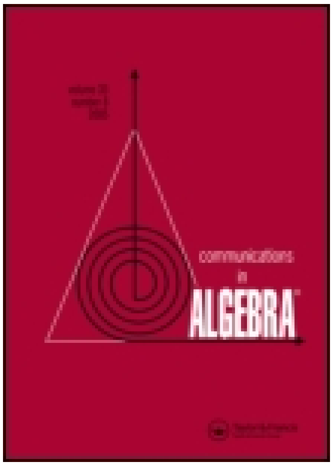

Communications in Algebra
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/lagb20

Cleft extensions for a hopf algebra generated by a nearly primitive element

Akira Masoka [a]

[a] Department of Mathematics , Shimane University , Shimane, 690, Japan

Published online: 27 Jun 2007.

COMMUNICATIONS IN ALGEBRA, 22(11), 4537-4559 (1994)

CLEFT EXTENSIONS FOR A HOPF ALGEBRA GENERATED BY A NEARLY PRIMITIVE ELEMENT

Akira MASUOKA
Department of Mathematics
Shimane University
Matsue, Shimane 690 JAPAN

The concept of cleft extensions, or equivalently of crossed products, for a Hopf algebra is a generalization of Galois extensions with normal basis and of crossed products for a group. The study of these subjects was founded independently by Blattner-Cohen-Montgomery [BCM] and by Doi-Takeuchi [DT1]. Afterward, Doi [D] improved the theory and determined, in particular, the isomorphic classes of cleft extensions for a certain commutative and cocommutative Hopf algebra. In this paper, we determine such classes of those for a non-commutative, non-cocommutative Hopf algebra A_N of free rank N^2, which is generated by a group-like g

and a (1,g)-primitive x. For example, the cyclic algebra will be seen to be a cleft extension for A_N over the ground ring.

In the course we do not depend on the general results in [D, § 2], but take a direct method using Bergman's results [B].

Throughout we work over a commutative ring R. Algebra, Hopf algebra, linear and $\otimes$ mean R-algebra, Hopf algebra over R, R-linear and $\otimes_R$, respectively.

§ 1 Preliminaries

In this section, for later use we recall some fundamental definitions and results on cleft extensions. The main reference is [D, § 1].

Let A be a Hopf algebra with coalgebra structure Δ, ε. Fix an algebra C.

A right A-comodule algebra B (with A-comodule structure $\rho : B \to B \otimes A$) is called an A-<u>cleft extension</u> over C [D, p.3056], if B contains C as coinvariant subalgebra, that is, $C = \{ b \in B \mid \rho(b) = b \otimes 1 \}$, and if there is such an A-comodule map $\phi : A \to B$ that is invertible under the convolution product $*$ [S, p.69]. In this case, ϕ can be chosen so as to be unitary ($\phi(1) = 1$) [DT1, p.813]. A unitary invertible A-comodule map $A \to B$ is called a <u>section</u> [D, p.3056].

We call a pair (B, ϕ) of an A-cleft extension B/C and a section ϕ a <u>cleft</u> <u>system</u> for A over C.

1.1 LEMMA. Let (B,ϕ) be a cleft system. A linear map $\phi' : A \to B$ is a section, if and only if there is a unitary invertible linear map $\gamma : A \to C$ such that $\phi' = \gamma * \phi$.

<u>Proof</u>. See the *proof of* [D, Lemma 2.1]. ∎

In general, an algebra B given an algebra map $C \to B$ is called a C-<u>ring</u> [B, p.195]. An A-cleft extension over C is a C-ring in an obvious way. An isomorphism $B \to B'$ between A-cleft extensions over C means an isomorphism of A-comodule C-rings (precisely, of A-comodules and of C-rings).

1.2 *DEFINITION. Denote by*

$$\mathrm{Cleft}(A, C)$$

the set of isomorphic classes of A-cleft extensions over C.

An A-cleft extension B/C is characterized as an A-Galois extension with normal basis [DT1, Thm.9], by which we mean that B is a right A-comodule algebra with coinvariant subalgebra C such that $b' \otimes b \mapsto b'\rho(b)$, $B \otimes_C B \to B \otimes A$ is an isomorphism and that there is a left C-module right A-comodule isomorphism $C \otimes A \simeq B$. This isomorphism is given by $c \otimes a \mapsto c\phi(a)$, if ϕ is a section.

1.3 LEMMA. Each A-comodule C-ring map $F : B \to B'$ between A-cleft extensions over C is an isomorphism.

Proof. Let $\phi : A \to B$ be a section. Then the composition $\phi' = F\phi : A \to B'$ is a section, too. The lemma follows from the commutative diagram:

$$\begin{tikzcd} & B \arrow[dd, "F"] \\ C \otimes A \arrow[ur, "\simeq"] \arrow[dr, "\simeq"'] & \\ & B' \end{tikzcd}$$

Here the isomorphisms are induced, as above, from ϕ, ϕ', respectively. ∎

A pair $(\rightharpoonup, \sigma)$ is called a crossed system for A over C [D, p.3055], if

$$\rightharpoonup \; : A \otimes C \to C$$

is a measuring action, if

$$\sigma : A \otimes A \to C$$

is an invertible linear map, and if these satisfy the normal condition

$$1 \rightharpoonup c = c \quad (c \in C)$$

$$\sigma(a,1) = \varepsilon(a)1 = \sigma(1,a) \quad (a \in A)$$

as well as the twisted module condition, the cocycle condition described in [D, (1),(2)].

From a cleft system (B, ϕ), a crossed system $(\rightharpoonup, \sigma)$ is obtained as follows:

$$a \rightharpoonup c = \Sigma\, \phi(a_1)\, c\, \phi^{-1}(a_2)$$

$$\sigma(a,a') = \Sigma\, \phi(a_1)\, \phi(a_1')\, \phi^{-1}(a_2 a_2')$$

where $\Delta(a) = \Sigma\, a_1 \otimes a_2$, as usual.

Conversely, let $(\rightharpoonup, \sigma)$ be a crossed system and define a bilinear product on the R-module $C \star A = C \otimes A$ by

$$(c \star a)(c' \star a') = \sum c(a_1 \rightharpoonup c')\sigma(a_2, a_1') \star a_3 a_2'$$

for $c, c' \in C$, $a, a' \in A$. Then $C \star A$ with A-coaction $c \star a \mapsto \sum (c \star a_1) \otimes a_2$ is a right A-comodule algebra, called a <u>crossed product</u>. Furthermore, $C \star A$ and $a \mapsto 1 \star a$, $A \to C \star A$ form a cleft system for A over $C = C \star R$. See [BM, Thm.1.18], [D, Prop.1.1].

1.4 PROPOSITION. These give a 1-1 correspondence between the isomorphic classes of cleft systems and the crossed systems (both for A over C). (An isomorphism of cleft systems means an A-comodule C-ring isomorphism consistent with the sections.)

<u>Proof</u>. This is essentially shown in [D, Prop.1.1; Thm.1.2]. ∎

An A-cleft extension B/C is said to be <u>twisted</u> (respectively, <u>smashed</u>), if $B \simeq C \star A$, a crossed product such that $\rightharpoonup$ (respectively, σ) is trivial. See [D, p.3056; p.3059].

§ 2 Cleft Extensions for A_N

We fix an integer N such that $N \geq 2$ and suppose R contains a root ζ of the N-th cyclotomic polynomial over $\mathbb{Z}$ [L, VIII, § 3]. Hence $\zeta^N = 1$ and there is a ring map $\mathbf{Z}[\zeta_N] \to R$, sending a primitive N-th root $\zeta_N \in \mathbf{C}$ of 1 to ζ. Note that ζ may not be a primitive N-th root of 1. For example ζ may be 1, if N is a power of a prime p and ch R = p.

2.1 DEFINITION. Let i, n be integers such that $0 \leq i \leq n$. We denote by

$$\binom{n}{i}$$

the element in R got by putting $q = \zeta$ into the Gauss polynomial

$$\binom{n}{i}_q = \frac{(q^n - 1)\ldots.(q^{n-i+1} - 1)}{(q^i - 1)\ldots.(q - 1)} .$$

2.2 LEMMA. 1) If $0 < i < N$, then $\binom{N}{i} = 0$.

2) If $0 < i < n$, then $\binom{n}{i} = \binom{n-1}{i-1} + \zeta^i \binom{n-1}{i}$.

<u>Proof</u>. 1) This follows, since $\binom{N}{i}_q = 0$ $(0 < i < N)$ if $q = \zeta_N$. 2) This is well-known. ∎

2.3 DEFINITION. Denote by

$$A_N \quad \text{or} \quad A_{N,\zeta}$$

the Hopf algebra defined as follows. As an algebra, this is generated by g, x with the relations:

r1) $g^N = 1$; r2) $x^N = 0$; r3) $xg = \zeta gx$.

The coalgebra structure is determined by:

$$\Delta(g) = g \otimes g, \quad \varepsilon(g) = 1$$

$$\Delta(x) = x \otimes g + 1 \otimes x, \ \varepsilon(x) = 0$$

(Recall that such an x is called <u>nearly primitive</u>, or more precisely (1,g)-primitive.) In fact A_N is a Hopf algebra whose antipode is the algebra anti-endomorphism determined by:

$$S(g) = g^{N-1}, \quad S(x) = -\zeta^{-1}g^{N-1}x$$

(We remark that $S^{2N} = 1$.)

To understand A_N adequately, one sees there are Hopf algebra quotients

$$A_{fr} \to A_\infty \to A_N.$$

Here

$$A_{fr} = R\{g,g^{-1},x\}/(gg^{-1}-1,\ g^{-1}g-1),$$

the (free) Hopf algebra defined in [S, Example-Exercise, p.89],

$$A_\infty = A_{fr}/(xg - \zeta gx)$$

(which is defined for any $\zeta \in R$), and finally

$$A_N = A_\infty/(g^N - 1,\ x^N).$$

Note that in a Hopf algebra an ideal generated by nearly primitives is a Hopf ideal.

2.4 REMARK. 1) A_N is a particular one of Taft's Hopf algebra [T], which is in fact generated by several group-likes $g, g_2, \ldots, g_n$ and x as above. A_2 was previously defined by Sweedler.

2) Let q be a unit in R such that $\zeta = q^{-2}$. Then A_∞ is regarded as a quantized enveloping algebra of the Lie algebra of upper triangular matrices in $sl(2)$ and, if $q - q^{-1}$ is a unit, this is a Hopf subalgebra of $U_q(sl(2))$.

2.5 LEMMA. 1) A_N is a free R-module with a basis $g^m x^n$, $0 \leq m, n < N$, of N^2 elements.

2) $\Delta(g^m x^n) = \sum_{i=0}^{n} \binom{n}{i} g^m x^{n-i} \otimes g^{m+n-i} x^i \quad (0 \leq m, n < N)$

Proof. 1) This is shown by applying the Bergman Theorem [B, Thm.1.2].

2) If $wz = \zeta zw$ in an algebra, then

$$(z + w)^n = \sum_{i=0}^{n} \binom{n}{i} z^{n-i} w^i.$$

Apply this to the sum $\Delta(x) = x \otimes g + 1 \otimes x$. ∎

Part 1) yields that A_N is not cocommutative as a coalgebra and that, if $\zeta \neq 1$, A_N is not commutative as an algebra.

Let E be an algebra. Denote by $E^\times$ the group of units in E.

2.6 LEMMA. A linear map $\gamma : A_N \to E$ is invertible, if and only if $\gamma(g^m) \in E^\times$ for all $m = 0, 1, .., N-1$.

Proof. "Only if". $\gamma(g^m)^{-1}$ is given by $\gamma^{-1}(g^m)$.

"If". By (2.5.2), $\gamma^{-1}(g^m x^n)$ is given inductively on n by

$$-\gamma(g^m)^{-1} \sum_{0}^{n-1} \binom{n}{i} \gamma(g^m x^{n-i})\ \gamma^{-1}(g^{m+n-i} x^i)$$

or equally by

$$-\sum_{1}^{n} \binom{n}{i} \gamma^{-1}(g^m x^{n-i})\ \gamma(g^{m+n-i} x^i)\ \gamma(g^{m+n})^{-1}. \quad ∎$$

In the following, we fix an algebra C to determine the set $\mathrm{Cleft}(A_N, C)$.

First, let (B, ϕ) be a cleft system for A_N over C and $(\triangleright, \sigma)$ the corresponding crossed system.

Write:

$$G = \phi(g), \quad X = \phi(x) \tag{2.7}$$

Set:

$$\left\{\begin{array}{ll} \alpha(c) = g \triangleright c = GcG^{-1} & \\ \delta(c) = x \triangleright c = [X,c]G^{-1} & (c \in C) \\ u = G^N & \\ a = X^N & \\ b = (\sigma(x,g) - \zeta\, \sigma(g,x))\, \sigma(g,g)^{-1} & \end{array}\right. \tag{2.8}$$

Here we use the usual bracket product: $[X,c] = Xc - cX$.

2.9 LEMMA. 1) $\alpha : C \to C$ is an algebra automorphism.

2) $\delta : C \to C$ is a $(1,\alpha)$-derivation, that is, a linear endomorphism such that

$$\delta(cc') = \delta(c)\alpha(c') + c\, \delta(c') \quad (c, c' \in C).$$

3) $u \in C^{\times}$, $a, b \in C$.

4) The following are fulfilled:

R1) $G^N = u$

R2) $X^N = a$

R3) $XG = \zeta\, GX + bG^2$

R4) $Gc = \alpha(c)G \qquad (c \in C)$

R5) $Xc = cX + \delta(c)G$

Proof. 1), 2). Easy.

3) By definition, $b \in C$. To show $u, a \in C$, we see through the A_N-coaction

$$u = G^N \mapsto G^N \otimes g^N = u \otimes 1,$$

$$a = X^N \mapsto \sum_{i=0}^{N} \binom{N}{i} X^{N-i} \otimes g^{N-i}x^i = a \otimes 1 \quad \text{(by (2.2.1))}.$$

4) R1), R2), R4) and R5) follow by the Definitions (2.8). R3) follows by some simple calculation. ∎

In turn, take α, δ, b arbitrarily, where α, δ $\in$ End C, the algebra of linear endomorphisms, and $b \in C$.

2.10 DEFINITION. Let $0 \leq n \leq N$.

1) Define $k_n = k_n(\alpha, \delta, b) \in C$ inductively by:

$$k_0 = 1$$

$$k_n = \delta(k_{n-1}) + k_{n-1}(b + \zeta\, \alpha(b) + \ldots + \zeta^{n-1}\alpha^{n-1}(b))$$
$$(n \geq 1)$$

2) Define $h_n(c) = h_n(\alpha, \delta, b, c) \in$ End C by:

$$h_0(c) = c, \quad h_1(c) = \delta(c)$$

$$h_n(c) = \delta\, h_{n-1}(c) + h_{n-1}(c)(b + \zeta\, \alpha(b) + \ldots + \zeta^{n-2}\alpha^{n-2}(b))$$
$$(n \geq 2)$$

Later in (2.15), we will apply Bergman's result [B, Prop.7.1], a generalization of his theorem quoted in the proof of (2.5.1). For this purpose, in the next lemma we regard R3)-R5) as a reduction system for the free algebra generated by elements G, X and the R-module C, that is, the tensor algebra $T(M)$ on $M = RG \oplus RX \oplus C$. Precisely, we regard R5), for example, as the linear endomorphisms r_{P-Q} of $T(M)$ defined as follows, where P, Q are iterated tensor products of RG, RX, C. r_{P-Q} is defined on the summand $P \otimes RX \otimes C \otimes Q$ by $r_{P-Q}(pXcq) = p(cX + \delta(c)G)q$ $(c \in C,$

$p \in P$, $q \in Q$), while r_{P-Q} is identical on the summands other than $P \otimes RX \otimes C \otimes Q$. See [B, (22),(23)].

2.11 LEMMA. Suppose the reduction system R3)-R5) for $T(M)$ is given. Let $1 \leq n \leq N$.

1) XG^n is reduced to

$$\zeta^n G^n X + (b + \zeta\ \alpha(b) + \ldots + \zeta^{n-1}\alpha^{n-1}(b))G^{n+1}.$$

2) $X^{n-1}(\zeta GX + bG^2)$ is reduced to

$$\sum_{i=0}^{n} \zeta^{n-i}\binom{n}{i}k_i G^{i+1}X^{n-i}.$$

In particular, $X^{N-1}(\zeta GX + bG^2)$ to $G^N X + k_N G^{N+1}$.

3) $X^{n-1}(cX + \delta(c)G)$ $(c \in C)$ is reduced to

$$\sum_{i=0}^{n} \binom{n}{i} h_i(c) G^i X^{n-i}.$$

In particular, $X^{N-1}(cX + \delta(c)G)$ to $cX^N + h_N(c)G^N$.

Proof. Induction on n.

1) Case $n = 1$. OK by R3).

Case $n > 1$. Suppose the result for $n-1$ holds. Then we have the following reductions:

$$\begin{aligned} XG^n &\mapsto \zeta^{n-1}G^{n-1}XG \\ &\quad + (b + \zeta\ \alpha(b) + \ldots + \zeta^{n-2}\alpha^{n-2}(b))G^n G \\ &\underset{R3)}{\mapsto} \zeta^{n-1}G^{n-1}(\zeta\ GX + bG^2) \\ &\quad + (b + \zeta\ \alpha(b) + \ldots + \zeta^{n-2}\alpha^{n-2}(b))G^{n+1} \\ &\underset{R4)}{\mapsto} \zeta^n G^n X + \zeta^{n-1}\alpha^{n-1}(b)G^{n+1} \\ &\quad + (b + \zeta\ \alpha(b) + \ldots + \zeta^{n-2}\alpha^{n-2}(b))G^{n+1} \\ &= \zeta^n G^n X + (b + \zeta\ \alpha(b) + \ldots + \zeta^{n-1}\alpha^{n-1}(b))G^{n+1} \end{aligned}$$

Thus the result for n holds.

2) Case $n = 1$. Trivial.

Case $n > 1$. Suppose the result for $n-1$ holds.

Then:

$$X^{n-1}(\zeta GX + bG^2) \mapsto \sum_0^{n-1} \zeta^{n-1-i}\binom{n-1}{i} Xk_i G^{i+1}X^{n-1-i}$$

$$\underset{R5)}{\mapsto} \sum_0^{n-1} \zeta^{n-1-i}\binom{n-1}{i}(k_i X + \delta(k_i)G)G^{i+1}X^{n-1-i}$$

$$\underset{1)}{\mapsto} \sum_0^{n-1} \zeta^{n-1-i}\binom{n-1}{i}k_i$$
$$\times(\zeta^{i+1}G^{i+1}X + (b + \dots + \zeta^i\alpha^i(b))G^{i+2})X^{n-1-i}$$
$$+ \sum_0^{n-1} \zeta^{n-1-i}\binom{n-1}{i} \delta(k_i)G^{i+2}X^{n-1-i}$$

$$= \sum_0^{n-1} \zeta^{n-1-i}\binom{n-1}{i}k_{i+1}G^{i+2}X^{n-1-i}$$
$$+ \sum_0^{n-1} \zeta^{n}\binom{n-1}{i}k_i G^{i+1}X^{n-i} \quad \text{(by (2.10.1))}$$

$$= \sum_0^{n} \zeta^{n-i}\binom{n}{i}k_i G^{i+1}X^{n-i} \quad \text{(by (2.2.2))}$$

Thus the result for n holds.

3) Similar. ∎

2.12 DEFINITION. A 5-tuple $\underline{d} = (\alpha, \delta, u, a, b)$ is called <u>cleft</u> <u>data</u> for A_N over C, if the following D0)-D7) are fulfilled:

D0) $\alpha : C \to C$ is an algebra automorphism, $\delta : C \to C$ a $(1, \alpha)$-derivation, and $u \in C^\times$, a, $b \in C$.

D1) $\alpha(u) = u$

D2) $\delta(u) = (b + \zeta\,\alpha(b) + \dots + \zeta^{N-1}\alpha^{N-1}(b))\,u$

D3) $\delta(a) = 0$

D4) $a - \alpha(a) = k_N(\alpha, \delta, b)u$

D5) $\alpha^N(c) = ucu^{-1}$

D6) $b\alpha^2(c) - \alpha(c)b = (\delta\ \alpha - \zeta\ \alpha\ \delta)(c) \qquad (c \in C)$

D7) $[a,c] = h_N(\alpha, \delta, b, c)u$

We denote the set of all such data by

$$\mathfrak{D} = \mathfrak{D}(A_N, C).$$

2.13 EXAMPLE. 1) Take $\alpha = 1$, $\delta = 0$. (Then $k_N = 0$, $h_n = 0$ $(n > 0)$.) $d = (1,0,u,a,b)$ is cleft data, if and only if $u \in Z(C)^\times$, a, $b \in Z(C)$, the center of C.

2) Take $u = 1$, $a = b = 0$. (Then $k_n = 0$, $h_n(c) = \delta^n(c)$ $(n > 0)$.) $\underline{d} = (\alpha, \delta, 1, 0, 0)$ is cleft data, if and only if α is an algebra automorphism, δ a $(1,\alpha)$-derivation, $\alpha^N = 1$, $\delta^N = 0$, and $\delta\ \alpha = \zeta\ \alpha\ \delta$.

2.14 DEFINITION. Let $\underline{d} = (\alpha, \delta, u, a, b) \in \mathfrak{D}$. Define a pair $(B_{\underline{d}}, \phi_{\underline{d}})$ as follows: $B_{\underline{d}}$ is the C-ring generated by G, X with the relations R1)-R5). $\phi_{\underline{d}} : A_N \to B_{\underline{d}}$ is the linear map defined by

$$\phi_{\underline{d}}(g^m x^n) = G^m X^n \quad (0 \leq m,\ n < N).$$

2.15 PROPOSITION. Let $\underline{d} \in \mathfrak{D}$.

1) $B_{\underline{d}}$ is a free left C-module with a basis

$$G^m X^n \quad (0 \leq m,\ n < N).$$

In particular, we have $C \subset B$.

2) $B_{\underline{d}}$ has a right A_N-comodule algebra structure determined by

$$G \mapsto G \otimes g, \quad X \mapsto X \otimes g + 1 \otimes x.$$

The coinvariant subalgebra equals C.

3) $\phi_{\underline{d}}$ is a section.

Thus $(B_{\underline{d}}, \phi_{\underline{d}})$ is a cleft system for A_N over C.

Proof. 1) We apply the left version of Bergman [B, Prop.7.1], in which we should replace the base ring $\mathbb{Z}$ by R.

We introduce a total ordering $\leq$ into the set of words consisting of G, X. Define $G < X$. For two words W, W', set $W < W'$, if either Length $W <$ Length W' or if Length $W =$ Length W' and W precedes W' under lexicographic ordering. This $\leq$ is consistent with R1)-R5) in the sense of [B, p.198, lines -10, -9] and satisfies the descending chain condition. Let R') be the reduction system for the tensor algebra $T(M)$ $(M = RG \oplus RX \oplus C)$ which consists of R1)-R5) and

R6) $c \cdot c'$ = the product of c and c' in C $(c, c' \in C)$

(see [B, (21)]). To show 1), by the left version of [B, Prop.7.1] it suffices to prove that all ambiguities of R') are resolvable. There are no inclusion ambiguities. We have the following overlap ambiguities:

(G^i, G^{N-i}, G^i), (X^i, X^{N-i}, X^i) $(0 < i < N)$

(X, G, G^{N-1}), (X^{N-1}, X, G)

(G^{N-1}, G, c), (X^{N-1}, X, c), (X, G, c)

(G, c, c'), (X, c, c') $(c, c' \in C)$

Here we omit the ways of reductions, since they seem obvious. For example, by saying (X, G, G^{N-1}) is resolvable we mean that $(\zeta GX + bG^2)G^{N-1}$ and Xu can be reduced to the same expression through R1)-R5).

This is resolvable in fact by D2) and (2.11.1). So is (X^{N-1}, X, G) by D4), (2.11.2), (X^{N-1}, X, c) by D7), (2.11.3), (G^i, G^{N-i}, G^i) by D1), (X^i, X^{N-i}, X^i) by D3), (G^{N-1}, G, c) by D5), (X, G, c) by D6), and finally (G, c, c') and (X, c, c') by D0).

2), 3). One sees directly that the algebra map $B_{\underline{d}} \to B_{\underline{d}} \otimes A_N$ defined in 2) is a well-defined A_N-comodule structure and that $\phi_{\underline{d}}$ is an A_N-comodule map. By (2.6), $\phi_{\underline{d}}$ is invertible since G is invertible in $B_{\underline{d}}$. By 1), $c \otimes a \mapsto c\phi_{\underline{d}}(a)$, $C \otimes A_N \to B_{\underline{d}}$ is a unitary, C-module and A_N-comodule isomorphism. Hence the coinvariant subalgebra equals C. ∎

2.16 EXAMPLE. Take $\alpha = 1$, $\delta = 0$, $u, a \in R^\times$, $b = 0$. Then one sees from (2.13.1), (2.15) that the cyclic algebra $\left(\frac{u,a}{R,\zeta}\right)$ [P, p.284] with a natural A_N-coaction is a (twisted) A_N-cleft extension over R.

2.17 PROPOSITION. Any A_N-cleft extension B over C is isomorphic with $B_{\underline{d}}$ for some $\underline{d} \in \mathfrak{D}$.

Proof. Suppose (B, ϕ) is a cleft system. Set G, X as in (2.7), $\underline{d} = (\alpha, \delta, u, a, b)$ as in (2.8). By (2.9), one traces the proof of (2.15.1) in reverse to see that $\underline{d}$ is cleft data. For example, for D2) one sees:

$$\begin{aligned}
uX + \delta(u)G &= Xu \quad \text{(by R5))} \\
&= XG^N \quad \text{(by R1))} \\
&= G^N X + (b + \zeta\,\alpha(b) + \dots + \zeta^{N-1}\alpha^{N-1}(b))G^{N+1} \\
&\qquad\qquad \text{(by R3),R4),(2.11.1))} \\
&= uX + (b + \zeta\,\alpha(b) + \dots + \zeta^{N-1}\alpha^{N-1}(b))uG \quad \text{(by R1))}
\end{aligned}$$

By (2.9) again, one has a natural A_N-comodule C-ring map $B_{\underline{d}} \to B$. This is an isomorphism by (1.3). ∎

2.18 DEFINITION. Suppose $\alpha, \delta \in \mathrm{End}\ C$, $b, t \in C$. Let $0 \leq n \leq N$. Define

$$p_n = p_n(\alpha, \delta, b, t) \in C$$

inductively by

$$p_0 = 1, \quad p_1 = t$$

$$p_n = (t\alpha + \delta)(p_{n-1}) + p_{n-1}(b + \zeta\, \alpha(b) + \ldots + \zeta^{n-2}\alpha^{n-2}(b))$$
$(n \geq 2)$

2.19 LEMMA. Let $\underline{d}, \underline{d}', \underline{d}'' \in \mathfrak{D}$.

1) Let $F : B_{\underline{d}'} \to B_{\underline{d}}$ be an isomorphism of A_N-comodule C-rings. Then there is a unique pair $(v, t) \in C^\times \times C$ such that

$$F(G') = vG, \quad F(X') = X + tG. \tag{2.20}$$

2) Let $(v, t) \in C^\times \times C$. Then the C-ring map $F : B_{\underline{d}'} \to B_{\underline{d}}$ determined by (2.20) is well-defined, if and only if

$$\left\{\begin{aligned} \alpha'(c) &= v\alpha(c)v^{-1} \\ \delta'(c) &= \{(t\alpha + \delta)(c) - ct\}v^{-1} \\ u' &= v\alpha(v)\ldots\alpha^{N-1}(v)u \\ a' &= a + p_N(\alpha, \delta, b, t)u \\ b' &= \{vb + (t\alpha + \delta)(v) - \zeta\, v\alpha(t)\}(v\alpha(v))^{-1} \end{aligned}\right. \quad (c \in C) \tag{2.21}$$

where $\underline{d} = (\alpha, \ldots\ldots)$, $\underline{d}' = (\alpha', \ldots\ldots)$. In this case, F is an A_N-comodule isomorphism.

3) Let $F' : B_{\underline{d}''} \to B_{\underline{d}'}$, $F : B_{\underline{d}'} \to B_{\underline{d}}$ be isomorphisms of A_N-comodule C-rings determined as in 1) by

(w,s), $(v,t) \in C^{\times} \times C$, respectively. Then the composition FF' is determined by $(wv, sv + t)$.

Proof. 1) $F\phi_{\underline{d}'}$, $\phi_{\underline{d}}$ are sections $A_N \to B_{\underline{d}}$. Hence by (1.1) there is a unitary, invertible linear map $\gamma : A_N \to C$ such that $F\phi_{\underline{d}'} = \gamma * \phi_{\underline{d}}$. Set $v = \gamma(g) \in C^{\times}$, $t = \gamma(x) \in C$. Then one sees easily that (2.20) holds. The uniqueness is obvious.

2) This is verified directly. For example, F is consistent with R2), if and only if $a' = (X + tG)^N$. Since one sees inductively that

$$(X + tG)^n = \sum_{i=0}^{n} \binom{n}{i} p_i G^i X^{n-i} \quad (0 \leq n \leq N),$$

the 4 th condition in (2.21) follows.

3) Easy. ∎

The group $C^{\times}$ acts on the additive group C by the right multiplication. So we have the group $C^{\times} \ltimes C$ of semi-direct product with the multiplication

$$(w \ltimes s)(v \ltimes t) = wv \ltimes (sv + t).$$

2.22 PROPOSITION. 1) $C^{\times} \ltimes C$ acts on the set $\mathfrak{D}$ from the left with the action

$$\underline{d}' = (v \ltimes t)\underline{d}$$

defined by (2.21).

2) Suppose d, $d' \in \mathfrak{D}$. Then $B_{\underline{d}} \simeq B_{\underline{d}'}$, if and only if $\underline{d}$ and $\underline{d}'$ are $C^{\times} \ltimes C$-equivalent.

Proof. 1) If $\underline{d} \in \mathfrak{D}$, then $\underline{d}'$ defined by (2.21) is contained in $\mathfrak{D}$. In fact, by the proof of

(2.19.1) $\underline{d}'$ is cleft data comming from a cleft system $(B_{\underline{d}}, \phi)$, where $\phi(g) = vG$, $\phi(x) = X + tG$.

Suppose $\underline{d}'' = (w \ltimes s)\underline{d}'$ in addition. Then by (2.19.2) we have the isomorphisms

$$F' : B_{\underline{d}''} \to B_{\underline{d}'}, \quad F : B_{\underline{d}'} \to B_{\underline{d}}.$$

By (2.19.3) the composition FF' is determined by $(w \ltimes s)(v \ltimes t)$. Hence by (2.19.2)

$$\underline{d}'' = ((w \ltimes s)(v \ltimes t))\underline{d} ,$$

so $C^\times \ltimes C$ acts as a group.

2) This follows by (2.19.1), (2.19.2). ∎

2.23 THEOREM. $d \mapsto B_{\underline{d}}$ gives a 1-1 correspondence between the set $C^\times \ltimes C \backslash \mathfrak{D}(A_N, C)$ of $C^\times \ltimes C$-orbits in $\mathfrak{D}(A_N, C)$ and the set $\mathrm{Cleft}(A_N, C)$ of isomorphic classes of A_N-cleft extensions over C.

<u>Proof</u>. This follows by (2.17), (2.22.2). ∎

2.24 PROPOSITION. Let $\underline{d} = (\alpha, \delta, u, a, b) \in \mathfrak{D}$.

1) $B_{\underline{d}}$ is twisted, if and only if there exist $v \in C^\times$, $t \in C$ such that

$$\alpha(c) = vcv^{-1} \quad (\alpha \text{ is inner})$$
$$\delta(c) = [t,c]v^{-1}$$

for $c \in C$. (Such δ may be called an inner $(1,\alpha)$-derivation.)

2) $B_{\underline{d}}$ is smashed, if and only if there exist $v \in C^\times$, $t \in C$ such that

$$u = \alpha^{N-1}(v) \dots \alpha(v)v$$
$$a = -p_N(\alpha, \delta, b, t)u$$

$$b = \zeta\ \alpha(t) + (\delta(v) - vt)\ \alpha(v)^{-1}.$$

<u>Proof</u>. Let $\underline{d}' \in \mathfrak{D}$ and $(\rightharpoonup, \sigma)$ be the crossed system corresponding to $(B_{\underline{d}'}, \phi_{\underline{d}'})$. Then it is easy to see:

$$\rightharpoonup \text{ is trivial} \Leftrightarrow \alpha' = 1,\ \delta' = 0$$
$$\sigma \text{ is trivial} \Leftrightarrow u' = 1,\ a' = b' = 0$$

1) This follows by [D, Thm.2.3], but here we show directly.

By (2.19), the equivalent condition follows by setting $\alpha' = 1$, $\delta' = 0$ in the first two equations in (2.21) and replacing v, t by v^{-1}, tv^{-1}, respectively (or equally, by setting $\alpha = 1$, $\delta = 0$ there and deleting the primes).

2) Similarly, set $u' = 1$, $a' = b' = 0$ in the last three equations in (2.21) and replace v by v^{-1}. ∎

It follows from (2.13.1) that any A_N-twisted extension B/C comes from such an extension E over $Z(C)$, that is, $B \simeq C \otimes_{Z(C)} E$. (Note $Z(C) \subset Z(E)$.)

§ 3 Cleft Extensions for A_2

Suppose $N = 2$ in § 2 (then $\zeta = -1$). We had better choose b in (2.8) rather as $b = \sigma(x,g) + \sigma(g,x)$. Under this change, we summarize the results. We also describe in (3.4) all crossed systems.

Define the Hopf algebra A_2 as in (2.3), setting $N = 2$, $\zeta = -1$. We need not assume anything on R.

A_2 is R-free with a basis 1, g, x, gx.

3.1 DEFINITION. A 5-tuple $\underline{d} = (\alpha, \delta, u, a, b)$ is called <u>cleft data</u> for A_2 over a fixed algebra C, if the following are fulfilled:

D0) $\alpha : C \to C$ is an algebra automorphism, $\delta : C \to C$ a $(1,\alpha)$-derivation, $u \in C^\times$, $a, b \in C$.

D1) $\alpha(u) = u$ D2) $\delta(u) = b - \alpha(b)$

D3) $\delta(a) = 0$ D4) $\delta(b) = a - \alpha(a)$

D5) $\alpha^2(c) = ucu^{-1}$

D6) $bc - \alpha(c)b = (\alpha\,\delta + \delta\,\alpha)(c)u$ $(c \in C)$

D7) $[a,c] = \delta(c)b + \delta^2(c)u$

We denote by $\mathfrak{D} = \mathfrak{D}(A_2, C)$ the set of all such data.

$C^\times \ltimes C$ acts on $\mathfrak{D}$ by

$$\underline{d}' = (v \ltimes t)\underline{d},$$

where

$$\begin{aligned} \alpha'(c) &= v\alpha(c)v^{-1} \\ \delta'(c) &= \{(t\alpha + \delta)(c) - ct\}v^{-1} \end{aligned} \qquad (c \in C)$$

$$u' = v\alpha(v)u$$

$$a' = a + tb + (t\alpha + \delta)(t)u$$

$$b' = vb + \{(t\alpha + \delta)(v) + v\alpha(t)\}u .$$

3.2 DEFINITION. Let $\underline{d} \in \mathfrak{D}$. Denote by

$$B_{\underline{d}}$$

the A_2-cleft exension over C defined as follows. As a C-ring $B_{\underline{d}}$ is generated by G, X with the relations:

R1) $G^2 = u$ R2) $X^2 = a$ R3) $XG = -GX + b$

R4) $Gc = \alpha(c)G$ R5) $Xc = cX + \delta(c)G$ $(c \in C)$

The A_2-comodule algebra structure of $B_{\underline{d}}$ is determined by $G \mapsto G \otimes g$, $X \mapsto X \otimes g + 1 \otimes x$.

In fact $B_{\underline{d}}$ is an A_2-extension over C with a canonical section $\phi_{\underline{d}} : A_2 \to B_{\underline{d}}$ defined by $\phi_{\underline{d}}(g) = G$, $\phi_{\underline{d}}(x) = X$, $\phi_{\underline{d}}(gx) = GX$.

3.3 THEOREM. $d \mapsto B_{\underline{d}}$ gives a 1-1 correspondence between $C^{\times} \ltimes C \setminus \mathfrak{D}(A_2, C)$ and $\mathrm{Cleft}(A_2, C)$.

3.4 PROPOSITION. There is a 1-1 correspondence between the set $\mathfrak{D} \times C$ and the set of crossed systems for A_2 over C. Here $(\alpha, \delta, u, a, b, s) \in \mathfrak{D} \times C$ corresponds to the crossed system $(\rightharpoonup, \sigma)$ defined as follows:

$$\begin{aligned} g \rightharpoonup c &= \alpha(c), \quad x \rightharpoonup c = \delta(c) \\ gx \rightharpoonup c &= \alpha\,\delta(c)u + sc - \alpha(c)s \end{aligned} \qquad (c \in C)$$

TABLE OF $\sigma(\flat, \#)$

$\flat \backslash \#$	g	x	gx
g	u	s	$\alpha(s)$
x	$b + s$	a	$-\alpha(a) + \delta(s)$
gx	$\alpha(b) + s$	$\alpha(a)$	$-ua + \alpha\,\delta(s)u$ $-\alpha(b+s)s$

Proof. For $s \in C$, define a linear map $\gamma_s : A_2 \to C$ by $\gamma_s(1) = \gamma_s(g) = 1$, $\gamma_s(x) = 0$, $\gamma_s(gx) = s$. Then one sees from the proof of (2.17) that $(\underline{d}, s) \mapsto (B_{\underline{d}}, \gamma_s * \phi_{\underline{d}})$ gives a 1-1 correspondence between $\mathfrak{D} \times C$

and the isomorphic classes of cleft systems. Hence the Proposition follows by (1.4) and some direct calculation. ∎

ACKNOWLEDGMENTS

I would like to thank Yukio Doi and Mitsuhiro Takeuchi. Professor Doi brought me the problem of determing Cleft(A_2, C), which motivated me to do this research. Professor Takeuchi gave me valuable comments, reading an earlier manuscript. In particular, He improved Lemma 1.3, dropping the assumption that the antipode of A was bijective. Following his suggestion, I added Remark 2.4 2) and the explanation after Definition 2.3 when I revised the paper.

REFERENCES

[B] G. Bergman, The diamond lemma for ring theory, Adv. in Math. 29(1978), 178-218.

[BCM] R. Blattner, M. Cohen and S. Montgomery, Crossed products and inner actions of Hopf algebras, Trans. Amer. Math. Soc. 298(1986), 671-711.

[BM] R. Blattner and S. Montgomery, Crossed products and Galois extensions of Hopf algebras, Pacific J. of Math. 137(1989), 37-54.

[D] Y. Doi, Equivalent crossed products for a Hopf algebra, Comm. Algebra 17(1989), 3053-3085.

[DT1] Y. Doi and M. Takeuchi, Cleft comodule algebras for a bialgebra, Comm. Algebra 14(1986), 801-817.

[DT2] Y. Doi and M. Takeuchi, Hopf-Galois extensions of algebras, the Miyashita-Ulbrich actions, and Azumaya algebras, J. Algebra 121(1989), 488-516.

[K] M. Koppinen, A duality theorem for crossed products of Hopf algebras, J. Algebra 146(1992), 153-174.

[L] S. Lang, "Algebra", Addison-Wesley, Reading, Massachusetts, 1965.

[P] R. Pierce, "Associative Algebras", GTM 88, Springer, New York-Heidelberg-Berlin, 1982.

[S] M. Sweedler, "Hopf Algebras", Benjamin, New York, 1969.

[T] E. Taft, The order of the antipode of finite-dimensional Hopf algebra, Proc. Nat. Acad. Sci. USA 68(1971), 2631-2633.

Received: July 1993

Revised: August 1993