ISOMORPHISM TYPES OF HOPF ALGEBRAS IN A CLASS OF ABELIAN EXTENSIONS. I.

LEONID KROP

Abstract. There is no systematic general procedure by which isomorphism classes of Hopf algebras that are extensions of \( kF \) by \( kG \) can be found. We develop the general procedure for classification of isomorphism classes of Hopf algebras which are extensions of the group algebra \( kC_p \) by \( kG \) where \( C_p \) is a cyclic group of prime order \( p \) and \( kG \) is the Hopf algebra dual of \( kG \), \( G \) a finite abelian \( p \)-group and \( k \) is an algebraically closed field of characteristic 0. We apply the method to calculate the number of isoclasses of commutative extensions and certain extensions of this kind of dimension \( \leq p^4 \).

Keywords Hopf algebras, Abelian extensions, Crossed products, Cohomology Groups

Mathematics Subject Classification (2000) 16W30 - 16G99

0. Introduction

There is no systematic general procedure by which isomorphism classes of Hopf algebras that are extensions of \( kH \) by \( kG \) can be found. The purpose of this article is to fill this gap in case \( H = C_p \) and \( G \) is a finite abelian \( p \)-group for a prime \( p \), and \( k \) is an algebraically closed field of characteristic zero.

Let us agree to write \( \text{Ext}(kC_p, kG) \) for the set of all equivalence classes of extensions of \( kC_p \) by \( kG \). Elements of \( \text{Ext}(kC_p, kG) \) possess two special features. Every algebra \( H \) there is equivalent as extension to smash product \( kG \# kC_p \) with respect to a certain action of \( C_p \) on \( kG \), and \( kC_p \) is central in the dual Hopf algebra \( H^* \). The action of \( C_p \) on \( kG \) induces an action \( \prec \) of \( C_p \) on \( G \), the corresponding \( ZC_p \)-module is denoted by \( (G, \prec) \). In consequence, \( H \) is determined up to equivalence by a pair \((\tau, \prec)\) where \( \tau : kC_p \to kG \otimes kG \) is a 2-cococycle deforming the tensor product coalgebra structure of \( kG \otimes kF \). Abelian extensions with undeformed multiplication were studied by M.Mastnak [11]. We

Date: 4/14/14.
Research partially supported by a grant from the College of Liberal Arts and Sciences at DePaul University.
adopt a version of his notation $H^2_c(\mathbb{k}C_p, \mathbb{k}G, \cdot)$ for the group of Hopf 2-cocycles.

The first major result is a structure theorem for the group $H^2_c(\mathbb{k}C_p, \mathbb{k}G, \cdot)$. It states that if $G$ is any finite abelian $p$-group with $p > 2$, or a finite elementary 2-group then there is a $C_p$-isomorphism

$$H^2_c(\mathbb{k}C_p, \mathbb{k}G, \cdot) \simeq H^2(C_p, \widehat{G}, \cdot) \times H^2_N(G, \mathbb{k}^*)$$

where $\widehat{G}$ is the dual group of $G$, $H^2(C_p, \widehat{G}, \cdot)$ is the second cohomology group of $C_p$ over $\widehat{G}$ with respect to the action $\cdot$, and $H^2_N(G, \mathbb{k}^*)$ is the kernel in the Schur multiplier of $G$ of the norm mapping. We point out that formula (0.1) can be seen as a generalization of the Baer’s exact sequence for the cohomology group $H^2(G, C_p)$ of central extensions of $G$ by $C_p$ [2, p.34]. For, setting $\cdot = \text{triv}$, the trivial action, we show (Section 4) that $H^2_c(\mathbb{k}C_p, \mathbb{k}G, \text{triv})$ coincides with $H^2(G, C_p)$ while $H^2(C_p, \widehat{G}, \text{triv})$ and $H^2_N(G, \mathbb{k}^*)$ can be identified with $\text{Ext}^1_{\mathbb{k}}(G, C_p)$ and $\text{Hom}(\wedge^2G, C_p)$, respectively. Hence (0.1) turns into the splitting of the norm mapping. We recall that by a fundamental result of D. Stefan [21] the number of isomorphism types in any of our classes is finite. In the case at hand, we show that there is a bijection between isotypes of noncocommutative Hopf algebras in $\text{Ext}^1_{\mathbb{k}}(\mathbb{k}C_p, \mathbb{k}G)$ and the orbits of $\mathcal{G}(\cdot)$ in $H^2_c(\mathbb{k}C_p, \mathbb{k}G, \cdot)$ not contained in the subgroup $H^2_{cc}(\mathbb{k}C_p, \mathbb{k}G, \cdot)$ parametrizing cocommutative extensions.

Let $I(\cdot, \cdot)$ be the set of automorphisms of $G$ intertwining actions $\cdot$ and $\cdot'$. $I(\cdot, \cdot')$ is an $A(\cdot)$-set, in fact a single orbit of $A(\cdot)$ in $\text{Aut}(G)$. For every $\alpha \in A_p$ fix some $\lambda_\alpha$ in $I(\cdot, \cdot')$. The group $\mathcal{G}(\cdot)$ is the subgroup of $\text{Aut}(G)$ generated by $A(\cdot)$ and all $\lambda_\alpha$. In fact, $\mathcal{G}(\cdot)$ is a crossed product of $A(\cdot)$ with a subgroup of $A_p$. It transpires that $H^2_c(\mathbb{k}C_p, \mathbb{k}G, \cdot)$ is a $\mathcal{G}(\cdot)$-module. The orbits of $\mathcal{G}(\cdot)$ in $H^2_c(\mathbb{k}C_p, \mathbb{k}G, \cdot)$ determine isotypes of extension in the following way. Let us denote by $[\cdot]$ the set of all actions $\cdot'$ isomorphic to $\cdot$ for some $\alpha$. We designate $\text{Ext}^1_{\mathbb{k}}(\mathbb{k}C_p, \mathbb{k}G)$ to the set of all equivalence classes of extensions whose $C_p$-action belongs to $[\cdot]$. We recall that by a fundamental result of D. Stefan [21] the number of isomorphism types in any of our classes is finite. In the case at hand, we show that there is a bijection between isotypes of noncocommutative Hopf algebras in $\text{Ext}^1_{\mathbb{k}}(\mathbb{k}C_p, \mathbb{k}G)$ and the orbits of $\mathcal{G}(\cdot)$ in $H^2_c(\mathbb{k}C_p, \mathbb{k}G, \cdot)$ not contained in the subgroup $H^2_{cc}(\mathbb{k}C_p, \mathbb{k}G, \cdot)$ parametrizing cocommutative extensions.
Assuming $G$ elementary abelian and $p$ odd we extend the bijection to all isoclasses in $\text{Ext}_{G}^{1}(kC_{p}, kG)$. This is done by showing that for cocommutative extensions $G$-orbits in $H_{cc}^{2}(kC_{p}, kG, \triangleright)$ coincide with $A(\triangleright)$-orbits there, and furthermore their isoclasses in are in 1 − 1 correspondence with the orbits of $A(\triangleright)$ in $H_{cc}^{2}(kC_{p}, kG, \triangleright)$.

The last part of the paper is devoted to explicit calculations of the orbit set in several cases. For concrete calculations the smaller space $X(\triangleright) := H^{2}(C_{p}, G, \triangleright) \times H^{2}_{N}(G, k^{*})$ is most convenient. $X(\triangleright)$ gets its $G(\triangleright)$ action by transport of action via isomorphism (0.1). The action is component-wise for every odd $p$. Assuming $G$ an elementary $p$-group and $p$ odd we show that there are $\lfloor \frac{3n+2}{2} \rfloor$ orbits for $\triangleright = \text{triv}$. We also describe orbit sets for all actions on elementary $p$-group $G$ of order $p^{3}$. Lower order cases, viz. $|G| = p, p^{2}$ are known with $|G| = p$ and $|G| = p^{2}$ due to [15] and [14], respectively.

The paper is organized in six sections. In Section 1 we review the necessary facts of the theory of abelian extension. In section 2 we prove formula (0.1) for the groups $H_{cc}^{2}(kC_{p}, kG, \triangleright)$. Section 3 contains the isomorphism and bijection theorems. In Sections 4 and 5 we determine the orbit sets for commutative extensions with $G$ elementary $p$-group, and all extensions with $G$ elementary $p$-group of order $\leq p^{3}$, respectively, and compute the number of isoclasses.

0.1. Notation and Convention. In addition to notation introduced in the Introduction we will use the following.  

- $A^{*}$ the group of units of a commutative ring $A$.
- $\Gamma^{n}$ direct product of $n$ copies of group $\Gamma$.
- $\text{Fun}(\Gamma, A^{*})$ the group of all functions from $\Gamma$ to $A^{*}$ with pointwise multiplication. We will identify groups $\text{Fun}(G^{n}, (kF^{m})^{*})$, $\text{Fun}(F^{m}, (k^{G^{m}})^{*})$ and $\text{Fun}(G^{n} \times F^{m}, \mathbb{k})$ via $f(a)(x) = f(x)(a) = f(a, x)$ where $a \in G^{n}, x \in F^{m}$.
- $Z^{2}(\Gamma, A^{*}, \bullet), B^{2}(\Gamma, A^{*}, \bullet)$ and $H^{2}(\Gamma, A^{*}, \bullet)$ are the group of 2-cocycles, 2-coboundaries, and the second degree cohomology group of $\Gamma$ over $A^{*}$ with respect to an action $\bullet$ of $\Gamma$ on $A$ by ring automorphisms.
- $\delta_{\Gamma}$ the differential of the standard cochain complex for cohomology of the triple $(\Gamma, A^{*}, \bullet)$ [12, IV.5].
- $Z_{p^{n}}$ cyclic group of order $p^{n}$ additively written.
- By abuse of notation we will often use the same symbol for an element of $Z^{2}(\Gamma, A^{*}, \triangleright)$ and its image in $H^{2}(\Gamma, A^{*}, \triangleright)$.

Throughout the paper we treat the terms $\Gamma$-module, $\Gamma$-linear, etc as synonymous to $\mathbb{Z}\Gamma$-module, $\mathbb{Z}\Gamma$-linear, etc.
1. Background Review

1.1. Extensions of Hopf Algebras. Let $k$ be a ground field. In this paper we are concerned with finite-dimensional Hopf algebras over $k$. For a Hopf algebra $H$ we use the standard notation $H^+ = \text{Ker} \varepsilon$. Let $\pi : H \to K$ be a morphism of Hopf algebras. We let $H^{\text{cor}}$ and $^{\text{cor}}H$ denote subalgebras of right/left coinvariants [17, 3.4]. We adopt H.-J. Schneider’s definition of a Hopf algebra extension [19]. In our context it is stated as follows.

**Definition 1.1.** A Hopf algebra $C$ is an extension of a Hopf algebra $B$ by a Hopf algebra $A$ if there is a sequence of Hopf mappings

\[ A \xrightarrow{\iota} C \xrightarrow{\pi} B. \]

with $\iota$ monomorphism, $\pi$ epimorphism, $\iota(A)$ normal in $C$ and $\text{Ker} \pi = \iota(A)^+C$.

We add some comments to the definition. By [20, Remark 1.2] or [17, 3.4.3] we have the fundamental fact that $\iota(A) = C^{\text{cor}}$. It follows that our definition coincides with the definition of extension in [1]. Conversely, the equality $\iota(A) = C^{\text{cor}}$ is equivalent to the equality $\iota(A) = ^{\text{cor}}C$ [3, 4.19], and both of them imply $\iota(A)$ is normal [3, 4.13]. Even more is true. Either condition $\iota(A) = C^{\text{cor}}$ or $\text{Ker} \pi = \iota(A)^+C$ renders the sequence (E) an extension. For details see [1, 3.3.1].

1.2. Abelian Extensions. We assume in what follows the ground field $k$ to be an algebraically closed field of characteristic 0 and $C$ to be a finite-dimensional Hopf algebra. An extension (E) is called abelian if $A$ is commutative and $B$ is cocommutative. It is well-known [10, Theorem 1] and [17, 2.3.1] that in this case $A = k^G$ and $B = kF$ for some finite groups $G$ and $F$. Below we consider only extensions of this kind and we use the notation

\[ (A) \quad k^G \xrightarrow{\iota} H \xrightarrow{\pi} kF. \]

To simplify notation we will refer to the Hopf algebra $H$ in a sequence (A) as an extension of $kF$ by $k^G$. Essential to the theory of abelian extensions is a result in [18], or general theorems [20, 2.4], [13, 3.5], asserting $H$ is a crossed product of $kF$ over $k^G$. The theorem entails existence of a mapping called section (see, e.g. [1, 3.1.13])

\[ (1.1) \quad \chi : kF \to H \]

\[ \text{A short independent proof for abelian extension is given in the Appendix} \]
giving rise to the crossed product structure on $H$. This means $H = \mathbb{k}^G\chi(F)$ with the multiplication

$$
(1.2) \quad (f\chi(x))(f'\chi(y)) = f(\chi(x)f'\chi^{-1}(x))\chi(x)\chi(y) = f(\chi(x)f'\chi^{-1}(x))[\chi(x)\chi(y)\chi^{-1}(xy)]\chi(xy)
$$

for $f, f' \in \mathbb{k}^G, x, y \in F$. The mapping $x \otimes f \mapsto x.f := \chi(x)f\chi^{-1}(x)$ defines a module algebra action of $F$ on $\mathbb{k}^G$ and the function $\sigma : F \times F \to \mathbb{k}^G, \sigma(x, y) = \chi(x)\chi(y)\chi^{-1}(xy)$ is a left, normalized 2-cocycle for that action [17, 7.2.3]. We recall that definition of action is independent of the choice of section, see e.g. [17, 7.3.5].

We consider the dual of the above action of $\mathbb{k}F$ on $\mathbb{k}^G$. For any finite group $G$ we identify $(\mathbb{k}^G)^*$ with $\mathbb{k}G$ by treating $r \in \mathbb{k}G$ as the functional $f \mapsto f(r), f \in \mathbb{k}^G$. By general principles the transpose of a left module action of $\mathbb{k}F$ on $\mathbb{k}^G$ is a right module coalgebra action, denoted $\triangleleft$ of $\mathbb{k}F$ on $(\mathbb{k}^G)^* = \mathbb{k}G$. Under this action $a \triangleleft x$ is that element of $G$ for which

$$
(1.3) \quad (a \triangleleft x)(f) := f(a \triangleleft x) = (x.f)(a), \text{ for all } f \in \mathbb{k}^G, a \in G, x \in F.
$$

This definition makes sense as $\Delta_{\mathbb{k}G}$ is a $\mathbb{k}F$-linear map, hence there holds $\Delta_{\mathbb{k}G}(a \triangleleft x) = a \triangleleft x \otimes a \triangleleft x$, whence $a \triangleleft x$ is a grouplike, hence in $G$. We note that, in general, $\triangleleft$ is a permutation action on $G$. Let $\{p_a | a \in G\}$ be a basis of $\mathbb{k}^G$ dual to the basis $\{a|a \in G\}$ of $\mathbb{k}G$. One can see easily that in the basis $\{p_a\}$ the two actions are related by the formula

$$
(1.4) \quad x.p_a = p_{ax^{-1}}
$$

Theory of extensions has a fundamental duality expressed by the fact that for each sequence $(E)$ its companion sequence

$$
(E^*) \quad B^* \xrightarrow{\pi^*} C^* \xrightarrow{\iota^*} A^*
$$

is also an extension, see [5, 4.1] or [1, 3.3.1]. Since for any finite group $F$, $(\mathbb{k}F)^* = \mathbb{k}^F$ and $(\mathbb{k}F)^* = \mathbb{k}F$, every diagram (A) induces a diagram

$$
(A^*) \quad \mathbb{k}F \to H^* \to \mathbb{k}G
$$

A crossed product structure on $H^*$ is effected by a section

$$
(1.5) \quad \omega : \mathbb{k}G \to H^*
$$

We choose to write $H^* = \omega(G)\mathbb{k}F$ with the multiplication

$$
(1.6) \quad (\omega(a)\beta)(\omega(b)\beta') = \omega(ab)\tau(a, b)(\beta.b)\beta',
$$

where for $a, b \in G$, $\beta, \beta' \in \mathbb{k}F$

$$
(1.7) \quad \beta.b = \omega^{-1}(b)\beta\omega(b), \text{ and }
$$

$$
(1.8) \quad \tau(a, b) = \omega^{-1}(ab)\omega(a)\omega(b).
$$
We note that $\tau : G \times G \to k^F$ is a right, normalized 2-cocycle for the action $\beta \otimes b \mapsto \beta.b$. As above the right action of $G$ on $k^F$ induces a left action of $G$ on $F$ by permutations denoted by $a \triangleright x$, and the two actions are related by

$$(1.9) \quad p_x.a = p_{a^{-1} \triangleright x}$$

We fuse both actions into the definition of a product on $F \times G$ via

$$(1.10) \quad (xa)(yb) = x(a \triangleright y)(a \triangleleft y)b$$

It was noted by M. Takeuchi [22] that the composition 1.10 defines a group structure on $F \rtimes G$ provided the actions $\triangleleft, \triangleright$ satisfy the conditions

$$(1.11) \quad ab \triangleleft x = (a \triangleleft (b \triangleright x))(b \triangleleft x)$$

$$(1.12) \quad a \triangleright xy = (a \triangleright x)((a \triangleleft x) \triangleright y)$$

We use the standard notation $F \triangleright \triangleleft G$ for the set $F \times G$ endowed with multiplication (1.10). We will also adopt the notation $\overline{\tau}$ for $\chi(x)$ and $\overline{a}$ for $\omega(a)$.

The above discussion enables us to associate a datum $\{\sigma, \tau, \triangleleft, \triangleright\}$ to every Hopf algebra $H$ in an extension of type (A), and we write $H = H(\sigma, \tau, \triangleleft, \triangleright)$ and $H^* = H^*(\sigma, \tau, \triangleleft, \triangleright)$ for $H$ and its dual.

1.3. Cocentral Extensions. An extension (A) is called cocentral [8] if $k^F$ is a central subalgebra of $H^*$. We record two properties of cocentral extensions needed below

**Lemma 1.2.** (1) An extension (A) is cocentral iff $\triangleright$ is trivial, or equivalently $G$ is a normal subgroup of $F \triangleright \triangleleft G$ in which case $F \triangleleft \triangleright G$ is a semidirect product $F \ltimes G$.

(2) If (A) is cocentral, then $\Delta_{k^G}$ is $F$-linear.

**Proof:** (1) It is well known [16, (4.10)] that $F \triangleright \triangleleft G$ is a group for any two actions $\triangleleft, \triangleright$ arising from an abelian extension. By (1.10) $x^{-1}ax = x^{-1}(a\triangleright x)(a\triangleleft x)$, hence $x^{-1}ax \in G$ for all $a \in G, x \in F$ iff $x^{-1}(a\triangleright x) = 1$, that is $a\triangleright x = x$. On the other hand $k^F$ is cocentral iff $p_x.a = p_{a^{-1} \triangleright x} = p_x$ by (1.9). The rest of part (1) is immediate from (1.11).

(2) We must show the equality $\Delta_{k^G}(x.p_a) = x.\Delta_{k^G}(p_a)$. On the one hand we have

$$x.\Delta_{k^G}(p_a) = \sum_{bc=a} x.p_b \otimes x.p_c = \sum_{bc=a} p_{bcx^{-1}} \otimes p_{cax^{-1}}.$$

In the second place

$$\Delta_{k^G}(x.p_a) = \Delta_{k^G}(p_{a\triangleright x^{-1}}) = \sum_{ef=a\triangleright x^{-1}} p_e \otimes p_f$$
It remains to notice that the mappings \((b, c) \mapsto (b \triangleleft x^{-1}, c \triangleleft x^{-1}), (e, f) \mapsto (e \triangleleft x, f \triangleleft x)\) give a bijective correspondence between the sets \(\{(b, c) | bc = a\}\) and \(\{(e, f) | ef = a \triangleleft x^{-1}\}\) as the action \('\triangleleft'\) is by group automorphisms.

Below we will write an extension datum \(\{\sigma, \tau, \triangleleft\}\) when \(\triangleright\) is trivial. We will need explicit formulas for coalgebra structure mappings on \(H\) and \(H^*\) expressed in terms of their datum. These are the duals of the algebra structures (1.2) and (1.6), and follow from \([16, (4.5)]\).

**Proposition 1.3.** Let \(H\) and \(H^*\) be defined by a datum \(\{\sigma, \tau, \triangleleft\}\). The coalgebra structure of \(H\) and \(H^*\) is given by the mappings

\[
\Delta_H(fx) = \sum_{a,b \in G} \tau(x, a, b)f_1p_a\bar{x} \otimes f_2p_b\bar{x},
\]
\[
\epsilon_H(fx) = f(1_G).
\]

\[
\Delta_{H^*}(ag) = \sum_{x,y \in F} \sigma(x, y, a)\bar{\sigma}_x g_1 \otimes (a \triangleleft y)p_y g_2,
\]
\[
\epsilon_{H^*}(ag) = g(1_F),
\]

where \(f \in \mathbb{k}^G, g \in \mathbb{k}^F\).

For discussion of cohomology of abelian extensions we introduce the subgroup \(\text{Map}(F^n \times G^m, \mathbb{k}^\bullet)\) of \(\text{Fun}(F^n \times G^m, \mathbb{k}^\bullet)\) of normalized \(n + m\)-dimensional cochains, i.e. functions satisfying \(f(x_1, \ldots, x_n, a_1, \ldots, a_m) = 1\) if at least one component of \((x_1, \ldots, x_n, a_1, \ldots, a_m)\) is the identity. Suppose \(F\) acts on \(G\) via \(\triangleleft\). We extend this action to \(\text{Map}(F^n \times G^m, \mathbb{k}^\bullet)\) by the rule

\[
y.f(x_1, \ldots, x_n, a_1, \ldots, a_m) = f(x_1, \ldots, x_n, a_1 \triangleleft y, \ldots, a_m \triangleleft y).
\]

Identifying \(\text{Map}(F^n \times G^m, \mathbb{k}^\bullet)\) with either \(\text{Map}(F^n, (\mathbb{k}G^m)^\bullet)\) or \(\text{Map}(G^m, (\mathbb{k}^F)^\bullet)\) (see \([11]\)) we denote by \(\delta_F, \delta_G\), respectively, the standard differentials of group cohomology. Finally we state conditions for equivalence \([16, 3.4]\) of two extensions in the form needed below. They are a particular case of\([16, 5.2]\).

**Lemma 1.4.** Two extensions \(H\) and \(H'\) defined by data \(\{\sigma, \tau, \triangleleft\}\) and \(\{\sigma', \tau', \triangleleft'\}\) are equivalent if and only if \(\triangleleft = \triangleleft'\) and there exists \(\zeta \in \text{Map}(F \times G, \mathbb{k}^\bullet)\) satisfying

\[
\sigma' = \sigma \delta_F \zeta^{-1} \text{ and } \tau' = \tau \delta_G \zeta
\]

If so, an isomorphism \(\psi : H \rightarrow H'\) defined by \(\psi(f\bar{x}) = f\zeta(x)\bar{x}, f \in \mathbb{k}^G, x \in F\) carries out the equivalence.
1.4. **Cohomology Groups** $H^2(kF, k^G, \triangleleft)$. We describe in some detail cohomology theory of abelian extensions in the special case studied below. In the rest of the paper we consider cocentral extensions (A) satisfying the condition

(1.17) \[ H^2(F, (k^G)^*, \triangleleft) = \{1\} \] for every action $\triangleleft$.

We observe a simple

**Lemma 1.5.** Under the assumption (1.17) every extension $H(\sigma, \tau, \triangleleft)$ is equivalent to an extension $H(1, \tau', \triangleleft)$

**Proof:** The condition (1.17) means $\sigma = \delta_F \zeta, \zeta \in \text{Map}(F \times G, k^*)$. Then by Lemma 1.4 the mapping $\psi : H(\sigma, \tau, \triangleleft) \to H(1, \tau', \triangleleft), \psi(f \tau) = f \zeta(x) \tau, f \in k^G, x \in F$ with $\tau' = \tau \delta_G \zeta$ is the required equivalence. \(\Box\)

Below we will write $H = H(\tau, \triangleleft)$ for an extension with a datum $\{\sigma, \tau, \triangleleft\}$ and $\sigma$ trivial. We let $\text{Ext}(kF, k^G)$ stand for the set of equivalence classes of extensions with fixed action $\triangleleft$.

Cocentral extensions satisfying (1.17) have been studied in [11]. It is shown there [11, 4.4] that the standard second cohomology group of abelian extensions [7] coincides with the one in the next definition.

**Definition 1.6.** We let $Z^2_{c}(kF, k^G, \triangleleft)$ denote the subgroup of all elements $\tau$ of $Z^2(G, (k^F)^*, \text{id})$ satisfying $\delta_F(\tau) = \epsilon$. We let $B^2_{c}(kF, k^G, \triangleleft)$ stand for the subgroup of 2-cocycles $\delta_G \eta, \eta \in \text{Map}(F \times G, k^*)$ satisfying $\delta_F \eta = 1$. We define the second degree Hopf cohomology group by

$$H^2_{c}(kF, k^G, \triangleleft) = Z^2_{c}(kF, k^G, \triangleleft)/B^2_{c}(kF, k^G, \triangleleft).$$

Explicitly both conditions $\delta_F \tau = \epsilon$ and $\delta_F \eta = \epsilon$ are expressed by:

\begin{align*}
\tau(xy) &= \tau(x) (x. \tau(y)) \\
\eta(xy) &= \eta(x) (x. \eta(y))
\end{align*}

for all $x, y \in F$.

We call elements of $Z^2_{c}(kF, k^G, \triangleleft)$ and $B^2_{c}(kF, k^G, \triangleleft)$ Hopf 2-cocycles and 2-coboundaries, respectively. We will use abbreviated symbols $Z^2_{c}(kF, k^G, \triangleleft), B^2_{c}(kF, k^G, \triangleleft)$, etc. for $Z^2(\triangleleft), B^2(\triangleleft)$, etc when the groups $G$ and $F$ are fixed. The restriction $B^2(G, (k^F)^*) \cap Z^2(\triangleleft)$ of the group of coboundaries to $Z^2(\triangleleft)$ will be denoted by $B^2_{cc}(\triangleleft)$. As $B^2_{cc}(\triangleleft) \subseteq B^2(\triangleleft)$ we can form the subgroup $H^2_{cc} = B^2_{cc}(\triangleleft)/B^2(\triangleleft)$ of $H^2(\triangleleft)$. Explicitly,

$$H^2_{cc}(kF, k^G, \triangleleft) := \{\delta_G \eta B^2_{c}(\triangleleft)|\eta \in \text{Map}(F \times G, k^*) \text{ with } \delta_F(\delta_G \eta) = 1\}.$$
Lemma 1.7. If \( F \) is abelian, then groups \( Z^2(F,\langle \cdot \rangle) \), \( B^2_0(\langle \cdot \rangle) \), and \( B^2_0(\langle \cdot \rangle) \) are \( F \)-invariant.

Proof: Suffices to show that for any \( f \in \text{Map}(F \times G^m, k^*) \) and \( g \in \text{Map}(F^n \times G, k^*) \) there holds
\[
(1.20) \quad x.\delta_F f = \delta_F(x.f),
\]
\[
(1.21) \quad x.\delta_G g = \delta_G(x.g)
\]
For, setting \( m = 1, 2, f = \eta, \tau \) and \( n = 1, g = \eta \) in (1.20) and (1.21), respectively we get our statement.

(1.21) is immediate from definitions in view of \( G \) acting trivially on \( F \). To show (1.20) we calculate
\[
(x.\delta_F f)(y, z, a_1, \ldots, a_m) = (\delta_F f)(y, z, a_1 \triangleleft x, \ldots, a_m \triangleleft x) =
\]
\[
f(y, a_1 \triangleleft x, \ldots, a_m \triangleleft x)(y.f)(z, a_1 \triangleleft x, \ldots, a_m \triangleleft x)
\]
\[
f(yz, a_1 \triangleleft x, \ldots, a_m \triangleleft x)^{-1} = f(y, a_1 \triangleleft x, \ldots, a_m \triangleleft x)
\]
\[
(xy.f)(z, a_1 x, \ldots, a_m f(y, a_1 \triangleleft x, \ldots, a_m \triangleleft x)^{-1}
\]
Switching around \( x \) and \( y \) in the middle term we get exactly \( \delta_F(x.f) \).

\[\square\]

2. Structure of \( H^2_c(\mathbb{k}C_p, \mathbb{k}G, \prec) \)

Unless stated otherwise \( G \) is a \( p \)-group and \( F = C_p \). The group \( C_p \triangleleft G \) is a \( p \)-group as well, hence nilpotent. As \( G \) has index \( p \) in \( C_p \triangleleft G \), \( G \) is normal in \( C_p \triangleleft G \). By Lemma 1.2(1) the action \( \triangleright \) is trivial. In addition, as \( \mathbb{k}^* \) is a divisible group the group \( H^2(C_p, (\mathbb{k}G)^*), \prec \) vanishes by e.g. [11, 4.4]. Thus the results of the preceding section are applicable. We note a simple fact.

Lemma 2.1. Let \( \tau \in Z^2(G, (\mathbb{k}F)^*) \). Then for every \( x \in C_p \) \( \tau(x) \) is a 2-cocycle for \( G \) with coefficients in \( \mathbb{k}^* \) with the trivial action of \( G \) on \( \mathbb{k}^* \).

Proof: The 2-cocycle condition for the trivial action is
\[
(2.1) \quad \tau(a, bc)\tau(b, c) = \tau(ab, c)\tau(a, b).
\]
Expanding both sides of the above equality in the basis \( \{p_x\} \) and equating coefficients of \( p_x \) proves the assertion. \[\square\]

Consider group \( F \) acting on an abelian group \( A \), written multiplicatively, by group automorphisms. Let \( ZF \) be the group algebra of \( F \) over \( \mathbb{Z} \). \( ZF \) acts on \( A \) via
\[
(\sum c_i x_i).a = \prod x_i.(a^{c_i}), \quad c_i \in \mathbb{Z}, \quad x_i \in F.
\]
For $F = C_p$ pick a generator $t$ of $C_p$ and set $\phi_i = 1 + t + \cdots + t^{i-1}$, $i = 1, \ldots, p$. Choose $\tau \in Z^2(G, (k^C)^*)$ and expand $\tau$ in terms of the standard basis $p_i$ for $k^C$, $\tau = \sum \tau(t^i)p_i$ with $\tau(t^i) \in Z^2(G, k^*)$. An easy induction on $i$ shows that condition (1.18) implies

$$\tau(t^i) = \phi_i \tau(t), \text{ for all } i = 1, \ldots, p$$

For $i = p$ we have

$$\phi_p \tau(t) = 1$$

in view of $t^p = 1$ and $\tau(1) = 1$.

Let $M$ be a $ZC_p$-module. Following [12] we define the mapping $N : M \rightarrow M$ by $N(m) = \phi_p(t).m$. We denote by $M_N$ the kernel of $N$ in $M$. For $M = Z^2(G, k^*)$, $B^2(G, k^*)$ or $H^2(G, k^*)$ we write $Z^2_N(G, k^*)$ for $Z^2(G, k^*)_N$ and similarly for the other groups. We abbreviate $Z^2_N(G, k^*)$ to $Z^2_N(\langle \rangle)$ and likewise for $B^2_N(G, k^*)$ and $H^2_N(G, k^*)$.

**Definition 2.2.** We call a 2-cocycle $s \in Z^2(G, k^*)$ admissible if $s$ satisfies the condition

$$\phi_p.s = 1$$

Thus by definition the set of all admissible cocycles is $Z^2_N(\langle \rangle)$. We note that $Z^2_N(\langle \rangle)$ is a subgroup of $Z^2(G, k^*)$ as $ZC_p$ acts by endomorphisms of $Z^2(G, k^*)$. We want to compare abelian groups $Z^2_\langle \rangle(\langle \rangle)$ and $Z^2_N(\langle \rangle)$. This is done via the mapping

$$\Theta : Z^2(G, (k^C)^*) \rightarrow Z^2(G, k^*), \Theta(\tau) = \tau(t).$$

**Lemma 2.3.** The mapping $\Theta$ induces a $C_p$-isomorphism between $Z^2_\langle \rangle(\langle \rangle)$ and $Z^2_N(\langle \rangle)$.

**Proof:** We begin with an obvious equality $x.(\tau(y)) = (x.\tau)(y)$. Taking $y = t$ we get $\Theta(x.\tau) = x.\Theta(\tau)$, that is $C_p$-linearity of $\Theta$. The relations (2.2) show that $\Theta$ is monic. It remains to establish that $\Theta$ is epic.

Suppose $s$ is an admissible 2-cocycle of $G$ in $k^*$. Define $\tau : G \times G \rightarrow (k^C)^*$ by setting $\tau(t^i) = \phi_i(t).s$, $1 \leq i \leq p$. The proof will be complete if we demonstrate that $\tau$ satisfies (1.18).

For any $i, j \leq p$ we have

$$\tau(t^i)(t^i.\tau(t^j)) = (\phi_i(t).s)(t^i.\phi_j(t).s) = (\phi_i(t) + t^i \phi_j(t)).s$$

One sees easily that $\phi_i(t) + t^i \phi_j(t) = \sum_{k=0}^{i+j-1} t^k$. Hence if $i+j < p$ we have

$$\phi_i(t) + t^i \phi_j(t) = \phi_{i+j}(t)$$

and so $\tau(t^i)(t^i.\tau(t^j)) = \tau(t^{i+j})$. If $i+j = p+m$
with \( m \geq 0 \), then \( \sum_{k=0}^{p+m-1} t^k = \phi_p(t) + t^p(1 + \cdots + t^{m-1}) \) which implies
\[
( \sum_{k=0}^{p+m-1} t^k ).s = \phi_p(t).s \cdot t^p \phi_m(t).s = \phi_m(t).s = \tau(t^{i+j}) \text{ by (2.4)} \text{ and as } t^p = 1.
\]

The next step is to describe structure of \( H^2_{cc}(<) \). We need some preliminaries. First, we write \( x.f \) for the left action of \( C_k \) on \( k^G \) dual to \( < \) as in (1.3). Since \( \hat{G} \) is the group of grouplikes of \( k^G \), \( \hat{G} \) is \( C_p \)-stable by Lemma 1.2(2). Further, we use \( \delta \) for the differential on the group of 1-cochains of \( G \) in \( k^\bullet \). We also note \( B^2_N(<) = B^2(G, k^\bullet) \cap Z^2_N(<) \). By (2.4) \( \delta f \in B^2_N(<) \) iff \( \phi_p(t).\delta f = \delta \chi \) which, in view of \( \delta \) being \( C_p \)-linear, is the same as \( \delta(\phi_p(t).f) = 1 \). Since \( (\delta f)(a,b) = f(a)f(b)f(ab)^{-1} \), \text{Ker} \( \delta \) consists of characters of \( G \), whence \( \delta f \in B^2_N(<) \) iff \( \phi_p(t).f \) is a character of \( G \). Say \( \chi = \phi_p(t).f \in \hat{G} \). Then as \( t\phi_p(t) = \phi_p(t) \), \( \chi \) is a fixed point of the \( C_p \)-module \( \hat{G} \). Letting \( \hat{G}^{c_p} \) stand for the set of fixed points in \( \hat{G} \) we have by [12, IV.7.1] an isomorphism \( H^2(C_p, \hat{G}, \bullet) \approx \hat{G}^{c_p}/N(\hat{G}) \).

We connect \( B^2_N(<) \) to \( H^2(C_p, \hat{G}) \) via the homomorphism
\[
(2.5) \quad \Phi : B^2_N(<) \to H^2(C_p, \hat{G}, \bullet), \delta f \mapsto (\phi_p.f)N(\hat{G})
\]

**Lemma 2.4.** The following properties holds

- (i) \( \Theta(B^2_N(<)) = B^2_N(<) \),
- (ii) \( \Theta(B^2(<)) = \text{Ker} \Phi \),
- (iii) \( B^2_N(<)/\text{Ker} \Phi \simeq H^2(C_p, \hat{G}, \bullet) \),
- (iv) \( H^2_{cc}(<) \simeq H^2(C_p, \hat{G}, \bullet) \).

**Proof:** First we show that \( \Phi \) is well-defined. For, \( \delta f = \delta g \) iff \( fg^{-1} = \chi \in \hat{G} \), hence
\[
\Phi(\delta f) = (\phi_p.f)N(\hat{G}) = (\phi_p.g\chi)N(\hat{G}) = (\phi_p.g)N(\hat{G}) = \Phi(\delta g)
\]

(i) Take some \( \delta(\eta) \in B^2_N(<) \). Evidently for every \( x \in C_p (^x) \delta(\eta)(x) = \delta(\eta(x)) \), hence \( \Theta(\delta(\eta)) = \delta(\eta(t)) \) is a coboundary, and \( \phi_p(\delta(\eta) = 1 \) by (2.3), whence \( \Theta(\delta(\eta)) \in B^2_N(<) \). Conversely, pick \( \delta f \in B^2_N(<) \) and define \( \omega = \sum_{i=1}^{p} (\phi_i.f)p_{i^\ell} \). The argument of Lemma 2.3 shows \( \omega \) lies in \( Z^2_N(<) \). Set \( \eta = \sum_{i=1}^{p} (\phi_i.f)p_{i^\ell} \). Using \(^x\) again we derive
\[
\delta G\eta = \sum_{i=1}^{p} (\phi_i.\delta f)p_{i^\ell} = \omega,
\]

hence \( \delta G\eta \in B^2_{cc}(<) \). Clearly \( \Theta(\delta G\eta) = \delta f \).
(ii) The argument of Lemma 2.3 is applicable to 1-cocycles satisfying (1.19). It shows that \( \eta \) satisfies (1.19) iff
\[
\eta(t^i) = \phi_i \eta(t)
\]
For \( i = p \) we get \( \phi_p, \eta(t) = \epsilon \), hence the calculation
\[
\Phi(\Theta(\delta_G \eta)) = \Phi(\delta(\eta(t))) = (\phi_p, \eta(t))N(\hat{G}) = N(\hat{G}).
\]
gives one direction. Conversely, \( \Phi(\delta f) \in N(\hat{G}) \) means \( \phi_p, f = \phi_p, \chi \)
which implies \( \phi_p, f \chi^{-1} = \epsilon \). Set \( g = f \chi^{-1} \) and define 1-cocycle \( \eta_g = \sum_{i=1}^p (\phi_i, g) p_i \). Since \( \phi_p, g = \epsilon \), \( g \) satisfies (1.19), whence \( \delta G \eta_g \in B^2_G(\chi) \).
As \( (\delta G \eta_g)(t) = \delta g = \delta f \) by construction, \( \Theta(\delta G \eta_g) = \delta f \).

(iii) We must show that \( \Phi \) is onto. For every character \( \chi \) in \( \hat{G}^C_p \) we want to construct an \( f : G \to \mathbb{k}^* \) satisfying \( \phi_p, f = \chi \). To this end we consider splitting of \( G \) into the orbits under the action of \( C_p \). Since every orbit is either regular, or a fixed point under the action by \( C_p \). Thus every orbit is either regular or a fixed point we have
\[
G = \bigcup_{i=1}^r \{ g_i \triangleleft t^i, \ldots, g_i \triangleleft t^{p-1} \} \cup G^C_p
\]
For every \( s \in G^C_p \) we pick a \( \rho_s \in \mathbb{k} \) satisfying \( \rho_s^p = \chi(s) \). We define \( f \) by the rule
\[
f(g_i) = \chi(g_i), \quad f(g_i \triangleleft t^j) = 1 \quad \text{for all} \quad j \neq 1 \quad \text{and all} \quad i = 1, \ldots, r, \quad \text{and} \quad f(s) = \rho_s \quad \text{for every} \quad s \in G^C_p
\]
By definition \( (\phi_p, f)(g) = \prod_{i=0}^{p-1} f(g \triangleleft t^i) \). Therefore \( (\phi_p, f)(s) = \rho_s^p = \chi(s) \) for every \( s \in G^C_p \). If \( g = g_i \triangleleft t^j \) for some \( i, j \), then a calculation \( (\phi_p, f)(g) = f(g_i) = \chi(g_i) = \chi(g_i \triangleleft t^j) = \chi(g) \), which uses the fact that \( \chi \) is a fixed point under the action by \( C_p \), completes the proof.

(iv) follows immediately from \( H^2_{cc}(\chi) = B^2_{cc}/B^2_c(\chi) \) and parts (i)-(iii). \( \square \)

**Corollary 2.5.** There is a \( C_p \) isomorphism \( H^2_c(\chi) \cong Z^2_N(\chi)/\ker \Phi \).

**Proof:** Combining Lemmas 2.3 and 2.4 with the natural epimorphism \( Z^2_N(\chi) \to Z^2_N(\chi)/\ker \Phi \) proves the Corollary. \( \square \)

We proceed to the main result of the section.

**Proposition 2.6.** Suppose \( G \) is a finite abelian \( p \)-group. If \( p \) is odd, or \( p = 2 \) and either \( C_2 \)-action is trivial, or \( G \) is an elementary \( 2 \)-group, there exists a \( C_p \)-isomorphism
\[
H^2_c(\chi) \cong H^2(C_p, \hat{G}, \bullet) \times H^2_N(G, \mathbb{k}^*)
\]

**Proof:** (1) First we take up the odd case. By the preceding Corollary we need to decompose \( Z^2_N(\chi)/\ker \Phi \). We note that for any \( p \) there is a
group splitting $Z^2(G, \mathbb{k}^*) = B^2(G, \mathbb{k}^*) \times H^2(G, \mathbb{k}^*)$ due to the fact that the group of 1-cocycles $\mathbb{k}^*G$ is injective, and hence so is $B^2(G, \mathbb{k}^*)$. We aim at finding a $C_p$-invariant complement to $B^2(G, \mathbb{k}^*)$. To this end we recall a well-known isomorphism $a : H^2(G, \mathbb{k}^*) \rightarrow \text{Alt}(G)$, see e.g. [23, §2.3]. There $\text{Alt}(G)$ is the group of all bimultiplicative alternating functions

$\beta : G \times G \rightarrow \mathbb{k}^*$, $\beta(ab, c) = \beta(a, c)\beta(b, c)$, and $\beta(a, a) = 1$ for all $a \in G$. For future applications we outline the construction of $a$. Namely, $a$ is the antisymmetrization mapping sending $z \in Z^2(G, \mathbb{k}^*)$ to $a(z)$ defined by $a(z)(a, b) = z(a, b)z^{-1}(b, a)$. One can check that $a$ is bimultiplicative (cf. [23, (10)]) and it is immediate that $a$ is $C_p$-linear. Another verification gives $\text{im } a = \text{Alt}(G)$ and, moreover, $\ker a = B^2(G, \mathbb{k}^*)$, see [23, Thm.2.2]. Thus we obtain a $C_p$-isomorphism $H^2(G, \mathbb{k}^*) \cong \text{Alt}(G)$.

For every $\beta = a(z)$ a simple calculation gives $a(\beta) = \beta^2$. Since elements of $\text{Alt}(G)$ are bimultiplicative mappings, they have orders dividing the exponent of $G$. Thus $a(\beta) \neq 1$ for all $\beta \in \text{Alt}(G)$. It follows $B^2(G, \mathbb{k}^*) \cap \text{Alt}(G) = \{1\}$. We arrive at a splitting of abelian groups

$$Z^2(G, \mathbb{k}^*) = B^2(G, \mathbb{k}^*) \times \text{Alt}(G)$$

But now both subgroups $B^2(G, \mathbb{k}^*)$ and $\text{Alt}(G)$ are $C_p$-invariant hence there holds $Z^2_N(G, \mathbb{k}^*) = B^2_N(G, \mathbb{k}^*) \times \text{Alt}_N(G)$ which, in view of $\text{Alt}(G) = H^2(G, \mathbb{k}^*)$, is the same as

$$Z^2_N(a) = B^2_N(a) \times H^2_N(G, \mathbb{k}^*).$$

Now part (iii) of Lemma 2.4 completes the proof of part (1).

(2) Here we prove the second claim of the Proposition. We decompose $G$ into a product of cyclic groups $\langle x_i \rangle$, $1 \leq i \leq m$. For every $\alpha \in \text{Alt}(G)$ we define $s_\alpha \in Z^2(G, \mathbb{k}^*)$ via

$$s_\alpha(x_i, x_j) = \begin{cases} \alpha(x_i, x_j), & \text{if } i \leq j \\ 1, & \text{else.} \end{cases}$$

The set $S = \{s_\alpha | \alpha \in \text{Alt}(G)\}$ is a subgroup. One can see easily that $a(s_\alpha) = \alpha$, hence $S$ is isomorphic to $\text{Alt}(G)$ under $a$. Let us write $G_{(p)}$ for the set of elements of order $p$. We observe that $Z^2_N(\text{triv}) = Z^2(\text{triv})_{(2)}$, hence $S_{(2)} \subset Z^2_N(\text{triv})$. For every $z \in Z^2_N(\text{triv}), a(z) \in \text{Alt}(G)_{(2)}$, and therefore $a(z) = a(s)$ for some $s \in S_{(2)}$. We have $zs^{-1} \in B^2(G, \mathbb{k}^*)$, and, as $zs^{-1}$ has order 2, $zs^{-1} \in B^2_N(\text{triv})$. Thus $Z^2_N(\text{triv}) = B^2_N(\text{triv}) \times S_{(2)}$ which implies (2.7) as $S_{(2)} \cong \text{Alt}(G)_{(2)} \cong H^2_N(\text{triv})$.

(3) We prove the last claim of the Proposition. Below $G$ is an elementary 2-group, and action of $C_2$ is nontrivial. First we establish an intermediate result, namely
**Lemma 2.7.** If action $\triangleleft$ is nontrivial, then $Z^2_N(\triangleleft)$ is a nonsplit extension of $\text{Alt}_N(G)$ by $B^2_N(\triangleleft)$.

**Proof:** This will be carried out in steps.

(i) We aim at finding a basis for $\text{Alt}_N(G)$. We begin by noting that as $\text{Alt}(G)$ has exponent 2, $\text{Alt}_N(G)$ is the set of all fixed points in $\text{Alt}(G)$. Put $R = \mathbb{Z}_2C_2$. One can see easily that $R$-module $G$ decomposes as

$$G = R_1 \times \cdots \times R_m \times G_0$$

where $R_i \simeq R$ as a right $C_2$-module, and $G_0 = G^{C_2}$. Denote by $t$ the generator of $C_2$. For each $i$ let $\{x_{2i-1}, x_{2i}\}$ be a basis of $R_i$ such that $x_{2i-1} \triangleleft t = x_{2i}$. We also fix a basis $\{x_{2m+1}, \ldots, x_n\}$ of $G_0$.

We associate to every subset $\{i, j\}$ the bilinear form $\alpha_{ij}$ by setting

$$\alpha_{ij}(x_i, x_j) = \alpha_{ij}(x_j, x_i) = -1, \text{ and } \alpha_{ij}(x_k, x_i) = 1 \text{ for any } \{k, l\} \neq \{i, j\}.$$ 

The set $\{\alpha_{ij}\}$ forms a basis of $\text{Alt}(G)$. One can check easily that $t$ acts on basic elements as follows

$$t.\alpha_{ij} = \alpha_{kl} \text{ if and only if } \{x_i, x_j\} \triangleleft t := \{x_i \triangleleft t, x_j \triangleleft t\} = \{x_k, x_l\}. $$

Recall the element $\phi_2 = 1 + t \in \mathbb{Z}C_2$. We define forms $\beta_{ij}$ via

$$\beta_{ij} = \phi_2.\alpha_{ij} \text{ if } t.\alpha_{ij} \neq \alpha_{ij}, \text{ and } \beta_{ij} = \alpha_{ij}, \text{ otherwise.}$$

The label $ij$ on $\beta_{ij}$ is not unique as $\beta_{ij} = \beta_{kl}$ whenever $\{x_i, x_j\} \triangleleft t = \{x_k, x_l\}$. Of the two sets $\{i, j\}$ and $\{k, l\}$ labeling $\beta_{ij}$ we agree to use the one with the smallest element, and call such minimal. We claim:

$$\beta_{ij} \text{ the one with the smallest element, and call such minimal. We claim:}$$

(ii) We want to show $\text{Alt}_N(G)$ is an epimorphic image of $Z^2_N(\triangleleft)$.

The restriction $\hat{\alpha}^* \otimes \hat{\alpha}^*$ of $\hat{\alpha}$ to $Z^2_N(\triangleleft)$ induces a $C_2$-homomorphism $Z^2_N(\triangleleft) \xrightarrow{\hat{\alpha}^*} \text{Alt}_N(G)$. We have ker $\hat{\alpha}^* = B^2(G, k^*) \cap Z^2_N(\triangleleft) = B^2_N(\triangleleft)$. First we show $\phi_2.\text{Alt}(G) \subset \text{im} \hat{\alpha}^*$. For, if $\beta = \phi_2.\alpha$, pick an $s \in Z^2(G, k^*)$ with $\hat{\alpha}(s) = \alpha$. Then $(t-1).s \in Z^2_N(\triangleleft)$, and $\hat{\alpha}((t-1).s) = (t-1).\hat{\alpha}(s) = (t-1).\alpha = \phi_2.\alpha = \beta$, as $\alpha^2 = 1$, which gives the inclusion.

By step (i) and definition (2.11) it remains to show that all fixed points $\alpha_{ij}$ lie in $\text{im} \hat{\alpha}^*$. By formula (2.10) $\alpha_{ij}$ is a fixed point if and only if either (a) $\{i, j\} \subset \{2m+1, \ldots, n\}$ or (b) $\{i, j\} = \{2k-1, 2k\}$ for some $k, 1 \leq k \leq m$. Below we find it convenient to write $s_{ij}$ for $s_{\alpha_{ij}}$. 

\begin{thebibliography}{99}

\end{thebibliography}
Consider case (a). We claim \( s_{i,j} \) is a fixed point. For, \( t.s_{i,j} \) is bi-
multiplicative, hence is determined by its values at \((x_k, x_l)\). It is im-
mediate that \( t.s_{i,j}(x_k, x_l) = s_{i,j}(x_k, x_l) \) for all \((x_k, x_l)\), whence the as-
sertion. Since \( s_{i,j}^2 = 1 \) for all \( i, j \), \( \phi_2.s_{i,j} = 1 \), hence \( s_{i,j} \in \mathbb{Z}_N^2(\langle \rangle) \). As
\( g(s_{i,j}) = \alpha_{ij} \), this case is done.

We take up (b). Say \( z = s_{2i-1,2i} \) for some \( i, 1 \leq i \leq m \). An easy
verification gives \( \phi_2.z = \alpha_{2i-12i} \neq 1 \). Thus \( z \notin \mathbb{Z}_N^2(\langle \rangle) \). To prove
(ii) we need to find a coboundary \( \delta g \) such that \( z\delta g \in \mathbb{Z}_N^2(\langle \rangle) \). Since
\( g(\alpha_{2i-12i}) = 1, \alpha_{2i-12i} = \delta f_i \) for some \( f_i : G \to \mathbb{k}^* \). Put \( G_i \) for
the subgroup of \( G \) generated by all \( x_j, j \neq 2i-1, 2i \). We assert that one
choice is the function \( f_i \) defined by

\[
(2.13) \quad f_i(x_{2i-1}^{j_1} x_{2i}^{j_2} x') = (-1)^{j_1+j_2+j_1j_2} \text{ for all } x' \in G_i
\]

For, on the other hand it is immediate that for any \( x', x'' \in G_i \)
\[
\alpha_{2i-12i}(x_{2i-1}^{j_1} x_{2i}^{j_2} x', x_{2i-1}^{k_1} x_{2i}^{k_2} x'') = (-1)^{j_1k_2+j_2k_1}
\]

On the other hand the definitions of \( f_i \) and differential \( \delta \) give
\[
\delta f_i(x_{2i-1}^{j_1} x_{2i}^{j_2} x', x_{2i-1}^{k_1} x_{2i}^{k_2} x'') = (-1)^{j_1+k_1+j_2+k_2} (-1)^{j_1+k_1+j_2} = (-1)^{j_1+j_2+j_1j_2}
\]
Define the function \( g_i : G \to \mathbb{k}^* \) by \( g_i(x_{2i-1}^{j_1} x_{2i}^{j_2} x') = i^{j_1+j_2+j_1j_2} \) where
\( i^2 = -1 \). One can check easily the equalities \( f_i^2 = 1 \) and \( t.g_i = g_i, g_i^2 = f_i \). Hence we have \( f_i(\phi_2.g_i) = f_i g_i^2 = f_i^2 = 1 \), and then a calculation
\[
\phi_2(z\delta g_i) = (\phi_2.z)(\phi_2.\delta g_i) = \delta f_i \cdot \delta(\phi_2.g_i) = \delta(f_i(\phi_2.g_i)) = 1
\]
completes the proof of (ii).

(iii) Suppose \( \mathbb{Z}_N^2(\langle \rangle) = B_N^2(\langle \rangle) \times C \) where \( C \) is a \( C_2 \)-invariant subgroup.
Then \( C \) is mapped isomorphically on \( \text{Alt}_N(G) \) under \( g \) and so there is
a unique \( z \in C \) such that \( g(z) = \alpha_{12} \). Since \( g(s_{1,2}) = \alpha_{12} \), \( z = s_{1,2}\delta g \)
for some \( g : G \to \mathbb{k}^* \). Further, as \( \alpha_{12} \) is a fixed point \( g(t.z) = \alpha_{12} \)
as well, hence \( t.z = z \). In addition, since \( \text{Alt}(G) \) is an elementary
2-group, \( 1 = z^2 = (s_{1,2}\delta g)^2 = (\delta g)^2 = \delta(g^2) \). It follows that \( g^2 \) is a
character of \( G \). Moreover, \( t.z = z \) is equivalent to \( t.s_{1,2}(t.\delta g) = s_{1,2}\delta g \)
which in turn gives \( s_{1,2}(t.s_{1,2}(t.\delta g) = \delta g \). As \( \phi_2.s_{1,2} = \alpha_{12} = \delta f_1 \)
we have \( \delta f_1(t.\delta g) = \delta g \) which implies \( \delta f_1 = \delta g(t.\delta g) \) on the account of \( (\delta g)^2 = \delta(g^2) = 1 \) as \( g^2 \) is a character. Equivalently we have the equality

\[
(2.14) \quad f_1 = g \cdot (t.g) \cdot \chi \text{ for some } \chi \in \hat{G}.
\]
Noting that \( f_1 \) is defined up to a character of \( G \) we can assume that
\( f_1(x_1) = 1 = f_1(x_2) \) and \( f_1(x_1x_2) = -1 \). For, \( f_1 \) is defined as any

function satisfying $\delta f_i = \alpha_{12}$. As $\delta(f_1 \chi) = \delta f_1$ for any $\chi \in \hat{G}$, $f_1$ can be modified by any $\chi$. By (2.13) $f_1(x_j) = -1 = f_1(x_1x_2)$, $j = 1, 2$ so we can take $\chi$ such that $\chi(x_1) = \chi(x_2) = -1$. The equality (2.14) implies that for some $\chi \in \hat{G}$ there holds

\[
(*) \quad 1 = f_1(x_j) = g(x_1)g(x_2)\chi(x_j), \quad j = 1, 2, \text{ and}
\]

\[
(**) \quad -1 = f_1(x_1x_2) = g(x_1x_2)^2\chi(x_1x_2)
\]

as $t$ swaps $x_1$ and $x_2$. Since $g^2$ is a character, $g^2(a) = \pm 1$ for every $a \in G$. It follows that $g(x_1) = \iota^m$ and $g(x_2) = \iota^k$ for some $0 \leq m, k \leq 3$. Then equation (*) gives $1 = \iota^{m+k}\chi(x_j)$. This equality shows that $\chi(x_1) = \chi(x_2)$ and $m + k$ is even, because $\chi(a) = \pm 1$ for all $a$. Now (**), and the fact that $g^2$ is a character, gives $-1 = g^2(x_1)g^2(x_2)x_1x_2 = \iota^{2(m+k)}\iota^{-2(m+k)} = 1$, a contradiction. This completes the proof of the Lemma.

Finally we prove (3). Let $G$ be a group with a decomposition (2.9). Set $C$ to be the subgroup of $Z_N^2(<a>)$ generated by the set $B = B' \cup B'' \cup B'''$ where

\[
B' = \{\phi_2, s_{i,j} | \alpha_{ij} \text{ is not a fixed point, and } \{ij\} \text{ is minimal}\}
\]

\[
B'' = \{s_{i,j} | i < j \text{ and } \{i,j\} \subset \{2m+1, \ldots, n\}\}
\]

\[
B''' = \{s_{2i-1,2i} \delta g_i | i = 1, \ldots, m\}
\]

There $\delta g_i$ is chosen as in the proof of the case (ii) of Lemma 2.7. Passing on to $Z_N^2(<a>/\ker \Phi$ we denote by $\overline{B'_N(<a>)}$ and $\overline{C}$ images of these subgroups in $Z_N^2(<a>/\ker \Phi$. Pick a $v \in B$. If $v \in B' \cup B''$ then $v^2 = 1$ because the corresponding $s_{i,j}$ has order 2. For $v = s_{2i-1,2i} \delta g_i$, $v^2 = \delta g_i^2 = \delta f_i$. We know $t.f_i = f_i$ and $f_i^2 = 1$ and therefore $\phi_2.f_i = 1$, whence $\delta f_i \in \ker \Phi$ by definition (2.5). It follows that $\overline{v} = 1$ for all $\overline{v} \in \overline{B}$. Furthermore, by Lemma 2.7 the mapping $\overline{a}$ sends $\overline{B}$ to the basis (2.12) of Alt$_N(G)$. Therefore $\overline{C}$ is isomorphic to Alt$_N(G)$ at least as an abelian group and forms a complement to $\overline{B'_N(<a>)}$ in $Z_N^2(<a>/\ker \Phi$. Since Alt$_N(G)$ consists of fixed points the proof will be completed if we show the same for $\overline{C}$. The fact that $B' \cup B''$ consists of fixed points follows from $t.\phi_2 = \phi_2$ and the case (i) of Lemma 2.7. For an $s_{2i-1,2i} \delta g_i$, the equality $\phi_2.s_{2i-1,2i} = s_{2i-1,2i}(t.s_{2i-1,2i}) = \alpha_{2i-1,2i} = \delta f_i$ gives $t.s_{2i-1,2i} = s_{2i-1,2i} \delta f_i$. Since $\delta f_i \in \ker \Phi$ and $t \delta g_i = \delta g_i$ we see that $s_{2i-1,2i} \delta g_i$ is a fixed point in $Z_N^2(<a>/\ker \Phi$ which completes the proof. \qed
3. The Isomorphism Theorems

We begin with a general observation. Let $H$ be an extension of type (A). The mapping $\pi$ induces a $kF$-comodule structure $\rho_\pi$ on $H$ via

\[(3.1) \quad \rho_\pi : H \to H \otimes kF, \quad \rho_\pi(h) = h_1 \otimes \pi(h_2).\]

$H$ becomes an $F$-graded algebra with the graded components $H_f = \{ h \in H | \rho_\pi(h) = h \otimes f \}$. Let $\chi : kF \to H$ be a section of $kF$ in $H$. By definition $\chi$ is a convolution invertible $kF$-comodule mapping, that is

\[(3.2) \quad \rho_\pi(\chi(f)) = \chi(f) \otimes f, \quad \text{for every } f \in F.\]

Set $f = \chi(f)$. The next lemma is similar to [16, 3.4] or [17, 7.3.4].

**Lemma 3.1.** For every $f \in F$ there holds $H_f = kGf$.

**Proof:** By definition of components $H_1 = H^\text{coG}$ which equals to $kG$ by the definition of extension. By the equation (3.2) $\rho_\pi(f) = f \otimes f$, hence $kGf \subset H_f$. Since the containment holds for all $f$, the equalities $H = \bigoplus_{f \in F} H_f = \bigoplus_{f \in F} kGf$ force the equalities $H_f = kGf$ for all $f \in F$. $\square$

**Definition 3.2.** Given two $F$-graded algebras $H = \bigoplus H_f$ and $H' = \bigoplus H'_f$ and an automorphism $\alpha : F \to F$ we say that a linear mapping $\psi : H \to H'$ is an $\alpha$-graded morphism if $\psi(H_f) = H'_\alpha(f)$ for all $f \in F$.

**Lemma 3.3.** Suppose $H$ and $H'$ are two extensions of $kF$ by $kG$ and $\psi : H \to H'$ a Hopf isomorphism sending $kG$ to $kG$. Then $\psi$ is an $\alpha$-graded mapping for some $\alpha$.

**Proof:** Suppose $H$ and $H'$ are given by sequences

\[
\begin{align*}
kG & \xrightarrow{\iota} H \xrightarrow{\pi} kF, \quad \text{and} \quad kG & \xrightarrow{\iota'} H' \xrightarrow{\pi'} kF.
\end{align*}
\]

By definition of extension $\text{Ker } \pi = H(kG)^+$ and likewise $\text{Ker } \pi' = H'(kG)^+$. By assumption $\psi(kG) = kG$, hence $\psi$ induces a Hopf isomorphism $\alpha : H/H(kG)^+ \to H'/H'(kG)^+$. Replacing $H/H(kG)^+$ and $H'/H'(kG)^+$ by $kF$ we can treat $\alpha$ as a Hopf isomorphism $\alpha : kF \to kF$. $\alpha$ is in fact an automorphism of $F$. We arrive at a commutative diagram

\[
\begin{array}{ccc}
kG & \xrightarrow{\iota} & H \xrightarrow{\pi} kF \xrightarrow{\alpha} kF \\
\psi & & \downarrow \psi \quad \downarrow \alpha \\
kG & \xrightarrow{\iota'} & H' \xrightarrow{\pi'} kF
\end{array}
\]
Since $\psi$ is a coalgebra mapping for every $f \in F$ we have

$$\Delta_{H'}(\psi(\overline{f})) = (\psi \otimes \psi)\Delta_{H}(\overline{f}) = \psi((\overline{f})_1) \otimes \psi((\overline{f})_2),$$

hence

$$\rho_{\pi'}(\psi(\overline{f})) = \psi((\overline{f})_1) \otimes \pi'\psi((\overline{f})_2) = \psi((\overline{f})_1) \otimes \alpha\pi((\overline{f})_2)$$

On the other hand, applying $\psi \otimes \alpha$ to the equality

$$\rho_{\pi}(\overline{f}) = (\overline{f})_1 \otimes \pi((\overline{f})_2) = \overline{f} \otimes f$$

gives

$$\psi((\overline{f})_1) \otimes \alpha\pi((\overline{f})_2) = \psi(\overline{f}) \otimes \alpha(f)$$

whence we deduce $\rho_{\pi'}(\psi(\overline{f})) = \psi(\overline{f}) \otimes \alpha(f)$. Thus $\psi(\overline{f}) \in H'_{\alpha(f)}$ which shows the inclusion

$$\rho_{\pi}(\overline{f}) = \psi(\overline{f}) \otimes \alpha(f) \subseteq \psi(\overline{f}) \otimes \alpha(f)$$

Since both sides of the above inclusion have equal dimensions, the proof is complete.

From this point on $F = C_p$. Let $\triangleleft$ and $\triangleright$ be two actions of $C_p$ on $G$. We denote $(G, \triangleleft)$ and $(G, \triangleright)$ the corresponding $C_p$-modules and we use the notation ‘$\bullet$’ and ‘$\circ$’ for the actions of $C_p$ on $\mathbb{K}^G$ corresponding by (1.3) to $\triangleleft$ and $\triangleright$, respectively. We let $I(\triangleleft, \triangleright)$ denote the set of all automorphisms of $G$ intertwining actions $\triangleleft$ and $\triangleright$, that is automorphisms $\lambda : G \to G$ satisfying

$$(a \triangleleft x)\lambda = a\lambda \triangleright x, \quad a \in G, \quad x \in C_p$$

We make every $\lambda$ act on functions $\tau : C_p \times G^2 \to \mathbb{K}^{C_p}$ by

$$(\tau.\lambda)(x, a, b) = \tau(x, a\lambda^{-1}, b\lambda^{-1}).$$

**Lemma 3.4.** (i) The group $Z^2(G, (\mathbb{K}^{C_p})^\bullet)$ is invariant under the action induced by any automorphism of $G$.

(ii) A $C_p$-isomorphism $\lambda : (G, \triangleleft) \to (G, \triangleright)$ induces $C_p$-isomorphisms between the groups $Z^2_c(\triangleleft), B^2_c(\triangleleft), H^2_c(\triangleleft)$ and $Z^2_c(\triangleright), B^2_c(\triangleright), H^2_c(\triangleright)$, respectively.

**Proof:** (i) is immediate.

(ii) We must check condition (1.18) for $\tau.\lambda$ and $\mathbb{Z}C_p$-linearity of the induced map. First we note $\lambda^{-1}$ is a $C_p$-isomorphism between $(G, \triangleright)$ and $(G, \triangleleft)$, as one can check readily. For, set $b = a\lambda$ in (3.3). Then we have $(b\lambda^{-1} \triangleleft x)\lambda = (b \triangleright x)$ hence $b\lambda^{-1} \triangleleft x = (b \triangleright x)\lambda^{-1}$.
Next we verify (1.18) and $C_p$-linearity in a single calculation

\[
(\tau.\lambda)(xy)(a, b) = \tau(xy, a\lambda^{-1}, b\lambda^{-1})
= \tau(x, a\lambda^{-1}, b\lambda^{-1})(x \bullet \tau(y, a\lambda^{-1}, b\lambda^{-1}))
= \tau(x, a\lambda^{-1}, b\lambda^{-1})\tau(y, a\lambda^{-1} < x, b\lambda^{-1} < x)
= \tau(x, a\lambda^{-1}, b\lambda^{-1})\tau(y, (a \triangleleft x)\lambda^{-1}, (b \triangleleft x)\lambda^{-1})
= (\tau.\lambda)(x)(x \circ (\tau.\lambda)(y))(a, b).
\]

In the case of $B^2_2(\triangleleft)$, first one checks the equality

\[
(\delta_G \eta).\lambda = \delta_G(\eta.\lambda) \text{ for any } \eta : C_p \times G \to k^*.
\]

It remains to verify the condition (1.19) for $\eta.\lambda$. That is done similarly to the calculation in (ii). \qed

Let $(G, \triangleleft)$ be a $C_p$-module. We denote by $A(\triangleleft)$ the group of $C_p$-automorphisms of $(G, \triangleleft)$. By the above Lemma $Z^2_c(\triangleleft)$ is an $A(\triangleleft)$-module. Symmetrically, we introduce the group $A_p = \text{Aut}(C_p)$ of automorphisms of $C_p$. We define an action of $A_p$ on $\text{Map}(C_p \times G^2, k^*)$ via

\[
\tau.\alpha(x, a, b) = \tau(\alpha(x), a, b)
\]

We want to know the effect of this action on $Z^2_c(\triangleleft)$. Let $(G, \triangleleft)$ be a $C_p$-module. For $\alpha \in A_p$ we define a $C_p$-module $(G, \triangleleft')$ via

\[
a \triangleleft' x = a \triangleleft \alpha(x), \quad a \in G, \quad x \in C_p
\]

Similarly, an action $\cdot'$ of $C_p$ on $k^G$ can be twisted by $\alpha$ into $\cdot'^\alpha$ by

\[
x \cdot'^\alpha r = \alpha(x) \cdot r, \quad r \in k^G
\]

One can see easily that if $\cdot'$ and $\triangleleft'$ correspond to each other by (1.3), then so do $\cdot'^\alpha$ and $\triangleleft'^\alpha$.

**Lemma 3.5.** (i) If $\lambda \in I(\triangleleft, \triangleleft')$, then $\lambda \in I(\triangleleft', \triangleleft'^\alpha)$ for every $\alpha \in A_p$.

(ii) The mapping $\tau \mapsto \tau.\alpha$ induces an $A(\triangleleft)$-isomorphism between $Z^2_c(\triangleleft), B^2_c(\triangleleft), H^2_c(\triangleleft)$ and $Z^2_c(\triangleleft'^\alpha), B^2_c(\triangleleft'^\alpha), H^2_c(\triangleleft'^\alpha)$, respectively for every $\alpha \in A_p$.

**Proof:** (i) For every $a \in G, x \in C_p$, we have

\[
(a \triangleleft'^\alpha)x = (a \triangleleft \alpha(x))x = a\lambda \triangleleft' \alpha(x) = a\lambda \triangleleft'^\alpha x
\]

(ii) First we note that $A(\triangleleft)$ can be identified with $A(\triangleleft'^\alpha)$ for any $\alpha$ by the folllowing calculation

\[
(g \triangleleft'^\alpha x)\phi = (g \triangleleft \alpha(x))\phi = (g\phi) \triangleleft \alpha(x) = g\phi \triangleleft'^\alpha x \text{ for every } \phi \in A(\triangleleft).
\]
Thus we will treat every $Z^2_c(\mathcal{A}^\alpha)$ as an $\mathcal{A}(\mathcal{A})$-module. Our next step is to show that for every $\tau \in Z^2_c(\mathcal{A})$, $\tau \alpha$ lies in $Z^2_c(\mathcal{A})$. This boils down to checking (1.18) for $\tau \alpha$ with the $\mathcal{A}(\mathcal{A})$-action:
\[
(\tau \alpha)(xy) = \tau(\alpha(x)\alpha(y)) = \tau(\alpha(\alpha(x))(\alpha(x) \bullet \alpha(\alpha(y))) = \tau(\alpha(x)(x \bullet \alpha(\alpha(y)) = (\tau \alpha)(x)(x \bullet \alpha(\alpha(y))) = (\tau \alpha)(x)(x \bullet \alpha(\alpha(y))).
\]
As for $\mathcal{A}(\mathcal{A})$-linearity, for every $\phi \in \mathcal{A}(\mathcal{A})$, we have
\[
((\tau \alpha) \phi)(x, a, b) = (\tau \alpha)(x, a\phi^{-1}, b\phi^{-1}) = \tau(\alpha(x), a\phi^{-1}, b\phi^{-1}) = (\tau \phi)(\alpha(x), a, b) = ((\tau \phi)(\alpha)(x, a, b).
\]

We need several short remarks.

**Lemma 3.6.** Suppose $\tau$ is a 2-cocycle. Assume $r \in (kG)^\bullet$ is such that $r = \epsilon$. Set $r_i = \phi_i r$, $1 \leq i \leq p$. Define a 1-cocycle $\zeta : G \rightarrow (kG)^\bullet$ by $\zeta(t^i) = r_i$ and a 2-cocycle $\tau' = \tau(\delta_G \zeta)$. Then the mapping
\[
i : H(\tau, \mathcal{A}) \rightarrow H(\tau', \mathcal{A}), i(p_a t^i) = p_a r_i t^i, a \in G, 1 \leq i \leq p
\]
is an equivalence of extensions.

**Proof:** We need to show $\delta_G \zeta \in B^2$ which means that $\zeta$ satisfies (1.19). The argument of Lemma 2.3 used to derive (1.18) from the condition (2.4) works verbatim for $\zeta$.

**Lemma 3.7.** $H(\tau, \mathcal{A})$ is cocommutative iff $\tau$ lies in $H^2_c(\mathcal{A})$.

**Proof:** $H^*(\tau, \mathcal{A})$ is commutative iff $a b = b a$ which is equivalent to $\tau(a, b) = \tau(b, a)$. The latter implies that $\tau(t) : G \times G \rightarrow k^\bullet$ is a symmetric 2-cocycle, hence a coboundary, that is an element of $B^2_N$. A reference to Lemma 2.4(i) completes the proof.

Unless stated otherwise, $H(\tau, \mathcal{A})$ is a noncocommutative Hopf algebra. We pick another algebra $H(\tau', \mathcal{A}')$ isomorphic to $H(\tau, \mathcal{A})$ via $\psi : H(\tau, \mathcal{A}) \rightarrow H(\tau', \mathcal{A}')$. The next observation is noted in [14, p. 802].

**Lemma 3.8.** Mapping $\psi$ induces an Hopf automorphism of $kG$.

Let $G$ be a finite group and $\text{Aut}_{HF}(kG)$ be the group of Hopf automorphisms of $kG$. For $\phi \in \text{Aut}_{HF}(kG)$ we denote by $\phi^*$ the mapping of $G$ induced by $\phi$ via
\[
(a\phi^*)(f) := f(a\phi^*) = \phi(f)(a), f \in kG.
\]
**Lemma 3.9.** Let $G$ be a finite abelian group. The mapping $\phi \mapsto \phi^*$ is an isomorphism between $\text{Aut}_H(\mathbb{k}G)$ and $\text{Aut}(G)$. $\phi$ is a $C_p$-isomorphism $(\mathbb{k}G, \bullet) \to (\mathbb{k}G, \circ)$ if and only if $\phi^*$ is a $C_p$-isomorphism $(G, \triangle) \to (G, \triangle)$.

**Proof:** In general $\phi^*$ is a permutation of the set $G$. When $G$ is abelian and $\mathbb{k}$ contains a $|G|$th root of 1, we have $\mathbb{k}G = \mathbb{k}G$. Then $\phi(G) = G$, as $\phi$ preserves grouplikes. It follows from a straightforward calculation that $\phi^*$ is a group automorphism and $\phi \mapsto \phi^*$ is an isomorphism.

We proceed to formulation of isomorphism theorems. We need several preliminary remarks. First off, let $\triangle$ be a $C_p$-action on $G$. We denote by $[\triangle]$ the class of $C_p$-actions $\triangle'$ isomorphic to $\triangle^\alpha$ for some $\alpha \in A_p$, that is such that $I(\triangle', \triangle^\alpha)$ is nonempty. We let $\text{Ext}_{\triangle}(\mathbb{k}C_p, \mathbb{k}G)$ stand for all equivalence classes of extensions whose $C_p$-action on $G$ lies in $[\triangle]$.

In the second place we construct groups $G(\triangle)$ that control isomorphism types of extensions. For the trivial action we set $G(\text{triv}) = \text{Aut}(G) \times A_p$. Else, we observe that by Lemma 3.5(i) if $\lambda \in I(\triangle, \triangle^\alpha)$, $\mu \in I(\triangle, \triangle^\beta)$, then $\lambda \mu \in I(\triangle, \triangle^{\alpha \beta})$. Therefore the set of all $\alpha \in A_p$ such that $I(\triangle, \triangle^\alpha) \neq \emptyset$ is a subgroup of $A_p$ denoted by $C(\triangle)$. Let us select an element $\lambda_\alpha \in I(\triangle, \triangle^\alpha)$ for every $\alpha \in C(\triangle)$. We define $G(\triangle)$ as the subgroup of $\text{Aut}(G)$ generated by $\mathbb{A}(\triangle)$ and the elements $\lambda_\alpha, \alpha \in C(\triangle)$.

**Proposition 3.10.** If action $\triangle$ is nontrivial, then $G(\triangle)$ is a crossed product of $\mathbb{A}(\triangle)$ with $C(\triangle)$.

**Proof:** It is evident that $\lambda \mathbb{A}(\triangle) \lambda^{-1} = \mathbb{A}(\triangle)$ for every $\lambda \in I(\triangle, \triangle^\alpha)$. In addition, for every $\lambda, \mu \in I(\triangle, \triangle^\alpha)$, $\lambda^{-1} \mu \in \mathbb{A}(\triangle)$. Thus we have $I(\triangle, \triangle^\alpha) = \mathbb{A}(\triangle) \lambda_\alpha$. It follows that $\lambda_\alpha : \lambda_\beta = \phi(\alpha, \beta)\lambda_{\alpha \beta}$ for some $\phi(\alpha, \beta) \in \mathbb{A}(\triangle)$. It remains to show that the kernel of $\pi : G(\triangle) \to C(\triangle)$, $\pi(\phi \lambda_\alpha) = \alpha$ equals $\mathbb{A}(\triangle)$. Pick $\alpha : x \to x^k, k \neq 1$. Clearly $\lambda \in I(\triangle, \triangle^\alpha)$ iff $t \lambda = \lambda t$ where we treat $t \in C_p$ as automorphism of $G$. Since elements of $\mathbb{A}(\triangle)$ commute with $t$, $I(\triangle, \triangle^\alpha) \cap \mathbb{A}(\triangle) = \emptyset$.

Our next goal is to define a $G(\triangle)$-module structure on $H^2_c(\triangle)$. For every $\lambda \in I(\triangle, \triangle^\alpha)$ Lemmas 3.4(ii), 3.5(ii) show that the mapping

\begin{equation}
(3.5) \quad \omega_{\lambda, \alpha} : \tau \mapsto \tau.\lambda \alpha^{-1}, \tau \in H^2_c(\triangle)
\end{equation}

is an automorphism of $H^2_c(\triangle)$. For $\lambda = \lambda_\alpha$ we write $\omega_\alpha = \omega_{\lambda, \alpha}$. $\mathbb{A}(\triangle)$ also acts on $H^2_c(\triangle)$, and we denote by $\overline{\phi}$ the automorphism of $H^2_c(\triangle)$ induced by $\phi \in \mathbb{A}(\triangle)$.

**Lemma 3.11.** The mapping $\phi \lambda_\alpha \mapsto \overline{\phi} \omega_\alpha, \phi \in \mathbb{A}(\triangle), \alpha \in C(\triangle)$ defines $\mathbb{G}(\triangle)$-module structure on $H^2_c(\triangle)$. 
Proof: $H^2_c(\langle \rangle)$ is a subquotient of $Z^2(G, (kC_p)^*)$, and actions of $A(\langle \rangle)$ and $\omega_A$ on $H^2_c(\langle \rangle)$ are induced from their actions on $Z^2(G, (kC_p)^*)$. By Lemma 3.4(i) $Z^2(G, (kC_p)^*)$ is an $\text{Aut}(G)$-module, hence it is a $G(\langle \rangle)$-module as well. On the other hand, it is elementary to check that every $\lambda \in \text{Aut}(G)$ commutes with every $\beta \in A_p$ as mappings of $Z^2(G, (kC_p)^*)$. It follows that the equalities $\omega_A \omega_B = \overline{\phi(\alpha, \beta)} \omega_{\alpha \beta}$ and $\omega_A \phi \omega_{\alpha}^{-1} = \lambda_{\alpha} \phi \lambda_{\alpha}^{-1}$ hold in $\text{Aut}(Z^2(G, (kC_p)^*))$. This shows that the mapping of the Lemma is a homomorphism, as needed.

Theorem 3.12. (I) Noncocommutative extensions $H(\tau, \langle \rangle$ and $H(\tau', \langle \rangle$ are isomorphic if and only if

(i) There exist $\alpha \in A_p$ and $C_p$-isomorphism $\lambda : (G, \langle \rangle) \to (G, \langle \rangle^\alpha)$ such that

(ii) $\tau' = \tau . (\lambda \alpha^{-1})$ in $H^2(\langle \rangle$.

(II) There is a bijection between the orbits of $G(\langle \rangle$ in $H^2_c(\langle \rangle$ not contained in $H^2_c(\langle \rangle$ and the isomorphism classes of noncocommutative extensions in $\text{Ext}_{G}(kC_p, kG)$.

Proof: (I). In one direction, suppose $\psi : H(\tau, \langle \rangle) \to H(\tau', \langle \rangle$ is an isomorphism. By Lemma 3.8 $\psi$ induces an automorphism $\phi : [kG] \to [kG]$, and from Lemma 3.3 we have the equality $\psi(t) = rt^k$ for some $k$ and $r \in kG$. The equality $\psi(t^p) = 1$ implies $(rt^k)^p = \phi_p(t^k) \circ r = 1$ and, as $\phi_p(t^k) = \phi_p(t)$, we have $\phi_p \circ r = 1$. This shows $r \in (kG)^*$. Let $\alpha : x \mapsto x^k, x \in C_p$ be this automorphism of $C_p$, and set $\phi = \psi|_{kG}$. Then the calculation

$$\phi(t \cdot f) = \psi(tft^{-1}) = r\alpha(t)\phi(f)\alpha(t)^{-1}r^{-1} = \alpha(t) \circ \phi(f), f \in kG$$

shows $\phi : (kG, \cdot) \to (kG, \circ^\alpha)$ is a $C_p$-isomorphism. It follows by Lemma 3.9 that $(G, \langle \rangle^\alpha)$ is isomorphic to $(G, \langle \rangle$ under $\phi^*$, hence $\lambda = (\phi^*)^{-1} : (G, \langle \rangle) \to (G, \langle \rangle^\alpha)$ is a required isomorphism.

It remains to establish the second condition of the theorem. Set $s = \phi^{-1}(r)$ and observe that, as $\phi^{-1}$ is a $C_p$-mapping, $\phi_p \cdot s = 1$. For $\phi_p \circ r = \phi_p \circ^\alpha r = 1$. Hence $\phi^{-1}(\phi_p \circ^\alpha r) = \phi_p \circ^{-1}(r) = \phi_p \circ s = 1$, and therefore by Lemma 3.6 there is an equivalence $\iota : H(\tau, \langle \rangle) \to H(\tilde{\tau}, \langle \rangle$ with $\iota(t) = st$.

By construction $\iota$ is an algebra map with $\iota(s) = s$ for all $s \in kG$. Hence $t = \iota(st) = st^{-1}(t)$ whence $\iota^{-1}(t) = s^{-1}t$. Thus we have $(\psi \iota^{-1})(t) = t^k$ by the choice of $s$. It follows we can assume $\psi(t) = t^k$ hence $\psi(x) = x^k$ for all $x \in C_p$.

Abbreviating $H(\tau, \langle \rangle, H(\tau', \langle \rangle$ to $H, H'$, respectively, we take up the identity.

$$\Delta_H'(\psi(x)) = (\psi \otimes \psi) \Delta_H(x), x \in C_p.$$
expressing comultiplicativity of $\psi$ on elements of $C_p$. By (1.13) this translates into
\[
(3.6) \quad \sum_{a,b} \tau'(x^k, a, b)p_a x^k \otimes p_b x^k = \sum_{c,d} \tau(x, c, d)\phi(p_c)x^k \otimes \phi(p_d)x^k.
\]

Next we connect $\phi(p_b)$ to the action of $\phi^*$. The argument used to prove (1.4) yields
\[
(3.7) \quad \phi(p_b) = p_b(\phi^*)^{-1}.
\]

For, since $\phi$ is an algebra map, $\phi(p_b) = p_c$ where $c$ is such that $\phi(p_b)(c) = 1$. By definition of action $\phi^*$, $\phi(p_b)(c) = (c\phi^*)(p_b) = p_b(c\phi^*)$, hence $c\phi^* = b$, whence $c = b(\phi^*)^{-1}$.

Switching summation symbols $c, d$ to $l = c(\phi^*)^{-1}$ and $m = d(\phi^*)^{-1}$, the right-hand side of (3.6) takes on the form
\[
\sum_{l,m} \tau(x, l\phi^*, m\phi^*)p_l x^k \otimes p_m x^k
\]

Thus $\psi$ is comultiplicative on $C_p$ iff
\[
(3.8) \quad \tau'(\alpha(x), a, b) = \tau(x, a\phi^*, b\phi^*) = \tau(\phi^*)^{-1}(x, a, b) = \tau.\lambda(x, a, b).
\]

Applying $\alpha^{-1}$ to the last displayed equation we arrive at
\[
(3.9) \quad \tau'(x, a, b) = \tau.\lambda\alpha^{-1}(x, a, b).
\]

as needed.

Conversely, let us assume hypotheses of part (I). Using Lemma 3.9 we infer that $\lambda^{-1}$ induces a Hopf $C_p$-isomorphism $\phi : (kG, \bullet) \to (kG, c^\alpha)$. We define
\[
\psi : H(\tau, \cdot, \cdot) \to H(\tau', \cdot, \cdot) \text{ via } \psi(f x) = \phi(f)\alpha(x), f \in kG, x \in C_p.
\]

A routine verification using $\phi(x \bullet f) = \alpha(x) \circ \phi(f)$ shows $\psi$ is an algebra mapping.
\[
\psi((f x)(f' x')) = \psi(f x \bullet f' x') = \phi(f)\phi(x \bullet f')\alpha(x)\alpha(x') = \phi(f)\alpha(x)\phi(f')\alpha^{-1}(x)\alpha(x)\alpha(x') = (\phi(f)\alpha(x))(\phi(f')\alpha(x') = \psi(f x)\psi(f' x').
\]

To see comultiplicativity of $\psi$ we need to verify
\[
(3.10) \quad \Delta_H(\psi(f x)) = (\psi \otimes \psi)\Delta_H(f x).
\]

By multiplicativity of $\Delta_H$, $\psi, \Delta_H$ it suffices to check (3.10) for $\phi$ and for every $\psi(x)$. Now the first case holds as $\phi$ is a coalgebra mapping, and the second follows from $\tau' = \tau.\lambda\alpha^{-1}$ by calculations (3.6) and (3.9).
(II). Pick an algebra $H(\tau', \delta')$ in $\text{Ext}_{\langle \alpha \rangle}(\mathbb{k}C_p, \mathbb{k}G)$. Let us define the set $\mathcal{C} = \mathcal{C}(\tau', \delta')$ by the formula
\[
\mathcal{C}(\tau', \delta') = \{(\tau'', \delta'')| H(\tau'', \delta'') \simeq H(\tau', \delta')\}.
\]
Clearly the family of sets $\{\mathcal{C}\}$ is identical to the set of isoclasses of extensions in $\text{Ext}_{\langle \alpha \rangle}(\mathbb{k}C_p, \mathbb{k}G)$. We look at the intersection $\mathcal{C} \cap H^2_c(\langle \alpha \rangle)$ as $\mathcal{C}$ runs over $\{\mathcal{C}\}$. First, we claim that $\mathcal{C}(\tau', \delta') \cap H^2_c(\langle \alpha \rangle) \neq \emptyset$ for every $(\tau', \delta')$. To this end we note that as $\delta' \in [\delta]$ there exists $\mu : (G, \delta') \to (G, \delta'' \alpha)$, and then setting $\tau = \tau', \mu \alpha^{-1}$ we have $(\tau, \langle \alpha \rangle \in \mathcal{C}(\tau', \delta')$ by part (I). Next we show the equality $\mathcal{C}(\tau', \delta') \cap H^2_c(\langle \alpha \rangle) = \tau\mathcal{G}(\langle \alpha \rangle)$. For, by definition $(\sigma, \langle \alpha \rangle) \in \mathcal{C}(\tau', \delta')$ iff $H(\sigma, \langle \alpha \rangle) \simeq H(\tau, \langle \alpha \rangle)$ which by part (I) implies $\sigma = \tau, \omega_{\lambda, \alpha}$ for some $\alpha \in A_p$ and $\lambda : (G, \langle \alpha \rangle) \to (G, \delta'')$. It follows that the mapping
\[
\mathcal{C} \to \mathcal{C} \cap H^2(\langle \alpha \rangle), \mathcal{C} \in \{\mathcal{C}\}
\]
is an injection from the set of isoclasses of noncocommutative extensions in $\text{Ext}_{\langle \alpha \rangle}(\mathbb{k}C_p, \mathbb{k}G)$ to the set of orbits of $\mathcal{G}(\langle \alpha \rangle)$ in $H^2_c(\langle \alpha \rangle)$ not contained in $H^2_c(\langle \alpha \rangle)$. This mapping is also a surjection as for every $\tau \in H^2_c(\langle \alpha \rangle), \mathcal{C}(\tau, \langle \alpha \rangle) \cap H^2_c(\langle \alpha \rangle) = \tau\mathcal{G}(\langle \alpha \rangle)$. □

**Corollary 3.13.** For every $\tau \in H^2_c(\langle \alpha \rangle)$ the cardinality of the orbit $\tau\mathcal{G}(\langle \alpha \rangle)$ satisfies
\[
|\tau\mathcal{A}(\langle \alpha \rangle)| \leq |\tau\mathcal{G}(\langle \alpha \rangle)| \leq |\mathcal{C}(\langle \alpha \rangle)||\tau\mathcal{A}(\langle \alpha \rangle)|.
\]

**Proof:** Let $X(\langle \alpha \rangle)/\mathcal{A}(\langle \alpha \rangle)$ be the set of $\mathcal{A}(\langle \alpha \rangle)$-orbits in $X(\langle \alpha \rangle)$. Since $\mathcal{A}(\langle \alpha \rangle)$ is normal in $\mathcal{G}(\langle \alpha \rangle)$, there is an induced action of $\mathcal{C}(\langle \alpha \rangle) = \mathcal{G}(\langle \alpha \rangle)/\mathcal{A}(\langle \alpha \rangle)$ on $X(\langle \alpha \rangle)/\mathcal{A}(\langle \alpha \rangle)$. An orbit of $\mathcal{G}(\langle \alpha \rangle)$ is union of points of some orbit of $\mathcal{C}(\langle \alpha \rangle)$. The latter has size $\leq |\mathcal{C}(\langle \alpha \rangle)|$ whence the Corollary. □

The second isomorphism theorem concerns cocommutative extensions in $\text{Ext}_{\langle \alpha \rangle}(\mathbb{k}C_p, \mathbb{k}G)$ under a stricter condition on $G$, namely we assume $G$ to be an elementary $p$-group.

**Theorem 3.14.** Let $G$ be a finite elementary $p$-group. Then there is a bijection between the set of orbits of $\mathcal{A}(\langle \alpha \rangle)$ in $H^2_{cc}(\langle \alpha \rangle)$ and the set of isoclasses of cocommutative Hopf algebras in $\text{Ext}_{\langle \alpha \rangle}(\mathbb{k}C_p, \mathbb{k}G)$.  

**Proof:** By Lemma 3.7 $\tau = \delta\eta \in H^2_{cc}(\langle \alpha \rangle)$. A proof of the Theorem comes down to the statement
\[
(3.11) \quad H(\delta\eta, \langle \alpha \rangle) \simeq H(\delta\zeta, \delta') \text{ iff } \delta\zeta = (\delta\eta) \cdot (\phi^*)^{-1}
\]
for a $C_p$-isomorphism $\phi : (\widehat{G}, \bullet) \to (\widehat{G}, \circ)$. This makes sense as $\phi : (\mathbb{k}^G, \bullet) \to (\mathbb{k}^G, \circ)$ restricts to $\phi : (\widehat{G}, \bullet) \to (\widehat{G}, \circ)$ by Lemma 3.9 and $\widehat{G}$ is $C_p$-stable by Lemma 1.2(2). The proof of (3.11) will be based on several intermediate results.
By general principles a cocommutative Hopf algebra $H(\tau, \langle \rangle)$ is a Hopf group algebra of some group $L$. Our first step is to identify that group.

**Lemma 3.15.** A cocommutative extension $H(\tau, \langle \rangle)$ is isomorphic as a Hopf algebra to a group algebra $kL$ with $L \in \text{Opext}(C_p, \hat{G}, \bullet)$.

**Proof:** Let $H \sim G(H)$ be the functor of taking the group of grouplikes of $H$. Applying $G(\cdot)$ to an extension $k^G \to kL \to kC_p \in \text{Ext}(kC_p, k^G, \langle \rangle)$ yields an extension $\hat{G} \to L \to C_p \in \text{Opext}(C_p, \hat{G}, \bullet)$.

On the other hand, by Lemma 2.4 we have a group isomorphism

$$H^2_G(\langle \rangle)/B^2_G(\langle \rangle) \simeq \hat{G}^{C_p}/N(\hat{G})$$

under the mapping $\delta \eta \mapsto \Phi(\delta \eta) = \phi_p \cdot \eta(t)N(\hat{G})$. We will write $L(\chi)$ when the cohomology class of $L$ is $\chi := \chi N(\hat{G})$, $\chi \in \hat{G}^{C_p}$. We want to construct an explicit isomorphism $H(\delta \eta, \langle \rangle) \simeq kL(\Phi(\delta \eta))$.

We will use the notation $\chi(t) = \hat{G} \to \hat{G}G$, $\eta(t) \to \chi N(\hat{G})$. Thus $\hat{G}$ is a Hopf coboundary. In this case $H(\delta \eta, \langle \rangle) \simeq H(\epsilon \otimes \epsilon, \langle \rangle)$, where $\epsilon \otimes \epsilon$ is the trivial 2-cocycle. By (1.13) we have in $H(\epsilon \otimes \epsilon, \langle \rangle)$

$$\Delta_H(t) = \sum_{a,b \in G} f(a) f(b) f(ab)^{-1} p_a t \otimes p_b t$$

Thus $\hat{G} \times C_p$ consists of grouplikes, hence $H(\epsilon \otimes \epsilon, \langle \rangle) = k(\hat{G} \times C_p)$. In general, that is if $\chi(t) \neq t$, $t$ can be twisted into a grouplike.

In the foregoing notation, let $f = \eta(t)$. We claim the element $ft$ is a grouplike in $H(\delta \eta, \langle \rangle)$. First, since $\eta : G \to (k^C)^\bullet$, $\eta(t) \in k^G$, and $ft$ makes sense. By (1.13)

$$\Delta_H(f) = \sum_{a,b} (\delta f)(a,b) p_a t \otimes p_b t$$

Next apply $\Delta_H$ to the standard expansion $f = \sum_a f(a)p_a$. We get

$$\Delta_H(f) = \sum_a f(a) \sum_{b,c = a} p_b \otimes p_c = \sum_{b,c} f(\eta(b) \otimes p_c$$

All in all we have

$$\Delta_H(ft) = \Delta_H(f) \Delta_H(t)$$

$$= \sum_{a,b} f(ab)p_a \otimes p_b \sum_{a,b} f(a) f(b) f(ab)^{-1} p_a t \otimes p_b t$$

$$= \sum_{a,b} f(a) f(b)p_a t \otimes p_b t = \sum_a f(a)p_a t \otimes (\sum_b f(b) p_b) t = ft \otimes ft,$$

as needed.
Set $x = ft, \chi = \chi_\eta$ and observe that $x^p = \phi_p \cdot f = \chi$. We see $x$ is a unit in $H(\delta \eta, \langle \rangle)$. The action of $x$ on $\hat{G}$ by conjugation coincides with the action of $t$. Let $G(\overline{\chi}, \bullet)$ be the subgroup of $H(\delta \eta, \langle \rangle)$ generated by $\hat{G}$ and $x$. Clearly $G(\overline{\chi}, \bullet)/\hat{G} = C_p$, hence $G(\overline{\chi}, \bullet)$ is an extension of $C_p$ by $\hat{G}$ associated to the datum $\{\chi, \bullet\}$. There $\overline{\chi}$ represents the cohomology class of $G(\overline{\chi}, \bullet)$ as an element of $\text{Opext}(C_p, \hat{G}, \bullet)$, since $H^2(C_p, \hat{G}, \bullet) = \hat{G}^{C_p}/N(\hat{G})$. From $|G(\overline{\chi}, \bullet)| = \dim H(\delta \eta, \langle \rangle)$ we conclude $H(\delta \eta, \langle \rangle) = kG(\overline{\chi}, \bullet)$.

It becomes apparent that we have reduced the isomorphism problem for Hopf algebras to the same problem for groups $G(\overline{\chi}, \bullet)$. We need to translate condition (3.11) into a condition for the data $\{\overline{\chi}, \bullet\}$ and $\{\overline{\omega}, \circ\}$. In keeping with our convention we treat a coboundary $\delta \eta$ as an element of either $H^2_c(\langle \rangle)$ or $H^2_c/B^2_c(\langle \rangle)$.

**Lemma 3.16.** Let $\phi : (\hat{G}, \bullet) \rightarrow (\hat{G}, \circ)$ be a $C_p$-isomorphism, and $\delta \eta \in H^2_c(\langle \rangle), \delta \zeta \in H^2_c(\langle \rangle)$. Put $\overline{\chi} = \Phi \Theta(\delta \eta)$ and $\overline{\omega} = \Phi \Theta(\delta \zeta)$. Then $\delta \zeta = (\delta \eta)(\phi^*)^{-1} \iff \phi(\overline{\chi}) = \overline{\omega}$.

**Proof:** In the above statement we used the same letter $\phi$ for the induced isomorphism $\hat{G}^{C_p}/N(\hat{G}, \bullet) \rightarrow \hat{G}^{C_p}/N(\hat{G}, \circ)$. By definition of $(\phi^*)^{-1}$, $(\delta \eta)(\phi^*)^{-1}(a, b) = \eta(a \phi^*)\eta(b \phi^*)\eta((ab)\phi^*)^{-1}$. As $\eta(a \phi^*) = \phi(\eta)(a)$ by (3.4), it follows that $(\delta \eta)(\phi^*)^{-1} = \delta(\phi(\eta))$, hence the condition of the Lemma says $\delta \zeta = \delta(\phi(\eta))$. Applying $\Phi \Theta$ to the last equation, and using $C_p$-linearity of $\phi$ we derive $\phi_p \circ \zeta(t)N(\hat{G}, \circ) = \phi(\phi_p \cdot \eta(t))N(\hat{G}, \bullet)$, that is $\overline{\omega} = \phi(\overline{\chi})$. Since all steps of the proof are reversible, the proof is complete.

The final step of the proof is

**Proposition 3.17.** $G(\overline{\chi}, \bullet) \simeq G(\overline{\omega}, \circ)$ if and only if $\exists C_p$-isomorphism $\phi : (\hat{G}, \bullet) \rightarrow (\hat{G}, \circ)$ such that $\phi(\overline{\chi}) = \overline{\omega}$.

**Proof:** The proof of the proposition will be carried out in steps.

(1) We assume action `$\bullet$' to be nontrivial which is equivalent to assuming $H(\delta \eta, \langle \rangle)$ is a noncommutative algebra. We simplify notations by replacing $\hat{G}$ with $G$, and $\overline{\chi}$ by $\overline{a}$ where $a \in G^{C_p}$ and $\overline{a} = a N(G)$. An extension of $C_p$ by $G$ defined by some $\overline{a}$ and `$\bullet$' will be denoted by $G(\overline{\pi}, \bullet)$. Recapping Lemma 3.15 we note that the group $G(\overline{\pi}, \bullet)$ is generated by $G$ and an element $x \notin G$ such that $x^p = a$ and the action of $x$ in $G$ by conjugation coincides with the action of a generator of $C_p$.

We note that if $\overline{a} = \overline{T}$ then $x$ can be chosen so that $x^p = 1$. For, from $x^p = \phi_p \cdot b$ we have $(b^{-1}x)^p = 1$. It follows each $G(\overline{\tau}, \bullet) = G \rtimes C_p$. 

26 LEONID KROP
1. We need only to show the necessary part, proof of elements of \( \psi \) does not exist. Hence \( \psi \) is an isomorphism. Let \( x, y \) be elements of \( G(\overline{\pi}, \bullet) \) and \( G(\overline{\pi}, \circ) \), respectively, with \( x^p = 1 \) and \( y^p = a \). Were \( \psi(g) = h g^k \) for some \( g, h \in G \), we would have \( 1 = \psi(g^p) = (\phi_p(y^k) \circ h) a^k = (\phi_p(y) \circ h) a^k \) contradicting to \( \overline{\pi} \neq \overline{\pi} \). Thus \( \psi(G) = G \), hence \( \psi(x) = cy^k, c \in G, 1 \leq k \leq p - 1 \). But then the preceding argument gives \( 1 = \psi(x^p) = (\phi_p(y) \circ c) a^k \) whence \( \overline{\pi} = \overline{\pi} \), a contradiction. Thus such \( \psi \) does not exist.

3. Here we show that \( C_p \)-modules \( (G, \bullet^a) \) and \( (G, \bullet) \) are isomorphic for every \( \alpha \in A_p \). Let us write \( G \) additively. Set \( R = \mathbb{Z}_p C_p \) and \( R_l = R/J \) where \( J_l = \langle (t - 1)^l \rangle, 1 \leq l \leq p \) with \( \langle u \rangle \) denoting the submodule generated by \( u \). The action of \( C_p \) in \( G \) induces an \( R \)-module structure in \( G \). Every indecomposable \( R \)-module is isomorphic to some \( R_l \) with the action of \( R \) by the left multiplication. Therefore the Krull-Schmidt decomposition of \( (G, \bullet) \)

\[
(G, \bullet) = B_1 \oplus \cdots \oplus B_p,
\]

consists of blocks \( B_l = R_{m_l} \) of direct sums of modules \( R_l \). There the action \( \bullet \) is taken to be the left multiplication. The sequence \( \{m_l\} \) determines the isomorphism type of \( (G, \bullet) \). An automorphism \( \alpha : x \mapsto x^k, x \in C_p \) induces the automorphism of \( R \) which sends \( J_l \) to itself. Therefore \( \alpha \) induces an automorphism of \( R_l \), hence the \( R \)-module isomorphism \( (R_l, \bullet) \sim (R_l, \bullet^a) \). This proves our claim.

4. Here we prove the proposition for groups \( G(\overline{\pi}, \bullet) \) and \( G(\overline{\delta}, \circ) \) with \( \overline{\pi} \neq \overline{\pi} \) and \( \overline{\delta} \neq \overline{\pi} \). We need only to show the necessary part, proof of sufficiency is fairly straightforward.

Suppose \( \psi : G(\overline{\pi}, \bullet) \to G(\overline{\delta}, \circ) \) is an isomorphism. Let \( x, y \) be elements of those groups such that \( x^p = a \) and \( y^p = b \). By the argument used in (2) there holds: \( \psi(G) = G \) and \( \psi(x) = cy^k \) for some \( c \in G \) and \( 1 \leq k \leq p - 1 \). We derive the equality

\[
\psi(x \bullet g) = \psi(x gx^{-1}) = y^k gy^{-k} = y^k \circ g.
\]

Note (3.13) shows the restriction \( \phi = \psi|_G \) to be a \( C_p \)-isomorphism \( \phi : (G, \bullet) \to (G, \circ^a) \) where \( \alpha : x \mapsto x^k \). Furthermore \( \psi(x) = cy^k \) implies \( \phi(a) = \psi(x^p) = (\phi_p(y^k) \circ c)y^{pk} = (\phi_p(y) \circ c)b^k \) as \( \phi_p(y^k) = \phi_p(y) \).

Say \( \lambda : (G, \circ^a) \to (G, \circ) \) is a \( C_p \)-isomorphism guaranteed by part (3). One can see easily that \( \phi_p(t)R = J_{p-1} \), hence \( N(G, \circ) = J_{p-1} \circ G \) for any action \( \circ \). Therefore \( N(G, \circ^a) = J_{p-1} \circ^a G = \alpha(J_{p-1} \circ G = J_{p-1} \circ G = N(G, \circ) \). As \( \lambda \) is \( R \)-isomorphism, \( \lambda(N(G, \circ^a)) = N(G, \circ) \), that is \( \lambda(N(G, \circ)) = N(G, \circ) \). Therefore as \( b \) is a fixed point, so is \( s = \lambda(b^k) \). Let \( b_i, s_i \) be the \( B_i \) components of \( b, s \) from a decomposition
(3.12) for \((G, \circ)\). Since \(b\) and \(s\) are fixed points, so are \(b_l\) and \(s_l\) for all \(l\). Therefore they lie in the socle of \(B_l\) and are simultaneously equal to 0, or distinct from 0, hence there is an automorphism of the socle mapping \(s_l\) to \(b_l\). Since each \(B_l\) is a free \(R_l\)-module there exists a \(C_{p^l}\)-automorphism \(\sigma_l\) such that \(\sigma_l(s_l) = b_l\). It follows that there exists a \(C_{p^l}\)-automorphism \(\sigma\) of \((G, \circ)\) with \(\sigma(s) = b\).

Indeed, suppose \(B_l = R_l^{(1)} \times \cdots \times R_l^{(m)}\). Let \(\overline{1} = 1 + J_l\) be a generator of \(R_l\) as a \(C_p\)-module, and \(g_j\) be a copy of \(\overline{1}\) in \(R_l^{(j)}\). Since \(b_l\) is a fixed point, \(b_l \in (t-1)^{l-1}B_l\), hence \(b_l = ((t-1)^{l-1}(\sum k_jg_j), k_j \in \mathbb{Z}_p\).

The mapping \(\beta : g_1 \mapsto k_1g_1 \cdots kmg_m, g_i \mapsto g_i, i > 1\) extends to a \(C_{p^l}\)-automorphism with \(\beta((t-1)^{l-1}g_1 = b_l\). If \(s_l\) is another element of \((t-1)^{l-1}B_l\), then there exists a \(C_{p^l}\)-automorphism \(\gamma : (t-1)^{l-1}g_1 \rightarrow s_l\). But then \(\beta\gamma^{-1}(s_l) = b_l\).

Since \(\sigma\) commutes with the action of \(C_{p^l}\), \(\sigma\lambda(N(G, \circ)) = N(G, \circ)\).

The mapping \(\phi = \sigma\lambda\) is a \(C_{p^l}\)-automorphism \((G, \bullet) \rightarrow (G, \circ)\) with the property \(\phi(a) = (\sigma\lambda(\phi_p \circ c))b, \) hence \(\phi(\overline{a}) = \overline{b}\). This completes the proof of (4).

(5) We consider an isomorphism \(\psi : G(\overline{T}, \bullet) \rightarrow G(\overline{T}, \circ)\). We need only to show the modules \((G, \bullet)\) and \((G, \circ)\) are isomorphic. Put \(G = G(\overline{T}, \bullet)\) and \(G_1 = G(\overline{T}, \circ)\). For a group \(F\) we let \(\{\gamma_r(F)\}\) denote the lower central series of \(F\) [6]. A routine calculation yields \(\gamma_r(G) = (t-1)^{r-1}\bullet G\). One can see easily \(\dim_{\mathbb{Z}_p} \gamma_l(G)/\gamma_{l+1}(G) = m_l + \cdots + m_p\). It becomes evident that the multiplicities \(m_j\) are determined by the lower central filtration. Since an isomorphism \(\psi : G \rightarrow G_1\) induces isomorphism between the lower central series in \(G\) and \(G_1\), the sequence \(m_1, \ldots, m_p\) is an isomorphism invariant. This proves (5).

(6) It remains to settle the case of the trivial action. Now \(G(\overline{a}) := G(\overline{a}, \text{triv})\) is abelian. We have \(N(G) = C_p = 1\), hence \(\overline{a} = a\). If \(a = 1, G(a) = G \times \langle x \rangle\) is an elementary \(p\)-group. Else, \(a \neq 1, x^p = a\) which shows \(x\) has order \(p^2\). It is clear \(G(1) \neq G(a)\) for every \(a \neq 1\). Furthermore, if \(a = 1\), let \(\overline{G}\) be a complement of \(a\) in \(G\). Evidently \(G(a) = \overline{G} \times \langle x \rangle\), hence if \(b \neq 1\) is another element of \(G\), \(G(a) \simeq G(b)\).

On the other hand, for every \(a, b \neq 1\) there is an automorphism \(\phi\) of \(G\) with \(\phi(a) = \phi(b)\). This completes the proof of the proposition. \(\square\)

For \(p = 2\) the isomorphism theorems yield

**Corollary 3.18.** Let \(G\) be an elementary 2-group. Then there is a bijection between the orbits of \(A(\langle \cdot \rangle)\) in \(H^2_c(\langle \cdot \rangle)\) and the isoclasses of extensions in \(\text{Ext}_{[\square]}(kC_p, k^G)\).
4. Commutative Extensions

An algebra $H(\tau, \cdot)$ is commutative iff the action ‘\cdot’ is trivial. Below we omit the symbol ‘\cdot’ and write $H(\tau)$ for $H(\tau, \text{triv})$. Every commutative finite-dimensional Hopf algebra over an algebraically closed field is of the form $k^L$ ([10], [17, 2.3.1]) for some finite group $L$. We will identify groups $L$ appearing in that formula for algebras $H(\tau)$. It is convenient to introduce the group $\text{Cext}(G, C_p)$ of central extensions of $C_p$ by $G$ [2].

**Proposition 4.1.** The group $\text{Ext}_{\text{triv}}(kC_p, k^G)$ of equivalence classes of commutative extensions is isomorphic to the group $\text{Cext}(G, C_p)$. The isomorphism is given by $H(\tau) \simeq k^G(\tau)$ where $G(\tau)$ is the central extension defined by the 2-cocycle $\tau$.

**Proof:** In one direction, pick $\tau \in H^2(\text{triv})$. We have by Proposition 1.3 for the trivial action that for every $a \in G$

$$\Delta_H(\tau) = \sum_{x, y \in C_p} \Delta p_x \otimes \Delta p_y = (\tau \otimes \tau)(\sum x p_x \otimes \sum y p_y) = \tau \otimes \tau$$

Thus $\tau$ is a grouplike for every $a \in G$. Let $\theta$ be a generator of $\hat{C}_p$. Since $k^C_{p}$ is a Hopf subalgebra of $H^*(\tau)$, $\theta$ is a grouplike of $H^*(\tau)$. We see that the set $G(\tau) = \{\Delta a|a \in G, 0 \leq i \leq p - 1\}$ consists of grouplikes. Moreover, $|G(\tau)| = \dim H^*(\tau)$, hence $G(\tau)$ is a basis of $H^*(\tau)$. Therefore $G(\tau) = \tau(\tau) = \text{G}(\tau)$ is a group and $H^*(\tau) = k\text{G}(\tau)$, whence $H(\tau) = k^G(\tau)$.

Since $\tau$ is a Hopf 2-cocycle it satisfies (1.18) which for the trivial action of $C_p$ turns into $\tau(xy) = \tau(x)\tau(y)$. Thus $\tau(a, b) : C_p \to k^*$ is a character for any choice of $a, b \in G$. We see that $\tau : C \times G \to \hat{C}_p$ is a 2-cocycle of $G$ in $\hat{C}_p$, hence $G(\tau)$ is a central extension of $G$ by $\hat{C}_p$ defined by $\tau$. It remains to notice that the subgroup $B^2_c$ consists of coboundaries in the group $Z^2(G, \hat{C}_p)$. For, by Definition 1.6 $\delta \eta \in B^2_c$ iff $\eta$ satisfies the condition (1.19), hence $\eta : G \to \hat{C}_p$.

The opposite direction is trivial. \qed

For calculations of orbits of $G(\cdot)$ in $H^2_c(\cdot)$ we prefer to use a much smaller space

$$\mathbb{X}(\cdot) = H^2(C_p, \hat{G}, \cdot) \times H^2_N(G, k^*)$$

(4.1)

We make several remarks regarding $\mathbb{X}(\cdot)$. Let $C_p$ act on $k^C_*$ by $\bullet$ with the induced action $\cdot$ on $G$. Then $C_p$ acts on $Z^2(G, (k^C_*))$ via $x \bullet \tau(y, a, b) = \tau(y, a < x, b < x), x \in C_p, a, b \in G$. Recall $Z^2_N(G, k^*)$ is the subgroup of $Z^2(G, k^*)$ of all $s \in Z^2(G, k^*)$ subject to $\phi_p \bullet s = 1$,
where $\phi_p \circ s = \prod(t^i \circ s)$, and $\phi_p = 1 + t + \cdots + t^{p-1}$. The next lemma is a strengthening of Lemma 3.4.

**Lemma 4.2.** (i) For every $\lambda \in I(\triangle, \triangle')$ the mapping $s \mapsto s.\lambda$ is a $C_p$ isomorphism $X(\triangle) \simeq X(\triangle')$.

(ii) $X(\triangle)$ is invariant under action by elements of $I(\triangle, \triangle')$ for every $\alpha \in A_p$.

**Proof:** (i) Let $\circ$ denote the action of $C_p$ on $Z^2(G, k^*)$ induced by $\triangle'$, i.e. $(x \circ s(a, b) = s(a \triangle' x, b \triangle' x)$. We need to show $\phi_p \circ (s.\lambda) = 1$. Since $\lambda^{-1} \in I(\triangle', \triangle)$ there holds $(a \triangle' x).\lambda^{-1} = a\lambda^{-1} \triangle x$. Therefore $t^i \circ (s.\lambda) = (t^i \circ s).\lambda$ as the following calculation shows:

$$t^i \circ (s.\lambda)(a, b) = (s.\lambda)(a \triangle' t^i, b \triangle' t^i) = s((a \triangle' t^i).\lambda^{-1}, (b \triangle' t^i).\lambda^{-1})$$

$$= s(a.\lambda^{-1} \triangle t^i, b.\lambda^{-1} \triangle t^i) = (t^i \circ s).\lambda(a, b).$$

We conclude that $\lambda$ induces a $C_p$-linear map $X(\triangle) \to X(\triangle')$, and also $\phi_p \circ (s.\lambda) = \prod(t^i \circ (s.\lambda)) = (\prod(t^i \circ s)).\lambda = 1$

(ii) We must show the equality $\phi_p \circ (s.\lambda) = 1$ for every $s \in Z^2_N(\triangle)$. By part (i) with $\circ = \bullet^\alpha$ there holds $\phi_p \circ (s.\lambda) = 1$. Assuming $\alpha : x \mapsto x^k$ and noting $\phi_p(t^k) = \phi_p(t)$ this gives

$$1 = \phi_p \circ (s.\lambda) = \phi_p(t^k) \circ (s.\lambda) = \phi_p \circ (s.\lambda)$$

Since $\lambda$ sends $\ker \Phi$ in $Z^2_N(\triangle)$ to $\ker \Phi$ in $Z^2_N(\triangle')$ the proof is complete. \qed

We turn $X(\triangle)$ into a $G(\triangle)$-module by transferring its action from $H^2_c(\triangle)$ to $Z^2_N(\triangle)$ along $\Theta$. Pick $\omega_{\lambda, \alpha}$ and suppose $\alpha^{-1} : x \mapsto x^t, x \in C_p$. For $s \in Z^2_N(G, k^*)$ we set

$$(4.3) \quad s.\omega_{\lambda, \alpha} = (\phi_t \circ s).\lambda.$$

Let $\Theta_*$ be the isomorphism of Corollary 2.5.

**Lemma 4.3.** (i) For every prime and any action ‘$\triangle$’ isomorphism $\Theta_* : H^2_c(\triangle) \simeq Z^2_N(G, k^*)/\ker \Phi$ is $G(\triangle)$-linear.

(ii) For every odd $p$ the isomorphism $Z^2_N(G, k^*)/\ker \Phi \simeq H^2(C_p, \tilde{G}) \times H^2_c(\triangle)$ is $G(\triangle)$-linear.

**Proof:** (i). For every $\tau \in Z^2_c(\triangle)$ we have by (2.2)

$$\Theta(\tau.\omega_{\lambda, \alpha}) = (\tau.\omega_{\lambda, \alpha})(t) = (\tau.\lambda)(t^i) = \phi_t \circ (t^i.\lambda(t)) = \phi_t \circ \alpha(\tau(t).\lambda)$$

(by (4.2)) = $(\phi_t \circ \tau(t)).\lambda = \Theta(\tau).\omega_{\lambda, \alpha}$
This equation demonstrates that (4.3) turns $\mathbb{Z}_2^N(\triangleright)$ into a $\mathcal{G}(\triangleright)$-module. It is immediate that $B^2_c(\triangleright)$ is a $\mathcal{G}(\triangleright)$-subgroup of $Z^2_c(\triangleright)$. By Lemma 2.4(ii) $\ker\Phi$ is a $\mathcal{G}(\triangleright)$-subgroup, which proves part (i).

(ii). For an odd $p$ splitting (2.8) is carried out by the mapping $s \mapsto s(s^2) \times g(s^2)$ which is clearly a $\mathcal{G}(\triangleright)$-map. It remains to note that homomorphism $\Phi$ is also a $\mathcal{G}(\triangleright)$-map. □

The next result gives the number of isotypes of commutative extensions in Ext($kC_p,kG$) for odd primes $p$ and elementary $p$-groups. By Proposition 4.1 this is also the number of nonisomorphic groups in $C_{ext}(G,C_p)$ which can be derived by group-theoretic methods. Our proof avoids group theory and sets up framework for generalization to non-elementary abelian groups. However, it does not cover 2-groups.

**Proposition 4.4.** Let $G$ be a finite elementary $p$-group of order $p^n$ for an odd $p$. There are $\left\lfloor \frac{3n+2}{2} \right\rfloor$ isotypes of commutative Hopf algebra extensions of $kC_p$ by $kG$ for any odd prime $p$.

**Proof:** Write $\mathcal{G}$ for $\mathcal{G}$(triv) and likewise $\mathbb{A} = \mathbb{A}$(triv). By Theorems 3.12, 3.14 and the preceding lemma the isotypes in question are in a bijection with the set of $\mathcal{G}$-orbits in $X$(triv). We observe that for every trivial $C_p$-module $M$, $N(M) = M^p$. Therefore, if $M$ has exponent $p$, $N(M) = 1$ and $M^p = M$. From these remarks, in view of $\hat{\mathcal{G}}$ and $\text{Alt}(G)$ having exponent $p$, we derive by Lemma 4.3 a $\mathcal{G}$-isomorphism

\[
H^2_c(\triangleright) \simeq \hat{\mathcal{G}} \times \text{Alt}(G).
\]

By definition $\mathcal{G} = \mathbb{A} \times A_p$ with elements $\alpha_k : x \mapsto x^k$ of $A_p$ acting on $X$(triv) by (4.3) as

\[
z.\alpha_k = \phi_k \bullet z = z^k \text{ as } \bullet \text{ is trivial}
\]

We proceed to description of orbits of $\mathbb{A}$ in $H^2_c(\triangleright)$. This description will show that every $\mathbb{A}$-orbit is closed to action by $A_p$, hence $\mathcal{G}$- and $\mathbb{A}$-orbits coincide. We switch to the additive notation in our treatment of $\hat{\mathcal{G}} \times \text{Alt}(G)$ and view the latter as a vector space over the prime field $\mathbb{Z}_p$.

We note $\mathbb{A}$ acts in $\hat{\mathcal{G}} \oplus \text{Alt}(G)$ componentwise. For a $\chi, \beta \in \hat{\mathcal{G}} \times \text{Alt}(G)$ we let $(\chi, \beta)\mathbb{A}$ denote the orbit of $(\chi, \beta)$. For every $\chi \in \hat{\mathcal{G}}$ we let $K_\chi$ denote $\ker \chi$.

Classification of orbits of $\mathbb{A}$ in $\hat{\mathcal{G}} \oplus \text{Alt}(G)$ relies on the theory of symplectic spaces. A symplectic space $(V, \beta)$ is a vector space with an alternating form $\beta$. We need a structure theorem for such spaces (see e.g. [9]). For a subspace $X$ of $V$ we denote by $X^\perp$ the subspace consisting of all $v \in V$ such that $\beta(x, v) = 0$ for all $x \in X$. We call $V^\perp$ the radical of $\beta$ and denote it by $\text{rad } \beta$. We say that two elements $x, y \in$
V are orthogonal if $\beta(x, y) = 0$. We call subspaces $X, Y$ orthogonal if $X \subset Y^\perp$, and we write $X \perp Y$ in this case. A symplectic space $(V, \beta)$ is an orthogonal sum of subspaces $U_1, \ldots, U_k$ if $V = U_1 \oplus \cdots \oplus U_k$ and $U_i \perp U_j$ for all $i \neq j$. We use the symbol $V = U_1 \perp \cdots \perp U_k$ to denote an orthogonal decomposition of $(V, \beta)$. A hyperbolic plane $P$ is a 2-dimensional subspace of $V$ such that $\beta(x, y) = 1$ relative to a basis $\{x, y\}$ of $P$. The elements $x, y$ are called a hyperbolic pair. The structure theorem states

\begin{equation}
V = P_1 \perp \cdots \perp P_r \perp \text{rad } \beta.
\end{equation}

We call this splitting of $V$ a complete orthogonal decomposition of $(V, \beta)$. The number $r$ will be referred to as the width of $\beta$, denoted by $w(\beta)$.

Let us agree to write $\text{Alt}_r(G)$ for the set of alternating forms of width $r$. We identify $\widehat{G} \oplus \text{Alt}_0(G)$ with $\widehat{G}$. The set $\widehat{G} \oplus \text{Alt}_r(G)$ is visibly stable under $\mathbb{A}$. Using (4.5) one can see easily $\mathbb{A}$ acts transitively on $\text{Alt}_r(G)$ for every $r$. It follows that every orbit of $\mathbb{A}$ lies in $\widehat{G} \oplus \text{Alt}_r(G)$ for some $r$. A refinement of $\widehat{G} \oplus \text{Alt}_r(G)$ gives all orbits of $\mathbb{A}$.

**Proposition 4.5.** The orbits of $\mathbb{A}$ in $\widehat{G} \oplus \text{Alt}_r(G)$ are as follows:

(i) $\{0\}$ and $\widehat{G} \setminus \{0\}$ if $r = 0$;

(ii) $\{(0, \beta)\}$, $\{(\chi, \beta) | \text{rad } \beta \subset K_\chi\}$, $\{(\chi, \beta) | \text{rad } \beta \not\subset K_\chi\}$ for every $1 \leq r \leq \lfloor n/2 \rfloor$ for an odd $n$, or $1 \leq r < n/2$ for an even $n$, where $\beta$ runs over $\text{Alt}_r(G)$;

(iii) $\{(0, \beta)\}$ and $\{(\chi, \beta) | 0 \neq \chi\}$, where $\beta$ runs over $\text{Alt}_{n/2}$ if $n$ is even.

**Proof:** Pick $\chi \in \widehat{G}$. Let $x \in G$ be an element, unique modulo $K_\chi$, such that $\chi(x) = 1$ where 1 is the unity of $\mathbb{Z}_p$. Clearly $\chi$ is uniquely determined by a pair $(K_\chi, x)$. For any $\lambda \in \widehat{G}$ with an associated pair $(K_\lambda, z)$ the equality $\chi.\phi = \lambda.\phi \in \mathbb{A}$ holds iff $K_\chi.\phi = K_\lambda$ and $x.\phi = k + z$ for some $k \in K_\lambda$. On the other hand, $\beta, \gamma \in \text{Alt}(G)$ are related by $\beta.\phi = \gamma$ iff there is a decomposition (4.5) of $(V, \beta)$ satisfying $P_i.\phi$ is a hyperbolic plane for $\gamma$ for all $i$ and $(\text{rad } \beta).\phi = \text{rad } \gamma$.

Let $\langle X \rangle$ denote the subspace spanned by a subset $X \subset G$. Note $\mathbb{A}$ acts transitively on the set of pairs $(L, x)$ such that $G = L \oplus \langle x \rangle$ whence $\mathbb{A}$ acts transitively on $\widehat{G} \setminus \{0\}$ which proves (i). (iii) is a special case of the second set in (ii) as $\text{rad } \beta = 0$ for every $\beta$ of width $n/2$.

We take up part (ii). First, we show that all sets there are $\mathbb{A}$ invariant. It suffices to consider the property $\text{rad } \beta \subset \ker \chi$ of $(\chi, \beta)$. Let $(\lambda, \gamma) = (\chi, \beta).\phi$. Then $\beta.\phi = \gamma$ implies $(\text{rad } \beta).\phi = \text{rad } \gamma$. The
second condition $\lambda = \chi.\phi$ yields the equality $K_\chi \phi = K_\lambda$. Therefore $\text{rad} \gamma = (\text{rad} \beta)\phi \subset K_\chi \phi = K_\lambda$.

Second, we prove that each set in (ii) is a single orbit. We begin with \{$(\chi, \beta)$|rad $\beta \subset K_\chi$\}. Let $\chi$ denote the restriction of $\beta$ to $K_\chi$. Take a complete orthogonal decomposition $(K_\chi, \beta) = P_1 \perp \cdots \perp P_m \perp \text{rad} \beta$. Suppose $w(\beta) = r$. Then $\dim \text{rad} \beta = n - 2r$ while $\dim \text{rad} \beta_\chi = n - 1 - 2m$. Since rad $\beta \subset$ rad $\beta_\chi$ it follows that $m < r$. Therefore $\dim \text{rad} \beta_\chi \geq n - 1 - 2(r - 1) = n - 2r + 1 > \dim \text{rad} \beta$. Further select an $x \in \text{rad} \beta_\chi \setminus \text{rad} \beta$ and some $y \notin K_\chi$. Notice $x$ is not orthogonal to $y$ for else, as $G = K_\chi \langle y \rangle$, $x \in \text{rad} \beta$, a contradiction. Let $R = \text{rad} \beta_\chi$. Since $\beta(x, y) \neq 0$ the functional $\beta(-, y) : R \to \mathbb{Z}_p$, $r \mapsto \beta(r, y)$, $r \in R$ is nonzero. Therefore $R$ splits up as $R = \langle x \rangle \oplus \ker \beta(-, y)$. It is clear that $\ker \beta(-, y) = \text{rad} \beta$ which implies $\dim R = n - 1 - 2m = n - 2r + 1$ hence $m = r - 1$. Put $P = P_1 \oplus \cdots \oplus P_{r-1}$ and observe that the restriction of $\beta$ to $P$ is nondegenerate forcing $P \cap P_\perp = 0$. From this we obtain a decomposition $G = P \perp P_\perp$. Since the number $w(\beta)$ is an invariant of decompositions (4.5) and $\text{rad} \beta|_{P_\perp} = \text{rad} \beta$, we conclude that there is a single hyperbolic plane $P_r$ such that $P_\perp = P_r \perp \text{rad} \beta$. In consequence $R \cap P_\perp = (R \cap P_r) \perp \text{rad} \beta$ as rad $\beta \subset R$. Let $u, v$ be a hyperbolic pair in $P_r$ with $u \in R$. Then $v \notin K_\chi$, for otherwise $K_\chi \supset P_r$, and then $K_\chi = G$. We see that $G$ decomposes in two ways

\begin{align*}
(4.6) & \quad (G, \beta) = K_\chi \perp \langle v \rangle, \text{ and} \\
(4.7) & \quad (G, \beta) = P_1 \perp \cdots \perp P_{r-1} \perp P_r \perp \text{rad} \beta
\end{align*}

with $K_\chi = P_1 \oplus \cdots \oplus P_{r-1} \oplus \langle u, \text{rad} \beta \rangle$ and $P_r = \langle u, v \rangle$. Pick another element $(\lambda, \gamma)$ of the set. By (4.6),(4.7) $(G, \gamma) = Q_1 \perp \cdots \perp Q_r \perp \text{rad} \gamma = K_\lambda \perp \langle w \rangle$ with $Q_r = \langle z, w \rangle$ and $K_\lambda = Q_1 \oplus \cdots \oplus Q_{r-1} \oplus \langle z, \text{rad} \gamma \rangle$. Then any automorphism $\phi$ sending $P_i$ to $Q_i$ for $i = 1, \ldots, r - 1$, rad $\beta$ to rad $\gamma$, and $u \mapsto z, v \mapsto w$ carries $(\chi, \beta)$ to $(\lambda, \gamma)$.

Finally we show that any set \{$(\chi, \beta)$|rad $\beta \notin K_\chi$\} is a single orbit. Pick $(\chi, \beta)$ from the set, and let $(K_\chi, \beta) = P_1 \perp \cdots \perp P_m \perp \text{rad} \beta_\chi$ be a complete orthogonal decomposition of $(K_\chi, \beta)$. Select some $y \in \text{rad} \beta \setminus K_\chi$. Then $G = K_\chi \perp \langle y \rangle$, hence rad $\beta = \text{rad} \beta_\chi \oplus \langle y \rangle$. We see $(G, \beta) = P_1 \perp \cdots \perp P_m \perp (\text{rad} \beta_\chi \oplus \langle y \rangle)$ is a complete orthogonal decomposition of $G$. It becomes evident that $m = r$ and for any other pair $(\lambda, \gamma)$ from the set $(\chi, \beta), \phi = (\lambda, \gamma)$ for some $\phi \in \mathbb{A}$.

A simple count of the number of orbits yields the formula. \hfill \Box

5. Some Extensions of Dimension $p^4$

In this section $p$ is an odd prime and $G$ is an abelian group of order $\leq p^3$. When $|G| = p$, any action of $C_p$ on itself is trivial, hence
Ext($k^p, kC_p$) = Ext_{triv}($k^p, kC_p$) which by Theorem 4.4 has two isoclasses. Moreover, as Alt($C_p$) = 1 every $H \in$ Ext_{triv}($kC_p, k^p$) is cocommutative. By Proposition 3.17 part (6) $H = kC_p^2$ or $H = k(C_p \times C_p)$, and we derive part of [15, Theorem 2]. The case $|G| = p^2$, also due to A. Masuoka [14], will be dealt with below as specialization of a more general theory for $|G| = p^3$.

We assume that, unless stated otherwise, $|G| = p^3$. In the additive notation $G = \mathbb{Z}_p^3$ or $G = \mathbb{Z}_p^2 \oplus \mathbb{Z}_p$, and the theory splits into two parts.

(A) Suppose $G = \mathbb{Z}_p^3$. There are up to isomorphism two nontrivial $\mathbb{Z}_p C_p$-module structures on $G$. Let $R_i = \mathbb{Z}_p C_p / \langle (t - 1)^i \rangle$, $0 \leq i \leq p - 1$. Then either $G \simeq R_2 \oplus R_1$ or $G \simeq R_3$. Before proceeding to cases we make a notational change. We write $\alpha_k$ for the mapping $x \mapsto x^k$, $x \in C_p$ and $\alpha_k^{\circ}$ for $x^{p^k}$.

(I) Suppose $G \simeq R_2 \oplus R_1$, and let $\triangleleft$ be the action of $C_p$ on $G$ composed of regular actions of $C_p$ on $R_2$ and $R_1$. We aim to prove

**Theorem 5.1.** Ext_{\triangleleft}($k^p, kC_p$) contains $2p + 11$ isoclasses of extensions.

We break up proof in steps.

(1) Here we compute $\mathcal{X}(\triangleleft)$. Select a basis $\{e, g, f\}$ for $G$ where $\{e, f\}$ span $R_2$, and $R_1 = \mathbb{Z}_p g$ with the action

$$
e \triangleleft t = e + f, \; g \triangleleft t = g, \; f \triangleleft t = f.
$$

Clearly the matrix $T$ of $t$ in that basis is $T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Let

$$\{e^*, g^*, f^*\}$$

be the dual basis for $\widehat{G}$, and let $\wedge$ denote the multiplication in the Grassman algebra over $\widehat{G}$. We fix a basis $\{e^* \wedge g^*, e^* \wedge f^*, g^* \wedge f^*\}$ for $\widehat{G} \wedge \widehat{G}$, hence a basis $\{e^*, g^*, f^*, e^* \wedge g^*, e^* \wedge f^*, g^* \wedge f^*\}$ for $\widehat{G} \oplus \widehat{G} \wedge \widehat{G}$. We refer to the above bases as standard.

**Proposition 5.2.** $\mathcal{X}(\triangleleft) = \widehat{G}^p \oplus \widehat{G} \wedge \widehat{G} = \langle e^*, g^* \rangle \oplus \widehat{G} \wedge \widehat{G}$.

**Proof:** Recall $\mathcal{X}(\triangleleft) = \widehat{G}^p \cap \widehat{G} \wedge \widehat{G} / \forall(G) \oplus \text{Alt}_N(G)$. We use the well known identification Alt($G$) = $\widehat{G} \wedge \widehat{G}$. One can see easily that action of $t$ in $\widehat{G}$ is described by $T^t$ in the standard basis of $\widehat{G}$. By general principles [4, III, 8.5] the matrix of $t$ in the standard basis of $\widehat{G} \wedge \widehat{G}$ is $T^t \wedge T^{t^*} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}$. It follows that $(t - 1)^{p - 1} \bullet \widehat{G} = 0$ and $(t - 1)^{p - 1} \bullet \widehat{G} \wedge \widehat{G} = 0$, and
that is \( N(\hat{G}) = 0 \) and \((\hat{G} \wedge \hat{G})_N = \hat{G} \wedge \hat{G}\). Further, one can see easily \( \hat{G}^{C_p} = \langle e^*, g^* \rangle \).

(2) Group \( A(\langle \rangle) \). Identifying \( \phi \in A(\langle \rangle) \) with its matrix \( \Phi \) one has \( \Phi \in A(\langle \rangle) \) iff \( \Phi T = T \Phi \). This condition leads up to a determination of \( A(\langle \rangle) \), viz.

\[
(5.2) \quad A(\langle \rangle) = \left\{ \Phi \mid \Phi = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{11} \end{pmatrix}, \ a_{ij} \in \mathbb{Z}_p, \ a_{11}a_{22} \neq 0 \right\}
\]

(3) Orbits of \( A(\langle \rangle) \) in \( X(\langle \rangle) \). Since \( A(\langle \rangle) \) acts on \( \hat{G} \) by \((v^* \phi)(a) = v^*(a \phi^{-1}), v^* \in \hat{G} \), the matrix of \( \phi \) in the standard basis for \( \hat{G} \) is \((\Phi^{-1})^\text{tr}\). We prefer to use coordinates \( u, v, q, r, s \) for \( \Phi^{-1} \) where \( u = a_{11}^{-1}, v = a_{22}^{-1} \) and \( q = ua_{12}, r = ua_{13}, s = va_{23} \). A routine calculation gives

\[
(5.3) \quad (\Phi^{-1})^\text{tr} = \begin{pmatrix} u & 0 & 0 \\ -vq & v & 0 \\ u(qs - r) & -us & u \end{pmatrix}
\]

We treat the tuple \((u, v, q, r, s)\) as coordinates of either \( \phi \) or \( \Phi \). On general principles [4, III,8.5] the matrices of \( \phi \) in the standard bases for \( \hat{G} \) and \( \hat{G} \wedge \hat{G} \) are \((\Phi^{-1})^\text{tr} \) and \((\Phi^{-1})^\text{tr} \wedge (\Phi^{-1})^\text{tr}\), respectively. For \( \Phi \) defined by \((u, v, q, r, s)\) the result is

\[
(5.4) \quad (\Phi^{-1})^\text{tr} \wedge (\Phi^{-1})^\text{tr} = \begin{pmatrix} uv & 0 & 0 \\ -u^2s & u^2 & 0 \\ uvr & -uvq & uv \end{pmatrix}
\]

Regarding \( \mathbb{Z}_p \) as field we let \( \zeta \) denote a generator of \( \mathbb{Z}_p^* \). We observe a simple lemma

**Lemma 5.3.** There are two and four nonzero orbits of \( A(\langle \rangle) \) in \( \hat{G}^{C_p} \) and \( \hat{G} \wedge \hat{G} \), respectively.

**Proof:** We assign a vector \((a_1, a_2)\) to the element \( a_1e^* + a_2g^* \) of \( \hat{G}^{C_p} \) and likewise \((b_1, b_2, b_3)\) to \( b_1e^* \wedge g^* + b_2e^* \wedge f^* + b_3g^* \wedge f^* \). By (5.3) \((0, 1).A(\langle \rangle) = \{(a_1, a_2|a_2 \neq 0\}, \) and \((1, 0).A(\langle \rangle) = \{(a_1, 0)|a_1 \neq 0\} \). This proves the first claim.

Similarly, using (5.4) one can derive readily the equalities

\[
(0, 0, 1).A(\langle \rangle) = \{(b_1, b_2, b_3)|b_3 \neq 0\}, \ (1, 0, 0).A(\langle \rangle) = \{(b_1, 0, 0)|b_1 \neq 0\}.
\]

However, the set \( \{(b_1, b_2, 0)|b_2 \neq 0\} \) is union of two orbits. Namely, if \( b_2 \in \mathbb{Z}_p^* \), then by (5.4) \((b_1, b_2, 0) \in (0, 1, 0).A(\langle \rangle) \). But if \( b_2 \notin \mathbb{Z}_p^* \), then \( b_2 \in \zeta \mathbb{Z}_p \) which implies \((b_1, b_2, 0) \in (0, \zeta, 0).A(\langle \rangle) \). \( \square \)
We introduce notation
\[ \Omega'_0 = \{(0, 0)\}, \Omega'_1 = (1, 0).\mathbb{A}(\phi), \Omega'_2 = (0, 1).\mathbb{A}(\phi), \]
\[ \Omega''_0 = \{(0, 0)\}, \Omega''_1 = (1, 0, 0).\mathbb{A}(\phi), \Omega''_{2,0} = (0, 1, 0).\mathbb{A}(\phi), \]
\[ \Omega''_{2,1} = (0, \zeta, 0).\mathbb{A}(\phi), \Omega''_3 = (0, 0, 1).\mathbb{A}(\phi). \]

Some of products \( \Omega'_i \times \Omega''_j \) are orbits itself. We list those that are in

**Lemma 5.4.** The following sets are orbits
\[ \begin{align*}
(0) & \quad \Omega'_0 \times \Omega''_0 \quad \text{and} \quad \Omega'_i \times \Omega''_j, \quad j = 0, 1, (2, 0), (2, 1), 3, \quad i = 1, 2. \\
(1) & \quad \Omega'_1 \times \Omega''_1 \quad \text{and} \quad \Omega'_1 \times \Omega''_3. \\
(2) & \quad \Omega'_2 \times \Omega''_1, \quad \Omega'_2 \times \Omega''_{2,0} \quad \text{and} \quad \Omega'_2 \times \Omega''_{2,1}.
\end{align*} \]

**Proof:** Vectors \((a_1, a_2)\) and \((b_1, b_2, b_3)\) give rise to a concatenated vector \((a_1, a_2; b_1, b_2, b_3)\). The claim is that concatenating generators of \( \Omega'_i, \Omega''_j \) for \( i, j \) as in the Lemma we get a generator for \( \Omega'_i \times \Omega''_j \). We give details for \( \Omega'_1 \times \Omega''_3 \). Other cases are treated similarly. Combining (5.3) with (5.4) we obtain
\[ (1, 0; 0, 0, 1).\mathbb{A}(\phi) = \{(u, o; uv, −uv, uv)|uv \neq 0, q, r, s \text{ arbitrary}\} \]
Now for every element \((a_1, 0; b_1, b_2, b_3)\) \( \in \Omega'_1 \times \Omega''_3 \) the equations \( u = a_1, uv = b_3, uvr = b_1, −uvq = b_2 \) are obviously solvable, which completes the proof. \( \square \)

We pick up \( p - 1 \) additional orbits in

**Lemma 5.5.** Each set \( \Omega'_i \times \Omega''_{2,i}, i = 0, 1 \) is union of \((p - 1)/2 \) orbits.

**Proof:** Say \( i = 0 \). By definition \( \Omega'_1 \times \Omega''_{2,0} = \{(a_1, 0; b_1, b_2, 0)|a_1 \in \mathbb{Z}_p^*, b_2 \in \mathbb{Z}_p^2, b_1 \text{ arbitrary}\} \). For every \( m \in \mathbb{Z}_p^2 \) we let \( z_m = (1, 0; 0, m, 0) \). By (5.3) and (5.4) \( z_m.\phi = (u, 0; −u^2sm, u^2m, 0) \) where \( u, s \) are among parameters of \( \phi \). It is immediate that \( |z_m.\mathbb{A}(\phi)| = (p - 1)p, \) and one can verify equally directly that \( z_m.\mathbb{A}(\phi) \cap z_n.\mathbb{A}(\phi) = \emptyset \) for \( m \neq n \). Since \( |\Omega'_1 \times \Omega''_{2,0}| = \frac{(p-1)}{2}(p-1)p \) this case is done. For \( i = 1 \) one should take \( z'_m = (1, 0; 0, \zeta m, 0) \).

We summarize

**Lemma 5.6.** There are \( 2p + 11 \) orbits of \( \mathbb{A}(\phi) \) in \( \mathbb{X}(\phi) \).

**Proof:** The previous two lemmas give \( p + 11 \) orbits. The rest will come from splitting of the remaining set \( \Omega''_2 \times \Omega''_3 \). The latter is defined as \( \{(a_1, a_2; b_1, b_2, b_3)|a_2, b_3 \in \mathbb{Z}_p^*, a_1, b_1, b_2 \text{ arbitrary}\} \). For every \( k \in \mathbb{Z}_p \) we define \( w_k = (k, 1; 0, 0, 1) \). Again by (5.3) and (5.4) we have
\[ w_k.\mathbb{A}(\phi) = \{(uk − vq, v; uvr, −uvq, uv)\}. \]
There \( u, v \) run over \( \mathbb{Z}_p^* \) and \( r, q \) run over \( \mathbb{Z}_p \). One can see easily that 
\[
|w_k.\mathcal{A}(\prec)| = (p - 1)^2 p^2.
\]
Furthermore, we claim that \( w_k.\mathcal{A}(\prec) \cap w_l.\mathcal{A}(\prec) = \emptyset \) for \( k \neq l \).

For, suppose
\[
(u^k - vq, v; uwr, -uvq, uv) = (u'l - v'q', v'; u'v'r', -u'v'q', u'v')
\]
for some \((u, v, q, r)\) and \((u', v', q', r')\). Then \( v = v' \) and \( uv = u'v' \) give \( u = u' \). This implies \( q = q' \), \( r = r' \), and finally \( uk = ul \) yields \( k = l \), a contradiction. We conclude that \( |\bigcup_{0 \leq k \leq p-1} w_k.\mathcal{A}(\prec)| = p^3(p - 1)^2 \). As this is the number of elements in \( \Omega_2' \times \Omega_2' \), the proof is complete. \( \square \)

(4) Orbits of \( \mathcal{G}(\prec) \). By definition \( \mathcal{G}(\prec) \) is generated by \( \mathcal{A}(\prec) \) and a select set \( \{\lambda_k|2 \leq k \leq p - 1\} \) of automorphisms of \( G \). There \( \lambda_k \in I(\prec, \prec^k) \), and by (3.3) \( \lambda \in I(\prec, \prec^k) \) iff its matrix \( \Lambda \) satisfies
\[(5.5)\]
\[T\Lambda = \Lambda T^k.\]

Set \( \Lambda_k = \text{diag}(1, 1, k) \) (that is the diagonal matrix with entries 1, 1, \( k \)), and observe that \( \Lambda_k \) satisfies (5.5). We denote by \( \lambda_k \) the automorphism whose matrix is \( \Lambda_k \), and we set \( \omega_k = \lambda_k^-1 \). We move on to calculation of matrices of automorphisms \( \omega_k \). We set \( l = k^{-1} \pmod{p} \).

**Lemma 5.7.** Action of \( \omega_k \) is described by
\[
e^* \omega_k = le^*, \ g^* \omega_k = lg^*
\]
\[
e^* \wedge g^* \omega_k = le^* \wedge g^*
\]
\[
e^* \wedge f^* \omega_k = l^2 e^* \wedge f^*
\]
\[
g^* \wedge f^* \omega_k = -\left(\frac{1}{2}\right) e^* \wedge g^* + l^2 g^* \wedge f^*
\]

**Proof:** By (4.3) for \( \tau \in X(\prec) \), \( \tau.\omega_k = (\phi_i \bullet \tau).\lambda_k \). For \( \tau = e^*, g^*, e^* \wedge g^*, e^* \wedge f^* \phi_i \bullet \tau = l\tau \) as such \( \tau \) is fixed by \( C_p \). Because \( (t-1)^2 \tilde{G} \wedge \tilde{G} = 0 \) we expand \( \phi_i \) in powers of \( t - 1 \), namely \( \phi_i = l + \left(\frac{1}{2}\right)(t - 1) \) \( + \) higher terms.

We deduce
\[
\phi_i \bullet g^* \wedge f^* = lg^* \wedge f^* + \left(\frac{1}{2}\right)(t - 1) \bullet g^* \wedge f^* = lg^* \wedge f^* - \left(\frac{1}{2}\right) e^* \wedge g^*
\]

Further \( (\Lambda_k^{-1})^\text{tr} = \text{diag}(1, 1, k^{-1}) \) and \( (\Lambda_k^{-1})^\text{tr} \wedge (\Lambda_k^{-1})^\text{tr} = \text{diag}(1, k^{-1}, k^{-1}) \). These matrices describe action of \( \lambda_k \). Applying \( \lambda_k \) to \( \phi_i \bullet \tau \) as \( \tau \) runs over the standard basis of \( X(\prec) \) we complete the proof of the Lemma. \( \square \)

The next Proposition completes the proof of the Theorem.

**Proposition 5.8.** The set of \( \mathcal{G}(\prec) \)-orbits coincides with the set of \( \mathcal{A}(\prec) \)-orbits.
Proof: By Corollary 3.13 for every \( \tau \in \mathcal{X}(\vartriangle) \), \( \tau \mathcal{G}(\vartriangle) \) is union of orbits \( \tau \omega_k \mathcal{A}(\vartriangle) \) for \( 1 \leq k \leq p - 1 \). Thus it suffices to show \( \tau \omega_k \in \tau \mathcal{A}(\vartriangle) \) for every \( k \). We note that Lemma 5.7 implies that \( \omega_k \not\in \mathcal{A}(\vartriangle) \). Nevertheless, the inclusion \( \tau \omega_k \in \tau \mathcal{A}(\vartriangle) \) holds for generators \( \tau \) of every orbit described in Lemmas 5.4, 5.5, 5.6. We give a sample calculation for \( \tau = w_m = me^* + g^* + g^* \wedge f^* \) of Lemma 5.6. By Lemma 5.7

\[
w_m \omega_k = lme^* + lg^* - \left( \frac{l}{2} \right) e^* \wedge g^* + l^2 g^* \wedge f^*
\]

Now take \( \phi \) with coordinates \( u = l, v = l, r = -l^2 \left( \frac{l}{2} \right), q = s = 0 \). By (5.3) and (5.4) one sees immediately that \( w_m \phi = w_m \omega_k \).

We can quickly dispose of the case \( G = C_p \times C_p \) as promised above. Let \( \triangle \) denote the right regular action of \( C_p \) on \( R_2 \).

**Proposition 5.9.** ([14]) There are up to isomorphism \( p + 7 \) Hopf algebras in \( \text{Ext}(kC_p \times C_p, kC_p) \).

Proof: Since all nontrivial actions of \( C_p \) form a single isomorphism class we have

\[
\text{Ext}(kC_p \times C_p, kC_p) = \text{Ext}_{\triangle}(kC_p \times C_p, kC_p) \cup \text{Ext}_{\text{triv}}(kC_p \times C_p, kC_p).
\]

By Proposition 4.4 \( \text{Ext}_{\text{triv}}(kC_p \times C_p, kC_p) \) contributes four nonisomorphic algebras. It remains to show that \( \text{Ext}_{\triangle}(kC_p \times C_p, kC_p) \) contains \( p + 3 \) isoclasses.

Setting \( g = 0 \) in the definition of \( G \) reduces it to \( G = \mathbb{Z}_p \times \mathbb{Z}_p \) with \( G \simeq R_2 \) as \( C_p \)-module. Further reductions are as follows. The classifying space is \( \mathcal{X}(\triangle) = \langle e^* \rangle \oplus \langle e^* \wedge f^* \rangle \),

\[
\mathcal{A}(\triangle) = \left\{ \Phi \in \text{GL}(G) \mid \Phi = \begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{11} \end{pmatrix}, a_{11} \not= 0 \right\},
\]

and automorphisms \( \lambda_k \in I(\triangle, \mathcal{A}) \) are defined by \( \Lambda_k = \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix}, 1 \leq k \leq p - 1 \). It becomes apparent that elements \( \phi \) and \( \omega_k \) act on \( \mathcal{X}(\triangle) \) by

\[
(a, b) \phi = (ua, u^2b)
\]

\[
(a, b) \omega_k = (la, l^2b)
\]

where \( ae^* + be^* \wedge f^* \) is identified with \((a, b)\) and \( l = k^{-1} \) (mod \( p \)) as above. Thus the orbits of \( \mathcal{G}(\triangle) \) in \( \mathcal{X}(\triangle) \) coincide with those of \( \mathcal{A}(\triangle) \). For the latter we note that the \( \mathcal{A}(\triangle) \)-orbit of every vector \((a, b)\) with \( a, b \not= 0 \) has \( p - 1 \) elements, hence there are \( p - 1 \) orbits of this kind. The set \( \{(0, b) \mid b \not= 0\} \) is the union of two orbits, viz. \( \{(0, m) \mid m \in \mathbb{Z}_p \wedge 2\} \) and \( \{(0, \zeta m) \mid m \in \mathbb{Z}_p \wedge 2\} \), and two more orbits \( \{(0, 0)\}, \{(a, 0) \mid a \not= 0\} \) are supplied by the set \( \{(a, 0) \mid a \in \mathbb{Z}_p\} \).

We return to algebras of dimension \( p^4 \). We consider the case
(II) $G \simeq R_3$. We denote by $\triangleleft_r$ the right multiplication in $R_3$. This case is sensitive to prime $p$. Let us agree to write $\mathbb{X}(\triangleleft_r)$ as $\mathbb{X}_p$ if $G$ is a $p$-group. For $r \in \mathbb{Z}_pC_p$ we denote by $\pi$ the image of $r$ in $R_3$. The elements $e = 1, f = (t - 1), g = (t - 1)^2$ form a basis for $R_3$ in which action of $t$ is defined by $T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$. Let $\{e^*, f^*, g^*\}$ be the dual basis for $\hat{G}$, and $\{e^* \wedge f^*, e^* \wedge g^*, f^* \wedge g^*\}$ the induced basis for $\hat{G} \wedge \hat{G}$. We call all these bases standard. We aim to prove

**Theorem 5.10.** $\text{Ext}_{\mathbb{Z}_p}(\mathbb{C}_p, \mathbb{C}_p)$ contains $p + 9$ isoclasses, if $p > 3$, and four isoclasses if $p = 3$.

Proof will be carried out in steps.

(1) Space $\mathbb{X}_p(\triangleleft_r)$.

**Lemma 5.11.** If $p = 3$, then

$$\mathbb{X}_3 = \langle e^* \wedge f^*, e^* \wedge g^* \rangle$$

For every $p > 3$

$$\mathbb{X}_p = \mathbb{Z}_p e^* \oplus \hat{G} \wedge \hat{G}$$

**Proof:** The matrices of $t$ in the standard bases of $\hat{G}$ and $\hat{G} \wedge \hat{G}$ are $T_{tr}$ and $T_{tr} \wedge T_{tr}$, respectively, with $T_{tr} \wedge T_{tr} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$. From this one computes directly $(t - 1)^3 \bullet \hat{G} = (t - 1)^3 \bullet \hat{G} \wedge \hat{G} = 0$. Since $\phi_p(t) = (t - 1)^p - 1$, it follows that $N(G) = 0$ and $(\hat{G} \wedge \hat{G})_N = \hat{G} \wedge \hat{G}$ for any $p > 3$. Furthermore $\hat{G}^C_r = \mathbb{Z}_p e^*$ for every $p$. Thus as $\mathbb{X}_p = \hat{G}^C_r / N(G) \oplus (\hat{G} \wedge \hat{G})_N$ the second statement of the Lemma follows.

Say $p = 3$. Then $N(\hat{G}) = (t - 1)^2 \bullet \hat{G} = \mathbb{Z}_3 e^*$, hence $\hat{G}^C_r / N(\hat{G}) = 0$. Another verification gives $(\hat{G} \wedge \hat{G})_N = \langle e^* \wedge f^*, e^* \wedge g^* \rangle$. \hfill \Box

(2) Group $\mathbb{A}(\triangleleft_r)$. For any ring $R$ with a unity viewed as a right regular $R$-module and any right $R$-module $M$ the mapping $\lambda_M : M \rightarrow \text{Hom}_R(R, M)$ defined by $\lambda_M(m)(x) = mx, x \in R$ is an $R$-isomorphism. Set $M = R = R_3$, and pick $r = a_1 e + a_2 f + a_3 g$. The matrix of $\lambda_R(r)$ in the standard basis is $\Phi = \begin{pmatrix} a_1 & a_2 & a_3 \\ 0 & a_1 & a_2 \\ 0 & 0 & a_1 \end{pmatrix}$. From this it is evident that

$$\mathbb{A}(\triangleleft_r) = \left\{ \Phi \in GL(G) | \Phi = \begin{pmatrix} a_1 & a_2 & a_3 \\ 0 & a_1 & a_2 \\ 0 & 0 & a_1 \end{pmatrix}, a_i \in \mathbb{Z}_p, a_1 \neq 0 \right\}$$
Take $\phi = \lambda_{R_3}(r)$. Action of $\phi$ in $\hat{G}$ and $\hat{G} \wedge \hat{G}$ is described by $(\Phi^{-1})^\text{tr}$ and $(\Phi^{-1})^\text{tr} \wedge (\Phi^{-1})^\text{tr}$. Set $u = a_1^{-1}, q = ua_2, r = ua_3$. A routine calculation gives

\begin{equation}
(\Phi^{-1})^\text{tr} = \begin{pmatrix}
u & 0 & 0 \\
uq & u & 0 \
u(q^2 - r) & -uq & u
\end{pmatrix}
\end{equation}

\begin{equation}
(\Phi^{-1})^\text{tr} \wedge (\Phi^{-1})^\text{tr} = \begin{pmatrix}
u^2 & 0 & 0 \\
u^2q & u^2 & 0 \\
u^2r & -u^2q & u^2
\end{pmatrix}
\end{equation}

At this point it is convenient to determine a family of isomorphisms $\lambda_k : (G, q_r) \to (G, q_k)$. To this end, let us take $M = (R_3, q_k^R)$ with $2 \leq k \leq p - 1$. We set $\lambda_k = \lambda_M(e)$. By definition of $\lambda_k$ we have

$\lambda_k(e) = e, \lambda_k(f) = e(t^k - 1), \lambda_k(g) = e(t^k - 1)^2$

Using the expansion $t^k - 1 = k(t - 1) + \binom{k}{2}(t - 1)^2 \pmod{(t - 1)^3}$ we conclude that $\Lambda_k = \begin{pmatrix}1 & 0 & 0 \\0 & k & \binom{k}{2} \\0 & 0 & k^2\end{pmatrix}$ is the matrix of $\lambda_k$ in the standard basis. We shall need an explicit form of the associated matrices describing the action of $\lambda_k$ in $\hat{G}$ and $\hat{G} \wedge \hat{G}$, respectively. Put $l = k^{-1} \pmod{p}$ as usual. Then an easy calculation gives

\begin{equation}
(\Lambda_k^{-1})^\text{tr} = \begin{pmatrix}1 & 0 & 0 \\0 & l & 0 \\0 & \binom{l}{2} & l^2\end{pmatrix},
\end{equation}

\begin{equation}
(\Lambda_k^{-1})^\text{tr} \wedge (\Lambda_k^{-1})^\text{tr} = \begin{pmatrix}l & 0 & 0 \\\binom{l}{2} & l^2 & 0 \\0 & 0 & l^3\end{pmatrix}.
\end{equation}

Unless stated otherwise we assume below that $p > 3$. The degenerate case $p = 3$ follows easily from the general one.

(3) Orbits of $\mathbb{A}(q_r)$ in $\mathbb{X}_p$. We identify an element of $\mathbb{X}_p$ with its coordinate vector $(a; b_1, b_2, b_3)$ relative to the standard basis of $\mathbb{X}_p$. We start by fixing a family of orbits separately in $\hat{G}^{C_p}$ and $\hat{G} \wedge \hat{G}$.

These are

$\Omega'_0 = \{(0)\}, \Omega'_1 = \{(a)|a \neq 0\}, \Omega''_0 = \{(0, 0, 0)\}$, $\Omega''_i = \{(*, \ldots, *, \zeta^j b_i, 0, \ldots, 0)|b_i \in \mathbb{Z}_p^\ast\}, i = 1, 2, 3; j = 0, 1$
where the \( * \) denotes an arbitrary element of \( \mathbb{Z}_p \). For more complex orbits we need vectors \( v_i(m) = (m; 0, \ldots, m, 0, \ldots, 0) \) with the second \( m \) filling the \( i \)th slot, and \( m \) running over \( \mathbb{Z}_p^* \).

**Lemma 5.12.** There are \( 3p + 5 \) orbits of \( A(\omega) \) in \( X_p \). These are 
\[
\Omega'_0 \times \Omega''_0, \quad \Omega'_1 \times \Omega''_0, \quad \Omega'_0 \times \Omega''_1, \quad \text{and} \quad v_i(m)A(\omega), \quad i = 1, 2, 3, \quad j = 0, 1; \quad m \in \mathbb{Z}_p^*
\]

**Proof:** It is obvious that \( \Omega'_1 = (1)A(\omega) \). By (5.7) \( (0, \ldots, \zeta^j, 0, \ldots, 0) \phi = (\ast, \ldots, \ast, \zeta^j u^2, 0, \ldots, 0) \) for all \( i, j \) with the \( \ast \) denoting an arbitrary element of \( \mathbb{Z}_p \). This shows \( \Omega''_i = (0, \ldots, \zeta^j, 0, \ldots, 0)A(\omega) \), hence an orbit. Similarly, by (5.6) and (5.7) we have
\[
(5.10) \quad v_i(m)\phi = (um; \ast, \ldots, \ast, u^2m, 0, \ldots, 0).
\]

From this one can see easily that \( v_i(m)A(\omega) \) has \( (p - 1)p^{i-1} \) elements. Another verification gives \( v_i(m)A(\omega) \cap v_i(n)A(\omega) = \emptyset \) for \( m \neq n \). Set \( \Omega''_i = \Omega''_0 \cup \Omega''_1 \) and observe that \( |\Omega''_i| = (p - 1)p^{i-1} \) which gives \( |\Omega'_1 \times \Omega''_i| = (p - 1)^2p^{i-1} \). Evidently \( v_i(m) \in \Omega'_1 \times \Omega''_i \) for all \( m \) and therefore comparing cardinalities we arrive at the equality \( \Omega'_1 \times \Omega''_i = \bigcup_m v_i(m)A(\omega) \). But clearly \( X_p = \bigcup k \Omega'_k \times \Omega''_i, \quad k = 0, 1; 0 \leq i \leq 3 \) which completes the proof.

(4) Orbits of \( G(\omega) \). These are listed in

**Proposition 5.13.** In the foregoing notation the orbits of \( G(\omega) \) in \( X_p \) are as follows.
\[
\Omega'_0 \times \Omega''_0, \quad \Omega'_1 \times \Omega''_0, \quad \Omega'_0 \times \Omega''_1, \quad \Omega'_1 \times \Omega''_2, \\
\Omega'_0 \times \Omega''_3, \quad v_i(m)A(\omega), \quad \Omega'_1 \times \Omega''_2, \quad \Omega'_1 \times \Omega''_3
\]

where \( j = 0, 1 \) and \( m \) runs over \( \mathbb{Z}_p^* \).

**Proof:** In view of Corollary 3.13 we need to determine the \( A(\omega) \)-orbit containing \( v\omega_k \) where \( v \) runs over a set of generators of \( A(\omega) \)-orbits of Lemma 5.12, and \( \omega_k = \lambda_k \alpha_k^{-1}, 2 \leq k \leq p - 1 \), as usual.

(i) For \( A(\omega) \)-orbits \( \Omega'_1 \times \Omega''_0 \) and \( \Omega'_1 \times \Omega''_1 \) generators can be chosen as \( v_1 = (1; 0, 0, 0) \) and \( v_{ij} = (0; 0, \ldots, \zeta^j, 0, \ldots, 0) \), respectively. In view of \( e^* \) and \( f^* \) being fixed points for the action of \( t \), and by (5.8), (5.9) it is immediate that
\[
(5.11) \quad v_1 \omega_k = lv_1 \quad \text{and} \quad v_{1j} \omega_k = t^2v_{1j},
\]

hence those sets are \( G(\omega) \)-orbits.

Next we take \( v_{20} = e^* \wedge g^* \). Noting that \( (t - 1)^2 \cdot e^* \wedge g^* = 0 \), we use the expansion \( \phi_1 = l + \left( \frac{1}{2} \right)(t - 1) \mod (t - 1)^2 \) to derive
\[
\phi_1 \cdot e^* \wedge g^* = ce^* \wedge f^* + le^* \wedge g^*, \quad c \in \mathbb{Z}_p.
\]
Applying $\lambda_k$ to the last equation we find with the help from (5.9)

\begin{equation}
(5.12) \quad e^* \wedge g^* \omega_k = c'e^* \wedge f^* + l^3 e^* \wedge g^*, \text{ for some } c' \in \mathbb{Z}_p.
\end{equation}

The last equation shows that $\nu_{20}.\omega_k \in \nu_{21}.A(\zeta_r)$ if $l$, hence $k$, is not a square, and $\nu_{20}.\omega_k \in \nu_{20}.A(\zeta_r)$, otherwise. This means $\nu_{20}G(\zeta_r) = \Omega'_0 \times (\Omega''_{20} \cup \Omega''_{21})$, that is $\Omega'_0 \times \Omega''_2$ as needed.

(ii) For a generator $\nu_{3j} = (0; 0, 0, \zeta^j) = \zeta^j f^* \wedge g^*$ of $\Omega'_0 \times \Omega''_{3j}$, we claim that $\nu_{3j}.\omega_k \in \nu_{3j}.A(\zeta_r)$ for all $k$. Using the expansion $\phi_l = l + c_1(t - 1) + c_2(t - 1)^2 \pmod{(t - 1)^3}$ we derive $\phi_l \bullet f^* \wedge g^* = (c_1 + c_2)e^* \wedge f^* + c_1e^* \wedge g^* + lf^* \wedge g^*$. Applying $\lambda_k$ we have by (5.9)

\begin{equation}
(5.13) \quad f^* \wedge g^*.\omega_k = c'_1e^* \wedge f^* + c_1l^2 e^* \wedge g^* + l^4 f^* \wedge g^*, \quad c'_1, c_1 \in \mathbb{Z}_p.
\end{equation}

which shows $f^* \wedge g^*.\omega_k \in \Omega_{3j}$. As $\Omega_{3j} = \nu_{3j}.A(\zeta_r)$ by part (3) the claim follows.

(iii) We pause to mention that the above arguments settle the $p = 3$-case. For, since $X_3 = \langle e^* \wedge f^*, e^* \wedge g^* \rangle$, by part (i) it has three nonzero orbits, namely $\Omega''_{1j}$, $\Omega''_1$, $j = 0, 1$.

(iv) Here we take $\nu_1(m) = (m; m, 0, 0)$. Calculations in part (i) give $\nu_1(1).\omega_k = (lm; l^2m, 0, 0) \in \nu_1(m)A(\zeta_r)$ by (5.10). That is, $\nu_1(m)A(\zeta_r)$ is a $G(\zeta_r)$-orbit for every $m \in \mathbb{Z}_p^*$.

It remains to show that the last three sets of the Proposition are $G(\zeta_r)$-orbits.

(v) $\Omega'_{1} \times \Omega''_3$ is an orbit. By Lemma 5.12 $\Omega'_{1} \times \Omega''_3 = \bigcup_m \nu_2(m).A(\zeta_r)$ where $\nu_2(m) = me^* + me^* \wedge g^*$. Note that by (5.11) and (5.12) there holds $\nu_2(m).\omega_k = (lm; c', l^3m, 0)$. On the other hand we have by (5.10) $\nu_2(n).\phi = (un; a, u^2n, 0)$ where $u, a$ run over $\mathbb{Z}_p^*$ and $\mathbb{Z}_p$, respectively. For every $l$ choosing $n = l^{-1}m, u = l^2$ and $a = c'$ we obtain $\nu_2(m).\omega_k \in \nu_2(n)A(\zeta_r)$. Letting $l$ run over $\mathbb{Z}_p^*$ we see that $\bigcup_n \nu_2(n)A(\zeta_r) = \nu_2(m)A(\zeta_r)$ which completes the proof.

(vi) Here we show that each $\Omega'_{1} \times \Omega''_{3j}$ is an orbit. By (5.12) and (5.13)

\begin{equation}
(5.14) \quad \nu_3(m).\omega_k = \nu_3(n).\phi \text{ for some } \phi \in A(\zeta_r).
\end{equation}

We seek an $n$ such that

By (5.10) $\nu_3(n).\phi = (un; a, b, u^2n)$ with $a, b$ and $u$ taking arbitrary values in $\mathbb{Z}_p$ and $\mathbb{Z}_p^*$, respectively. Setting $u = l^3, n = l^{-2}m, a = c'$ and $b = c''$ fullfils (5.14). We see $\nu_3(m)G(\zeta_r) = \bigcup_{n \in m\mathbb{Z}_p^*} (n; 0, 0, 0)A(\zeta_r)$. 

On the other hand $\Omega'_1 \times \Omega''_{3j} = \bigcup_{n \in \mathbb{Z}_p^2} (n; 0, 0, n) \mathbb{A}(\varsigma_r)$ by comparing cardinalities of both sides.

Case (B) $G = \mathbb{Z}_p^2 \oplus \mathbb{Z}_p$ is more involved. There are 6 classes $[\varsigma]$ of actions each one with its own extension theory. The final result is that $\text{Ext}(kC_p, k^G)$ contains $3p + 19$ nonisomorphic algebras $2p + 7$ of which are neither commutative, nor cocommutative. The details of the proof will appear elsewhere.

Appendix: Crossed product splitting of $H$

**Proposition.** Let $H$ be an extension of $kF$ by $k^G$. Then $H$ is a crossed product of $kF$ over $k^G$.

**Proof:** First observe that $H$ is a Hopf-Galois extension of $k^G$ by $kF$ via $\rho_{\pi} = (\text{id} \otimes \pi)\Delta_H : H \to H \otimes kF$, see e.g. the proof of [17, 3.4.3], hence by [17, 8.1.7] $H$ is a strongly $F$-graded algebra. Setting $H_x = \{h \in H|\rho_{\pi}(h) = h \otimes x\}$ we have $H = \bigoplus_{x \in F} H_x$ with $H_1 = k^G$ and $H_xH_{x^{-1}} = k^G$ for all $x \in F$. Next for every $a \in G$ we construct elements $u(a) \in H_x$, $v(a) \in H_{x^{-1}}$ such that

$$u(a)v(a) = p_a, p_au(a) = u(a), v(a)p_a = v(a), \text{ and}$$

$$u(a)v(b) = 0 \text{ for all } a \neq b.$$ 

Indeed, were all $uv, u \in H_x, v \in H_{x^{-1}}$ lie in span$\{p_b|b \neq a\}$, then so would $H_xH_{x^{-1}}$, a contradiction. Therefore for every $a \in G$ there are $u \in H_x, v \in H_{x^{-1}}$ such that $uv = \sum c_b p_b, c_a \neq 0$. Setting $u(a) = \frac{1}{c_a} p_a u, v(a) = v p_a$ we get elements satisfying the first three properties stated above. Furthermore, the last property also holds because $u(a)v(b) = p_a u(a)v(b)p_b = p_a p_b u(a)v(b) = 0$. It follows that the elements $u_x = \sum_{a \in G} u(a), v_x = \sum_{a \in G} v(a)$ satisfy $u_x v_x = 1$ hence, as $H$ is finite-dimensional, $v_x u_x = 1$ as well. Thus $u_x$ is a 2-sided unit in $H_x$.

Now define $\chi : kF \to H$ by $\chi(x) = \frac{1}{\epsilon_H(u_x)} u_x$. One can see immediately that $\chi$ is a convolution invertible mapping satisfying $\rho_{\pi} \circ \chi = \chi \otimes \text{id}, \chi(1_F) = 1$ and $\epsilon_H \circ \chi = \epsilon_F$. Thus $\chi$ is a section of $kF$ in $H$, which completes the proof. \qed

**References**

[1] N. Andruskiewitsch, Notes on extensions of Hopf algebras, *Can. J. Math.* 48(1)(1996), 3-42.

[2] F. R. Beyl and J. Tappe, Group Extensions, Representations, and the Schur Multiplier, Lecture Notes in Mathematics 958, Springer-Verlag, 1982.
[3] R.J. Blatttner, M. Cohen and S. Montgomery, Crossed Product and Inner Actions of Hopf Algebras, *Trans. Amer. Math. Soc* **298**(2)(1986),671-711.
[4] N. Bourbaki, Elements of Mathematics, Algebra I, Springer-Verlag, 1989.
[5] N.P. Byott, Cleft extensions of Hopf algebras, *J. Algebra* **157**(1993),405-429.
[6] M. Hall, Jr., “The Theory of Groups”, The Macmillan Company, New York, 1959.
[7] I. Hofstetter, Extensions of Hopf algebras and their cohomological description, *J. Algebra* **164**(1994), 264-298.
[8] Y. Kashina, G. Mason, S. Montgomery, Computing the Frobenius-Schur indicator for abelian extensions of Hopf algebras, *J. Algebra* **251**(2002), 888-913.
[9] S. Lang, “Algebra”, Addison-Wesley, 1993.
[10] R.G. Larson and D.E. Radford, Semisimple cosemisimple Hopf algebras, *Amer. J. Math.* **110**(1988), 187-195.
[11] M. Mastnak, Hopf algebra extensions arising from semi-direct products of groups, *J. Algebra* **251**(2002), 413-434.
[12] S. MacLane, “Homology”, Die Grundlehren der Mathematischen Wissenschaften **114**, Springer-Verlag, 1963.
[13] A. Masuoka and Y. Doi, Generalization of cleft comodule algebras, *Comm. Algebra* **20**(1992), 3703-3721.
[14] A. Masuoka, Self-dual Hopf algebras of dimension $p^3$ obtained by extensions, *J. Algebra* **178**(1995), 791-806.
[15] A.Masuoka, The $p^n$ theorem for semisimple Hopf algebras, *Proc. Amer. Math. Soc.*, **124**(3)(1996), 735-737.
[16] A. Masuoka, Extensions of Hopf algebras (Lecture Notes, University of Cordoba, 1997) Notas Mat.No. 41/99, FaMAF Uni. Nacional de Cordoba, 1999.
[17] S. Montgomery, Hopf Algebras and their Actions on Rings, in: *CMBS Reg. Conf. Ser. Math.* **82**, AMS, 1993.
[18] C. Nastasescu and F. Van Oystaeyen, On strongly graded rings and crossed products, *Comm. Algebra* **10** (1982), 2085-2106.
[19] H.-J. Schneider, Some remarks on exact sequences of quantum groups, *Comm. Algebra* (9)**21**(1993), 3337-3358.
[20] H.-J. Schneider, A normal basis and transitivity of crossed products for Hopf algebras, *J. Algebra* **152**(1992), 289-312.
[21] D. Stefan, The set of Types of $n$-dimensional semisimple and cosemisimple Hopf algebras is finite, *J. Algebra* **193**(1997), 571-580.
[22] M. Takeuchi, Matched pairs of groups and bismash products of Hopf algebras, *Comm. Algebra* **9**(1981), 841-882.
[23] K. Yamazaki, On projective representations and ring extensions of finite groups, *J. Fac. Science Univ. Tokyo, Sect. I* **10**(1964), 147-195.

DePaul University, Chicago, IL 60614

E-mail address: lkrop@depaul.edu