of $(1 + x_s T_0)^{-1} q(T_0, T_1) - b_i \in A_i[T_0, (1 + x_s T_0)^{-1}]$ is all of $A_i[T_0, (1 + x_s T_0)^{-1}]$. Thus by [M1, p. 10, Remark 2.6], each map $A_i \to A'_i$ is flat, and hence faithfully flat by [M1, Prop. 2.7]. Thus $(A \to A'_i)$ is a flat covering of $A$.

Now let $x_i, y_i$ denote the images of $T_0, T_1$ respectively under the canonical map

$$A_i[T_0, T_1, (1 + x_s T_0)^{-1}, (1 + x_r T_1)^{-1}] \to A'_i.$$

Then $(x_i, y_i) \in E_{s,r}(A'_i)$ with

$$\Theta(A'_i)((x_i, y_i)) = (a_i, b_i) = res_{A, A'_i}((a, b))$$

for all $i$, where $res_{A, A'_i}((a, b))$ is the image of $(a, b)$ under the induced maps

$$E_{ps,pr}(A) \to E_{ps,pr}(A'_i);$$
hence \( \Theta \) is an epimorphism of flat sheaves (group schemes) by [M1, p. 63, Thm. 2.15(c)].

We also have a canonical surjection of \( R \)-algebras:

\[
R[T_0, (1 + x_s T_0)^{-1}, T_1, (1 + x_r T_1)^{-1}] \twoheadrightarrow R[T_0, (1 + x_s T_0)^{-1}, T_1, (1 + x_r T_1)^{-1}]/(p(T_0), (1 + x_s T_0)^{-1}q(T_0, T_1)) \cong H(s, r),
\]

with \( T_0, T_1 \) identified with \( \frac{g^p - 1}{x_s} \) and \( \frac{g - 1}{x_r} \), respectively. Thus \( \ker \Theta = Sp_H(H(s, r)) \).

It follows that the resulting short exact sequence of \( R \)-group schemes

\[
Sp_R(H(s, r)) \to E_{s, r} \overset{\Theta}{\to} E_{ps, pr}
\]

is a resolution of the group scheme \( Sp_H \) where \( H \) is an arbitrary Larson order in \( KC_{p^2} \).

We are now in a position to prove our main theorem.

**Theorem 2.1.** Let \( H = H(s, r) \) be an arbitrary Larson order in \( KC_{p^2} \). Then the abelian group of \( H \)-Galois extensions is isomorphic to the quotient group

\[
E_{ps, pr}(R)/\Theta E_{s, r}(R),
\]

where the class \( [(w_{u_0}, w_{u_1})] \) corresponds to an \( H \)-Galois extension

\[
S = R \left[ \frac{v_0 - 1}{x_s}, \frac{v_1 - 1}{x_r} \right],
\]

where \( v_0^p = u_0, v_1^p = v_0 u_1 \). The comodule map \( \rho : S \to S \otimes H(s, r) \) is given by

\[
\rho : v_0 \mapsto v_0 \otimes g^p, \quad \rho : v_1 \mapsto v_1 \otimes g.
\]

**Proof.** Using the given resolution of \( Sp_H(s, r) \), we employ the long exact sequence in cohomology yielding

\[
H^0(R, Sp_H(s, r)) \to H^0(R, E_{s, r}) \to H^0(R, E_{ps, pr})
\]

\[
\to H^1(R, Sp_H(s, r)) \to H^1(R, E_{s, r}) \to H^1(R, E_{ps, pr}) \to \cdots.
\]

Note that

\[
H^0(R, E_{s, r}) = E_{s, r}(R)
\]

and

\[
H^0(R, E_{ps, pr}) = E_{ps, pr}(R);
\]

hence we have an exact sequence

\[
E_{s, r}(R) \to E_{ps, pr}(R) \to H^1(R, Sp_H(s, r)) \to H^1(R, E_{s, r}).
\]

We claim that the last term \( H^1(R, E_{s, r}) \) is trivial. To this end suppose not, and let \( S \) be a nontrivial \( B \)-Galois extension with structure map \( \rho \). (Recall that \( B \) is the representing algebra of \( E_{s, r} \)) By [G, Lemma II.1.6],

\[
\{ x \in S \mid \rho(x) \in S \otimes_R R[T_0, (1 + x_s T_0)^{-1}] \}
\]

is a non-trivial \( R[T_0, (1 + x_s T_0)^{-1}] \)-Galois extension, contradicting [G, Proposition I.2.2], proving our claim.
Now with $H^1(R, E_{s,r}) = 0$ we write the exact sequence

$$E_{s,r}(R) \xrightarrow{\Theta} E_{ps,pr}(R) \rightarrow H^1(R, SpH(s,r)).$$

It follows that

$$E_{ps,pr}(R)/E_{s,r}(R) \cong H^1(R, SpH(s,r)).$$

Given an element $(w_{u_0}, w_{u_1}) \in E_{ps,pr}(R)$ we construct the corresponding $H$-Galois extension $S$ by constructing the image of $(w_{u_0}, w_{u_1})$ under the connecting homomorphism

$$\delta : E_{ps,pr}(R) \rightarrow H^1(R, SpH(s,r)).$$

Following the standard description of $\delta$ (cf. [CF, p.97], [Gi, Ch. III]), we recall our surjection in the flat topology

$$\Theta : E_{s,r} \rightarrow E_{ps,pr}.$$

There exists a finite extension $L/K$, with ring extension $A = O_L/R$ and an element $(w_{v_0}, w_{v_1}) \in E_{s,r}(A)$ so that

$$\Theta(A)(w_{v_0}, w_{v_1}) = (w_{u_0}, w_{u_1}).$$

In other words, the element $(v_0, v_1)$ satisfies

$$v_0^p = u_0, \quad v_0^{-1}v_1^p = u_1.$$

We now let $\delta(w_{u_0}, w_{u_1})$ correspond to the pair $(v_0, v_1)$, forming the $R$-algebra

$$S = R \left[ \frac{v_0 - 1}{x_st}, \frac{v_1 - 1}{x_r} \right].$$

We claim that $S$ is an $H$-Galois extension contained in $O_L \subset L$. It is immediate that $S$ is finitely generated because by construction the generators $w_{v_0} = \frac{v_0 - 1}{x_s}$ and $w_{v_1} = \frac{v_1 - 1}{x_r}$ are in $A$. One can check by hand that $\rho$ is a comodule map, so it remains to show that $\rho$ induces a bijection

$$\gamma_\rho : S \otimes S \rightarrow S \otimes H.$$

Viewing the situation over $K$, we have that

$$S \otimes K = K(v_0, v_1) = K(\sqrt[p]{u_0}, \sqrt[p]{u_1} \sqrt[p]{u_0}) = K(\sqrt[p]{x_t u_0 u_1}) = K(v_1).$$

It follows that $S \otimes K$ is a $KC_{p^2}$-Galois extension with comodule map $\rho \otimes K$, by L. Robert’s isomorphism

$$U(K)/U(K)^{p^2} \cong H^1(K, \mu_{p^2}, K)$$

which computes all $KC_{p^2}$-Galois extensions, cf. [R, p. 693]. Now since

$$\gamma_\rho \otimes K : (S \otimes K) \otimes (S \otimes K) \rightarrow (S \otimes K) \otimes KC_{p^2}$$

is an isomorphism, then

$$\gamma_\rho : S \otimes S \rightarrow S \otimes H$$

is an injection. Following [G, II.1.5], we can show that $\gamma_\rho$ is an bijection by showing that $\text{disc}(S/R) = \text{disc}(H/R)$. To this end, by [G, Prop. II.2.1]

$$R \left[ \frac{v_0 - 1}{x_s} \right]$$
is an $H(s)$-Galois extension, where $H(s)$ is the Tate/Oort order $R \left[ \frac{g^p - 1}{x_s} \right]$. Thus by [G, Lemma II.1.5]

$$\text{disc} \left( R \left[ \frac{g^p - 1}{x_s} \right] / R \right) = \text{disc} \left( R \left[ \frac{v_0 - 1}{x_s} \right] / R \right);$$

hence

$$\text{disc} \left( R \left[ \frac{g^p - 1}{x_s} \right] \otimes R \left[ \frac{h - 1}{x_r} \right] / R \right) = \text{disc} \left( R \left[ \frac{v_0 - 1}{x_s} \right] \otimes R \left[ \frac{h - 1}{x_r} \right] / R \right),$$

where $h$ generates a cyclic group of order $p$. Additionally,

$$\text{disc} \left( R \left[ \frac{v_1 - 1}{x_r} \right] / R \right) = \text{disc} \left( R \left[ \frac{h - 1}{x_r} \right] / R \right);$$

hence

$$\text{disc} \left( R \left[ \frac{v_0 - 1}{x_s} \right] \otimes R \left[ \frac{h - 1}{x_r} \right] / R \right) = \text{disc} \left( R \left[ \frac{v_0 - 1}{x_s} \right] \otimes R \left[ \frac{v_1 - 1}{x_r} \right] / R \right).$$

It follows that $\text{disc}(S/R) = \text{disc}(H/R)$ and hence $S$ is an $H$-Galois extension. Moreover, if $(w_{u_0}, w_{u_1})$ is so that $(w_{u_0}, w_{u_1}) \in E_{s,r}^\theta(R)$, then

$$u_0 = v_0^p, \quad u_1 = v_0^{-1} v_1^p$$

where $(v_0, v_1) \in G_{s,r}(R)$. Now since $v_1 \in K$, $S \otimes K$ will correspond to the trivial $KC_{p^2}$-Galois extension (again use L. Roberts classification). Since the canonical map $H^1(R, SpH(s,r)) \rightarrow H^1(K, \mu_{p^2}, K)$ is injective (cf. [M2], III.1.1), we conclude that $(w_{u_0}, w_{u_1})$ corresponds to the trivial $H$-Galois extension if $(w_{u_0}, w_{u_1}) \in E_{s,r}^\theta(R)$. This completes the proof of the theorem.

We now turn our attention to calculating $H^1(R, SpA_v(s,r))$.

3. A Resolution of $SpR(A_v(s,r))$ When $A_v(s,r)$ is not Larson

To resolve $SpR(A_v(s,r))$, we first define the abelian group functor $W_{s,r}$. We construct this functor by generalizing the method used to construct functors presented in [SS1, Prop. 2.2, Remark 2.3] and [SS2, §3]. In these papers, the authors have resolved

$$SpA_v(1/(p-1), 1/(p-1)) = SpH(0,0)^* = SpR_{C_{p^2}}^*,$$

where $R_{C_{p^2}}^*$ is identified with the maximal integral order in $KC_{p^2}$.

Let $F_0$ be the constant polynomial $F_0 = 1$, and let $F_1(T_0)$ be the polynomial in the indeterminate $T_0$ defined

$$F_1(T_0) = \frac{1 + (1 + x_sT_0) + \cdots + (1 + x_sT_0)^{p-1}}{p}$$

$$+ v \left( \frac{1 + \zeta^{-p}(1 + x_sT_0) + \cdots + \zeta^{-(p-1)p}(1 + x_sT_0)^{p-1}}{p} \right) + \cdots$$

$$+ v^{p-1} \left( \frac{1 + \zeta^{-(p-1)p}(1 + x_sT_0) + \cdots + \zeta^{-(p-1)^2p}(1 + x_sT_0)^{p-1}}{p} \right).$$
Moreover, let
\[ \alpha^F_r(T_0) = x_r T_0 + F_0 = x_r T_0 + 1, \]
\[ \alpha^F_r(T_0, T_1) = x_r T_1 + F_1(T_0), \]
for \( T_0, T_1 \) indeterminate. Additionally, let
\[ \beta^F_r(U_0) = \frac{U_0 - 1}{x_s}, \]
\[ \Lambda^F_r(X_0, Y_0) = x_s X_0 Y_0 + X_0 + Y_0, \]
for indeterminates \( U_0, X_0, Y_0 \). Finally, put
\[ \omega^F_r(i) = \beta^F_r(\zeta^{pi}), \]
for \( i \in \mathbb{Z}_p \). Here \( \zeta^{pi} \) is defined as
\[ \zeta^{pi} = \zeta^{p^{i_0}} \]
where \( i = \sum_{k \geq 0} i_k p^k \).

**Lemma 3.0.** Let \( x_{s_0} = x_s \) and \( x_{s_1} = x_r \). The family \( \{F_r\} \), \( r = 0, 1, \) defined above satisfies the following conditions for each \( r \):

(i)
\[ F_r(0) = 1, \]

(ii)
\[ F_r(X_0)F_r(Y_0) \equiv F_r(\Lambda^F_r(X_0, Y_0))(\mod x_{s_r}), \]

(iii)
\[ F_r(\omega^F_r(1)) \equiv \zeta^{p^{i-r}}(\mod x_{s_r}). \]

**Proof.** This can be verified directly. For example, if \( p = 2 \), (ii) follows by the calculation
\[
F_1(X_0)F_1(Y_0) - F_1(x_s X_0 Y_0 + X_0 + Y_0)
= \left( \frac{1 + (1 + x_s X_0)}{2} + v(1 - (1 + x_s X_0)) \right)
\times \left( \frac{1 + (1 + x_s Y_0)}{2} + v(1 - (1 + x_s Y_0)) \right)
- \left( \frac{1 + (1 + x_s(x_s X_0 Y_0 + X_0 + Y_0))}{2} + v(1 - (1 + x_s(x_s X_0 Y_0 + X_0 + Y_0))) \right)
\equiv 0(\mod x_r)
\]
since \( v(1 - v^2) \geq 2s' + r \). \( \square \)

Thus by [SS1, Remark 2.3] we can construct an \( R \)-group scheme \( W_{s,r} \) with representing algebra
\[ C = R[T_0, T_1, (\alpha^F_r(T_0))^{-1}, (\alpha^F_r(T_0, T_1))^{-1}]. \]
Observe that property (ii) above guarantees a well-defined group law on \( W_{s,r} \): Let \( (m_0, m_1), (n_0, n_1) \in W_{s,r}(A) \) for an \( R \)-algebra \( A \). Then we define
\[ (m_0, m_1) \ast (n_0, n_1) = (m_0 + n_0 + x_s m_0 n_0, m_1 F_1(m_0) + n_1 F_1(m_0) + x_r m_1 n_1 + y) \]
where $y$ is some element of $A$ determined by the congruence in (ii). Moreover condition (i) implies an identity for $W_{s,r}$.

We realize that there is an inclusion of group schemes

$$Sp(A_v(s, r)) \hookrightarrow W_{s,r}$$

induced by the surjection

$$C \longrightarrow C/(x_{-ps}(1 - \alpha_0^G(T_0)^p), x_{-pr}(\alpha_0^G(T_0) - \alpha_1^G(T_0, T_1)^p)) \cong A_v(s, r)$$

with $T_0, T_1$ identified with $g_{ps}^{-1}x_s$ and $g_{pr}^{-1}x_r$, respectively. Moreover, there exists a commutative diagram

$$\begin{array}{ccc}
SpH(r) & \longrightarrow & SpA_v(s, r) \\
\downarrow & & \downarrow \\
SpR[T_0, (1 + x_rT_0)^{-1}] & \longrightarrow & W_{s,r} \\
\downarrow & & \downarrow \\
SpR[T_0, (1 + x_prT_0)^{-1}] & \longrightarrow & SpR[T_0, (1 + x_sT_0)^{-1}]
\end{array}$$

with all rows and columns s.e.s.’s. Here $H(s), H(r)$ denote Larson orders in $KC_{p^2}$.

Thus the quotient $W_{s,r}/SpA_v(s, r)$ is a filtered group scheme of type $(ps, pr)$, with filtration given by $SpR[T_0, (1 + x_{ps}T_0)^{-1}], SpR[T_0, (1 + x_{pr}T_0)^{-1}]$ (cf. [SS2, §3]).

Thus by [SS2, Thm. 3.3]

$$V_{ps, pr} := W_{s,r}/Sp(A_v(s, r)) = Sp(R[T_0, T_1, (\alpha_0^G(T_0))^{-1}, (\alpha_1^G(T_0, T_1))^{-1}]$$

where

$$\alpha_0^G(T_0) = 1 + x_{ps}T_0$$

and

$$\alpha_1^G(T_0, T_1) = G_1(T_0) + x_{pr}T_1,$$

for some polynomial $G_1(T_0) \in R[T_0]$ satisfying the conditions

(i) $G_1(0) = 1,

(ii) $G_1(X_0)G_1(Y_0) \equiv G_1(X_0 + Y_0 + x_{ps}X_0Y_0)(mod \ x_{pr}).$

It follows that the resulting short exact sequence of $R$-group schemes

$$SpR(A_v(s, r)) \longrightarrow W_{s,r} \xrightarrow{\Psi} V_{ps, pr},$$

where $\Psi$ is the canonical surjection, is a resolution of the group scheme $SpH$ where $H$ is an arbitrary non-Larson order in $KC_{p^2}$.

We are now in a position to prove our second main theorem.

**Theorem 3.1.** Let $H = A_v(s, r)$ be an arbitrary non-Larson order in $KC_{p^2}$. Then the abelian group of $H$-Galois extensions is isomorphic to the quotient group

$$V_{ps, pr}(R)/W_{s,r}(R).$$
where the class \([t_0, t_1]\) corresponds to an \(H\)-Galois extension \(S\) of the form
\[
S = R \left[ \frac{v_0 - 1}{x_s}, \frac{v_1 - F_1(t_0)}{x_r} \right],
\]
where \(v_0^p = \alpha_0^G(t_0), \quad v_0^{-1}v_1^p = \alpha_1^G(t_0, t_1)\) and \(v_0' = \frac{v_0 - 1}{x_s}\). The comodule map \(\rho: S \to S \otimes A_v(s, r)\) is given by
\[
\rho: v_0 \mapsto v_0 \otimes g^p, \\
\rho: v_1 \mapsto v_1 \otimes g.
\]

**Proof.** Using the given resolution of \(Sp(A_v(s, r))\), we employ the long exact sequence in cohomology yielding
\[
H^0(R, SpA_v(s, r)) \to H^0(R, W_{s, r}) \to H^0(R, V_{ps, pr}) \\
\to H^1(R, SpA_v(s, r)) \to H^1(R, W_{s, r}) \to H^1(R, V_{ps, pr}) \to \cdots.
\]

Note that
\[
H^0(R, W_{s, r}) = W_{s, r}(R)
\]
and
\[
H^0(R, V_{ps, pr}) = V_{ps, pr}(R);
\]
hence we have an exact sequence
\[
W_{s, r}(R) \to V_{ps, pr}(R) \to H^1(R, SpA_v(s, r)) \to H^1(R, W_{s, r}).
\]

Now since \(H^1(R, W_{s, r}) \cong 0\), we obtain the isomorphism
\[
V_{ps, pr}(R)/W_{s, r}^\Psi(R) \cong H^1(R, SpA_v(s, r)).
\]

Suppose \((t_0, t_1) \in V_{ps, pr}(R)\). We will construct the corresponding \(H\)-Galois extension by computing the image of \((t_0, t_1)\) under the connecting homomorphism
\[
\delta: V_{ps, pr}(R) \to H^1(R, SpA_v(s, r)).
\]

By [SS1, §2.3, p. 109], the canonical flat surjection \(\Psi: W_{s, r} \to V_{ps, pr}\) can be defined via polynomials:
\[
(T_0, T_1) \mapsto (\Psi_0(T_0), \Psi_1(T_0, T_1))
\]
where
\[
\Psi_0(T_0) = \frac{(x_s T_0 + 1)^p - 1}{x_{ps}}, \\
\Psi_1(T_0, T_1) = \frac{(x_s T_0 + 1)^{-1}(x_r T_1 + F_1(T_0))^p - G_1(\Psi_0(T_0))}{x_{pr}}.
\]

Moreover, there exists a finite extension \(L/K\) with ring extension \(A = O_L/R\) and an element \((p_0, p_1) \in W_{s, r}(A)\) so that
\[
\Psi_0(p_0) = \frac{(x_s p_0 + 1)^p - 1}{x_{ps}} = t_0, \\
\Psi_1(p_0, p_1) = \frac{(x_s p_0 + 1)^{-1}(x_r p_1 + F_1(p_0))^p - G_1(\Psi_0(p_0))}{x_{pr}} = t_1.
\]
If we write \( v_0 = 1 + x_sp_0, \ v_1 = F_1(p_0) + x_rp_1 \), we have that \( \delta((t_0, t_1)) \) corresponds to the \( H \)-Galois extension
\[
S = R \left[ \frac{v_0 - 1}{x_s}, \frac{v_1 - F_1(v_0^p)}{x_r} \right],
\]
where \( v_0^p = p_0 \). This follows exactly as in Theorem 2.1, and we outline the proof. We first see that \( S \) is finitely generated since \( (p_0, p_1) \in W_{s,r}(A) \). We then check that \( S \otimes K \) is a \( KC_{p^2} \)-Galois extension, using L. Roberts isomorphism. Finally we conclude that \( S \) is an \( H \)-Galois extension by showing that \( disc(S/R) = disc(H/R) \).

Now suppose \( (t_0, t_1) \in W_{s,r}^g(R) \). Then there exists \( (p_0, p_1) \in W_{s,r}(R) \) so that
\[
t_0 = \frac{\alpha_0^F(p_0)p^p - 1}{x_{ps}},
\]
\[
t_1 = \frac{\alpha_0^F(p_0)^{p-1}(\alpha_1^G(p_0, p_1))p^p - G_1(t_0)}{x_{pr}}.
\]
Over \( K \),
\[
S \otimes K = K(\alpha_0^F(p_0), \alpha_1^F(p_0, p_1)) = K(\sqrt[3]{\alpha_0^G(t_0, t_1)p^p \alpha_0^G(t_0)}) = K(\alpha_1^F(p_0, p_1)),
\]
with \( \alpha_0^F(p_0, p_1) \in K \). Hence \( S \otimes K \) is the trivial \( KC_{p^2} \)-Galois extension. It follows that \( S \) is the trivial \( A_{s,r} \)-Galois extension if and only if the corresponding element \( (t_0, t_1) \in W_{s,r}^g(R) \). This completes the proof of the theorem.

\section*{References}


\textsc{Department of Mathematics, Auburn University at Montgomery, Montgomery, Alabama 36117}

\textit{E-mail address: underw@tango.aum.edu}