Note di Matematica
*Note Mat.* **33** (2013) no. 1, 95–101.
ISSN 1123-2536, e-ISSN 1590-0932
doi:10.1285/i15900932v33n1p95

# Regular groups, radical rings, and Abelian Hopf Galois structures on prime-power Galois field extensions

**A. Caranti**[i]
*Department of Mathematics*
*Università degli Studi di Trento*
*via Sommarive 14*
*I-38123 Trento*
*Italy*

**Keywords:** Galois field extensions, Hopf Galois structures, regular groups, radical rings

**MSC 2000 classification:** 12F10 16Txx

This is a report on joint work of the author with S. C. Featherstonhaugh and L. N. Childs, and expands slightly on the presentation given by the author at Porto Cesareo, on June 9, 2011, at the Conference on Advances in Group Theory and Applications. The full results appear in [5].

## 1 Hopf Galois structures

The concept of *Hopf Galois structures* arose in the study of purely inseparable field extensions, and was introduced by Chase and Sweedler, in their 1969 work [4]. It was later recognized that the Hopf algebras in question were too small to be able to describe the full automorphism structure of a purely inseparable extension of arbitrary height. However, Greither and Pareigis gave new life to the subject in 1987 [6], showing that the concept of Hopf Galois extension could be profitably applied to separable and Galois field extensions.

We will not give a definition of Hopf Galois structures (we refer to [3] for that), because we take advantage of the following result, which provides a translation in terms of regular subgroups of symmetric groups.

**Theorem 1** (Greither-Pareigis)**.** *Let $L/K$ be a separable extension with normal closure $E$.*

[i]The author is very grateful to the organizers of the Conference *Advances in Group Theory and Applications 2011* for inviting him to give the talk of which this paper is a reworking. The author has been supported by MIUR–Italy via PRIN 2008 *Lie algebras, groups, computational methods, combinatorial identities, derivations.*

*Let* $G = \mathrm{Gal}(E/K)$, $G' = \mathrm{Gal}(E/L)$, *and* $X = G/G' = \{\, aG' : a \in G \,\}$ *be the space of left coset.*

*Then there is a bijection between*

*(1) Hopf Galois structures on* $L/K$, *and*

*(2) regular subgroups* $N$ *of* $\mathrm{Sym}(X)$ *normalized by* $\lambda(G)$.

Here $\lambda : G \to \mathrm{Sym}(X)$ is the usual action of $G$ on the left cosets:

$$g \mapsto (aG' \mapsto gaG').$$

It might be remarked that in this context the only Hopf algebras that occur are the group algebras $EN$.

Byott [1] was able to rephrase and refine Theorem 1.

**Theorem 2** (Byott)**.** *Let* $G' \leq G$ *be finite groups,* $X = G/G'$, *and* $N$ *a group of order* $|X|$. *There is a correspondence between*

*(1) injective morphisms* $\alpha : N \to \mathrm{Sym}(X)$ *such that* $\alpha(N)$ *is regular, and*

*(2) injective morphisms* $\beta : G \to \mathrm{Sym}(N)$ *such that* $\beta(G')$ *is the stabilizer of the identity of* $N$.

*Here* $\alpha_1(N) = \alpha_2(N)$ *if and only if* $\beta_1(G)$ *and* $\beta_2(G)$ *are conjugate under* $\mathrm{Aut}(N)$. *Moreover* $\alpha(N)$ *is normalized by* $\lambda(G)$ *if and only if* $\beta(G) \leq \mathrm{Hol}(N)$.

These results can be summed up as follows.

**Theorem 3.** *Let* $L/K$ *be a separable field extension with normal closure* $E$. *Let* $G = \mathrm{Gal}(E/K)$, $G' = \mathrm{Gal}(E/L)$. *Let* $\mathcal{S}$ *be the set of isomorphism classes of groups* $N$ *of order* $|G/G'|$.

*Then the number of Hopf Galois structures on* $L/K$ *is*

$$\sum_{N \in \mathcal{S}} e(G, N),$$

*where* $e(G, N)$ *is the number of equivalence classes,* modulo conjugation under $\mathrm{Aut}(N)$, *of regular embeddings* $\beta : G \to \mathrm{Hol}(N)$ *such that* $\beta(G')$ *is the stabilizer of the identity of* $N$.

The main goal of [5] is to prove the following vanishing result for the summand $e(G, N)$ in Theorem 3.

**Theorem 4.** *Suppose* $G$ *and* $N$ *are non-isomorphic* abelian $p$*-groups, where* $N$ *has rank* $m$, *and* $p > m + 1$.

*Then*

$$e(G, N) = 0,$$

*that is,* all abelian regular subgroups of $\mathrm{Hol}(N)$ are isomorphic to $N$.

*It follows that if $L/K$ is a Galois extension of fields with abelian Galois group $G$, and if $L/K$ is $H$-Hopf Galois, where the $K$-Hopf algebra $H$ has associated group $N$, then $N$ is isomorphic to $G$.*

## 2 Regular abelian subgroups

The key to our proof is the following result of [2].

**Theorem 5.** *Let $F$ be an arbitrary field, and $(V,+)$ a vector space of arbitrary dimension over $F$.*

*There is a one-to-one correspondence between*

*(1) abelian regular subgroups $T$ of $\mathrm{AGL}(V)$, and*

*(2) commutative, associative $F$-algebra structures $(V,+,\cdot)$ that one can impose on the vector space structure $(V,+)$, such that the resulting ring is radical.*

*In this correspondence, isomorphism classes of $F$-algebras correspond to conjugacy classes under the action of $\mathrm{GL}(V)$ of abelian regular subgroups of $\mathrm{AGL}(V)$.*

Now $\mathrm{AGL}(V)$ is the split extension of $V$ by $\mathrm{GL}(V)$. This acts naturally on $V$. The above result holds verbatim if one replaces $V$ by any abelian group $N$, and $\mathrm{AGL}(V)$ by the holomorph $\mathrm{Hol}(N)$ of $N$, that is the split extension of $N$ by $\mathrm{Aut}(N)$. This also acts naturally on $N$. Thus we have

**Theorem 6.** *Let $(N,+)$ be an abelian group.*
*There is a one-to-one correspondence between*

*(1) abelian regular subgroups $T$ of $\mathrm{Hol}(N)$, and*

*(2) commutative, associative ring structures $(N,+,\cdot)$ that one can impose on the abelian group structure $(N,+)$, such that the resulting ring is radical.*

*In this correspondence, isomorphism classes of rings correspond to conjugacy classes under the action of $\mathrm{Aut}(N)$ of abelian regular subgroups of $\mathrm{Hol}(N)$.*

Note how the equivalence classes fit perfectly with those of Theorem 2, involved in counting Hopf Galois structures.

## 3 An elementary result

Let $p$ be a prime. Let $(N,+)$ be an elementary abelian group of order $p^m$. Let $(N,+,\cdot)$ be a commutative, associative, nilpotent ring based on the group $(N,+)$. Then $(N,\circ)$ is also a group, where

$$u \circ v = u + v + u \cdot v.$$

Because of the result above, each regular subgroup $G$ of $\mathrm{Hol}(N)$ is isomorphic to such a $(N, \circ)$.

We begin with

**Lemma 1.** *If $(N, +)$ is elementary abelian of order $p^m$, with $p > m$, then $(N, \circ)$ is also elementary abelian.*

Note that this is simply stating the obvious fact that a $p$-element of $\mathrm{GL}(m, p)$, with $m < p$, has order $p$. However, we are using this simple instance as a first illustration of the way we are using Theorem 6 in the proof of Theorem 4.

We will be using repeatedly the simple relation

$$\begin{aligned} p_\circ a &= \sum_{i=1}^{p} \binom{p}{i} a^i \\ &= pa + \sum_{i=2}^{p-1} \binom{p}{i} a^i + a^p, \end{aligned}$$

where we use the notation $k_\circ a = \underbrace{a \circ \cdots \circ a}_{k \text{ times}}$.

*Proof of Lemma 1.* $(N, +, \cdot)$ is a nilpotent ring of order $p^m$. $p \geq m + 1$. Thus $N^p \subseteq N^{m+1} = \{ 0 \}$. It follows that $a^p = 0$ for $a \in N$. Now

$$p_\circ a = \sum_{i=1}^{p-1} \binom{p}{i} a^i + a^p$$

implies that $(N, \circ)$ is also elementary abelian. QED

## 4 Two examples

In constructing examples, the idea is to start with a suitable ring. Let $F$ be the field with $p$ elements, $p$ a prime. Consider the ring of order $p^p$

$$(N, +, \cdot) = xF[x]/x^{p+1}F[x],$$

where $F[x]$ is the ring of polynomials in the indeterminate $x$. Now $(N, \circ)$ is (isomorphic to) a regular abelian subgroup of $\mathrm{Hol}(N, +)$, where $u \circ v = u + v + u \cdot v$. Let $a$ be the image of $x$ in the ring $N$. Then

$$p_\circ a = \sum_{i=1}^{p-1} \binom{p}{i} a^i + a^p = a^p \neq 0,$$

so that $(N, \circ)$ has exponent (at least) $p^2$. (It would be easy to see that $(N, \circ)$ has type $(p^2, p, \ldots, p)$.)

This shows that the result of Lemma 1 is sharp.

For a "converse", start with the ring $x\mathbb{Z}[x]/x^{p+1}\mathbb{Z}[x]$, where $p$ is a prime. Consider the quotient ring $(N, +, \cdot)$ of it modulo the ideal spanned by the image of $px + x^p$. Write $a$ for the image of $x$ in $N$. Then $N$ has order $p^p$,

$$pa + a^p = 0, \qquad pa^i = 0, \text{ for } i > 1,$$

and $(N, +)$ has $m = p - 1$ generators $a, a^2, \ldots, a^{p-1}$, and type $(p^2, p, \ldots, p)$. Then there is an abelian regular subgroup of $\mathrm{Hol}(N, +)$ which is isomorphic to $(N, \circ)$. In $(N, \circ)$ we have $p \circ a^i = 0$ for $i > 1$, and

$$p \circ a = pa + \sum_{i=2}^{p-1} \binom{p}{i} a^i + a^p = pa + a^p = 0,$$

so that $(N, \circ)$ is elementary abelian.

In this example, $m = p + 1$, and the conclusion of Theorem 4 fails. This shows that the result of Theorem 4 is sharp.

# 5 Proof of Theorem 4

Because of the correspondence established in Theorem 6, we have to prove that, under the assumptions of Theorem 4, if $(N, +, \cdot)$ is any associative, nilpotent ring, then $(N, +)$ and $(N, \circ)$ are isomorphic.

We will show that the two finite abelian groups $(N, +)$ and $(N, \circ)$ have the same number of elements of each order, from which isomorphism follows.

Consider the subgroups of $(N, +)$

$$\Omega_i(N, +) = \left\{ x \in N : p^i x = 0 \right\}.$$

These are ideals of $(N, +, \cdot)$, so that they are also subgroups of $(N, \circ)$, as $x \circ y = x + y + x \cdot y$. We want to show that for each $i$ the following *equalities* hold

$$\Omega_{i+1}(N, +) \setminus \Omega_i(N, +) = \Omega_{i+1}(N, \circ) \setminus \Omega_i(N, \circ) \tag{5.1}$$

between the set of elements of order $p^{i+1}$ in $(N, +)$, respectively $(N, \circ)$.

However, we only need to prove the *inequalities*

$$\Omega_{i+1}(N, +) \setminus \Omega_i(N, +) \subseteq \Omega_{i+1}(N, \circ) \setminus \Omega_i(N, \circ). \tag{5.2}$$

In fact, suppose all of the (5.2) hold. If this is the case, note that $N$ is the disjoint union of the left-hand terms of (5.2) (plus $\{ 0 \}$). Since $N$ is finite, it

follows that all inequalities in (5.2) are equalities, that is, all of the (5.1) also hold.

Consider the sections of the group $(N, +)$

$$S_i = \Omega_{i+1}(N, +)/\Omega_{i-1}(N, +),$$

for $1 \leq i < e$, where $p^e$ is the exponent of $(N, +)$. These sections have exponent $p^2$ as groups with respect to $+$. Note that these are also sections of the ring $(N, +, \cdot)$ and of the group $(N, \circ)$.

We will now prove the following

**Lemma 2.** *The orders of the elements of each $S_i$ are the same with respect to $+$ and $\circ$.*

From this the inequalities (5.2) will follow, and thus the main result. In fact, the cases $i = 0, 1$ of (5.2) are taken care directly by the Lemma for $i = 1$, as in this case $S = \Omega_2(N, +)$. Proceeding by induction, if $a \in \Omega_{i+1}(N, +) \setminus \Omega_i(N, +)$, the Lemma states that $p \circ a \in \Omega_i(N, +) \setminus \Omega_{i-1}(N, +)$. By the inductive hypothesis, this is contained in $\Omega_i(N, \circ) \setminus \Omega_{i-1}(N, \circ)$, so that $a \in \Omega_{i+1}(N, \circ) \setminus \Omega_i(N, \circ)$.

*Proof of Lemma 2.* Clearly $T = \Omega_1(S, +) = \Omega_i(N, +)/\Omega_{i-1}(N, +)$, and $pS \subseteq T$.

Consider first an element $0 \neq a \in T$, so that $a$ has order $p$ with respect to $+$. We want to show that $a$ has order $p$ also with respect to $\circ$. Since $T$ is an elementary abelian section of $(N, +)$, it has order at most $p^m$. Since $p > m + 1 > m$, Lemma 1 implies that $(T, \circ)$ is also elementary abelian.

Suppose now $a \in S \setminus T$, so that $a$ has order $p^2$ with respect to $+$. We want to show that $a$ has order $p^2$ also with respect to $\circ$.

Note that $(S/T, +)$ is an elementary abelian section of $(N, +)$, and thus $S/T$ has order at most $p^m$. Now $(S/T, +, \cdot)$ is a nilpotent ring of order at most $p^m < p^p$, so that $S^p \subseteq S^{m+1} \subseteq T$. Using this, and the fact that $pS \subseteq T$, in the formula

$$p \circ a = \sum_{i=1}^{p-1} \binom{p}{i} a^i + a^p,$$

we obtain that $p \circ a \in T$, and so $a$ has order *at most* $p^2$ with respect to $\circ$.

We will now show that $p \circ a \neq 0$, so that $a$ will have order *exactly* $p^2$ also with respect to $\circ$. Since we are only working in the subring of $S$ spanned by $a$, we redefine $S$ to be just that. If $pa \notin S^2$, then it is clear from

$$p \circ a = pa + \sum_{i=2}^{p} \binom{p}{i} a^i$$

that $p \circ a \equiv pa \not\equiv 0$ modulo $S^2$, so that $p \circ a \neq 0$, and we are done.

So assume $pa \in S^2$, and let $k \geq 2$ be such that $pa \in S^k \setminus S^{k+1}$. Since $S$ is generated by $a$, we will have $pS \subseteq S^k$. This means that $(S/S^k, +)$ is elementary abelian. Now $S^k \neq \{0\}$, as it contains $pa \neq 0$. Thus in the nilpotent ring $S$ we have the proper inclusions $S \supset S^2 \supset \cdots \supset S^k \supset \{0\}$. It follows that the elementary abelian section $(S/S^k, +)$ of $(N, +)$ has a basis given by $a, a^2, \ldots, a^{k-1}$, so that it has order $p^{k-1}$, and thus $k - 1 \leq m$.

Consider once more

$$p_\circ a = pa + \sum_{i=2}^{p-1} \binom{p}{i} a^i + a^p.$$

Since $pa \in S^k$, for $2 \leq i \leq p-1$ we have

$$\binom{p}{i} a^i \in S^k S = S^{k+1}.$$

Since $p \geq m + 2 \geq k + 1$, we have also $a^p \in S^p \subseteq S^{k+1}$. Now the formula above yields $p_\circ a \equiv pa \not\equiv 0$ modulo $S^{k+1}$, so that $p_\circ a \neq 0$, and we are done. QED

# References


[1] N. P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Algebra **24** (1996), no. 10, 3217–3228.

[2] A. Caranti, F. Dalla Volta and M. Sala, *Abelian regular subgroups of the affine group and radical rings*, Publ. Math. Debrecen **69** (2006), no. 3, 297–308.

[3] Lindsay N. Childs, *Taming wild extensions: Hopf algebras and local Galois module theory*, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, Providence, RI, 2000.

[4] Stephen U. Chase and Moss E. Sweedler, *Hopf algebras and Galois theory*, Lecture Notes in Mathematics, vol. 97, Springer-Verlag, Berlin, 1969.

[5] S.C. Featherstonhaugh, A. Caranti and L.N. Childs, *Abelian Hopf Galois structures on prime-power Galois extensions*, Trans. Amer. Math. Soc. **364** (2012), 3675–3684.

[6] Cornelius Greither and Bodo Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), no. 1, 239–258.