

SURVEY ON MATCHED PAIRS OF GROUPS— AN ELEMENTARY APPROACH TO THE ESS-LYZ THEORY

MITSUHIRO TAKEUCHI

Institute of Mathematics, University of Tsukuba, Tsukuba, Japan

E-mail: akira@math.tsukuba.ac.jp

Abstract. The theory of matched pairs of groups is surveyed with special interest in applications to braided groups and quasitriangular structures on the bi-smash product Hopf algebra.

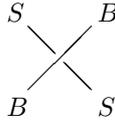
Introduction. In 1981, I introduced the notion of a matched pair of groups (S, B) and defined the bi-smash product Hopf algebra $(kS)^* \otimes kB$ over a field k , when S is a finite group [T], motivated by W. M. Singer's work [Si] on Hopf algebra extensions. Later, S. Majid [Mj] extended and applied this work in the study of quantum groups. Further, the cohomology theory of matched pairs of Hopf algebras was studied by I. Hofstetter [H] and A. Masuoka [Ms1], [Ms2]. During this research, Masuoka found out that the notion of a matched pair of groups had been obtained essentially by G. I. Kac [K] in 1968 and that the cohomology theory of matched pairs of groups had been studied there.

Recently, some interesting progress in the study of matched pairs of groups has been made by two groups of algebraists, ESS (Etingof, Schedler, Soloviev) and LYZ (Lu, Yan, Zhu), during their study of set-theoretical solutions of the Yang-Baxter equation. Especially, the group ESS [ESS] has obtained some deep results on classification of finite braided sets. In this survey, I give an elementary and diagrammatic approach to the introductory part of the ESS-LYZ theory. This will enable the reader to appreciate their deeper results (which are not discussed here) more easily. On the other hand, the latter group LYZ has obtained some interesting construction of quasitriangular structures on the bi-smash product Hopf algebra $H(S, B) = (kS)^* \otimes kB$ [LYZ2]. I also give a natural categorical explanation of this construction, based on Masuoka's observation [Ms3].

In §1, we review the notion of a matched pair of groups (S, B) and matched product $B \bowtie S$, and explain the matched pair condition by means of diagrams of the form

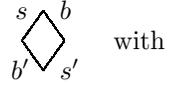
2000 *Mathematics Subject Classification*: 16W35, 18D10.

The paper is in final form and no version of it will be published elsewhere.



motivated by [LYZ1]. This idea is used throughout the paper.

We describe the structure of $H(S, B)$ in terms of jigsaw puzzle pieces edges decorated by elements in S and B .



In §2, we introduce the notion of a braided group as the group version of a braided set. It is a matched pair of groups of the form (G, G) and appears implicitly in [LYZ1]. The works [ESS], [So] are written in terms of 1-cocycle data which are equivalent to our braided groups. We briefly review the equivalence of these two notions.

In §3, we review the construction of the structure group G_X of a braided set X , and interpret the results of [LYZ1] to show that G_X becomes a braided group. Let (G_X, N_X, π_X) be the 1-cocycle datum corresponding to this braided group. Soloviev [So] has presented the group N_X by generators and relations. We give an elementary proof of this presentation.

In §4, we define an LYZ pair $\xi, \eta : S \rightarrow B$ for a matched pair of groups (S, B) . LYZ pairs are characterized by:

- (a) ξ and η can be extended to group homomorphisms

$$\bar{\xi}, \bar{\eta} : B \bowtie S \rightarrow B$$

which are identity on B ,

- (b) every element of $\text{Ker}(\bar{\xi})$ commutes with every element of $\text{Ker}(\bar{\eta})$.

If (ξ, η) is an LYZ pair for (S, B) , it induces a braided group structure on S (Theorem 4.5), and this enables us to combine the study of LYZ pairs with our previous consideration of braided groups, especially leading to the construction of the universal LYZ pair and study of minimal LYZ pairs in §5.

Let S be a braided group. We show (Proposition 5.1) that there is a unique matched pair structure on $(S, S \bowtie S)$ such that the injections

$$\text{in}_2, \text{in}_1 : S \rightarrow S \bowtie S$$

form an LYZ pair. Further this pair $(\text{in}_2, \text{in}_1)$ enjoys some universality.

We call an LYZ pair (ξ, η) minimal if they are group isomorphisms $S \xrightarrow{\sim} B$, because if this is the case (and the groups are finite), the corresponding quasitriangular Hopf algebra $H(S, B)$ is minimal. To study minimal LYZ pairs, it is enough to assume $S = B$ and $\eta = \text{id}$. This leads to the notion of a ξ -braided group which means a pair of a braided group S and its group automorphism ξ such that (ξ, id) is an LYZ pair for (S, S) . This condition is easy to describe and admits to define the notion of a ξ -braided set (X, ξ) as its set version. We generalize some of the previous results on braided sets and groups to ξ -braided sets and groups.

In §6, we review the construction of a quasitriangular structure on $H(S, B)$ from an LYZ pair (ξ, η) [LYZ2]. We give some nice categorical interpretation to the braiding

structure on the category of right $H(S, B)$ modules $\mathcal{M}_{H(S, B)}$ associated to the LYZ pair (ξ, η) . The original idea is due to Masuoka [Ms3]. The monoidal category $\mathcal{M}_{H(S, B)}$ is monoidally equivalent to some category ${}^G_B\mathcal{M}_B$, with $G = B \bowtie S$. Masuoka has constructed a natural braiding on ${}^G_B\mathcal{M}_B$ from a pair of group projections $\bar{\xi}, \bar{\eta} : G \rightarrow B$ whose kernels commute with each other element-wise. The LYZ braiding is simply the transport of the Masuoka braiding through the monoidal equivalence.

1. Matched pairs of groups

DEFINITION 1.1 ([T]). A *matched pair of groups* means a triple (S, B, σ) where S and B are groups and

$$\sigma : S \times B \rightarrow B \times S, \quad (s, b) \mapsto (s \rightarrow b, s \leftarrow b)$$

is a map satisfying the conditions

- (1.1) $s \rightarrow (t \rightarrow b) = st \rightarrow b,$
- (1.2) $st \leftarrow b = (s \leftarrow (t \rightarrow b))(t \leftarrow b),$
- (1.3) $(s \leftarrow b) \leftarrow c = s \leftarrow bc,$
- (1.4) $s \rightarrow bc = (s \rightarrow b)((s \leftarrow b) \rightarrow c)$

for $s, t \in S, b, c \in B$.

The product $B \times S$ forms a group with product

$$(1.5) \quad (b, s)(c, t) = (b(s \rightarrow c), (s \leftarrow c)t).$$

This group is denoted by $B \bowtie S$. Conversely, if B and S are subgroups of a group G such that the product map $B \times S \rightarrow G$ is bijective, then (S, B) forms a matched pair with structure $\sigma(s, b) = (s \rightarrow b, s \leftarrow b)$ defined by $sb = (s \rightarrow b)(s \leftarrow b)$.

The structure map σ of a matched pair (S, B) is bijective. The triple (B, S, σ^{-1}) forms a matched pair, called the opposite of (S, B) . The group $S \bowtie B$ is isomorphic to $B \bowtie S$ by $(s, b) \mapsto (1, s)(b, 1)$.

Let $s, s' \in S$ and $b, b' \in B$. We denote the relation

$$(1.6) \quad (b', s') = \sigma(s, b)$$

by the diagram

$$(1.7) \quad \begin{array}{ccc} s & & b \\ & \searrow & / \\ & & s' \\ & / & \searrow \\ b' & & \end{array} \quad \text{or} \quad \begin{array}{ccc} b' & & s' \\ & \searrow & / \\ & & s \\ & / & \searrow \\ s & & b \end{array} .$$

The structure map $\sigma : S \times B \rightarrow B \times S$ is non-degenerate in the sense of [ESS], [LYZ1]. Hence if we choose (s, b) (resp. (s, b') , resp. (b', s') , resp. (b, s')), then the rest elements (b', s') (resp. (b, s') , resp. (s, b) , resp. (s, b')) are determined by diagram (1.7).

Characterization of matched pairs of groups by group factorizations yields that (1.7) implies

$$(1.8) \quad \begin{array}{ccc} s^{-1} & b' & \\ & \diagdown & \diagup \\ & & (s')^{-1} \\ b & & \end{array}, \quad \begin{array}{ccc} s' & b^{-1} & \\ & \diagdown & \diagup \\ & & s \\ (b')^{-1} & & \end{array}, \quad \begin{array}{ccc} b^{-1} & s^{-1} & \\ & \diagdown & \diagup \\ & & (s')^{-1} \\ (s')^{-1} & & (b')^{-1} \end{array}.$$

The diagrammatic notation yields the following simple expression of conditions (1.1)–(1.4) (cf. [LYZ1], (4), (5)).

PROPOSITION 1.2. *Conditions (1.1)–(1.4) are equivalent to:*

$$(1.9) \quad \begin{array}{ccc} s & t & b \\ & \diagdown & \diagup \\ b' & & s' \\ & & t' \end{array} \Rightarrow \begin{array}{ccc} st & b & \\ & \diagdown & \diagup \\ b' & & s't' \end{array},$$

$$(1.10) \quad \begin{array}{ccc} s & b & c \\ & \diagdown & \diagup \\ b' & & c' \\ & & s' \end{array} \Rightarrow \begin{array}{ccc} s & bc & \\ & \diagdown & \diagup \\ b'c' & & s' \end{array}.$$

Proof. The assumption of (1.9) implies $b' = s \rightarrow (t \rightarrow b)$, $s' = s \leftarrow (t \rightarrow b)$, $t' = t \leftarrow b$. Hence (1.9) is equivalent to (1.1) and (1.2). Similarly, (1.10) is equivalent to (1.3) and (1.4). ■

Let k be a field and let (S, B) be a matched pair of groups where S is a finite group. Let $H = kB$ be the group Hopf algebra and $K = (kS)^*$ the dual group Hopf algebra. The right action $S \leftarrow B$ induces a left action of B on K , making a left H module algebra K . The left action $S \rightarrow B$ makes H into a right K comodule coalgebra. The pair (H, K) becomes an abelian matched pair of Hopf algebras in the sense of [T, 1.1], hence the smash product algebra and the co-smash product coalgebra structures on $K \otimes H$ give rise to a Hopf algebra called the *bi-smash product* [T, 1.4]. We denote this bi-smash product Hopf algebra by $H(S, B)$. This is denoted as $k(S) \blacktriangleright \blacktriangleleft kB$ by Majid [Mj, 6.2.1].

The structures on $H(S, B)$ are described as follows (cf. [Mj, Fig. 6.2 and 6.3]). We prepare the set \mathcal{S} of jigsaw puzzle pieces

$$(1.11) \quad \begin{array}{ccc} s & b \\ \diagdown & \diagup \\ b' & s' \end{array} \quad \text{where} \quad \begin{array}{ccc} s & b \\ \diagdown & \diagup \\ b' & s' \end{array} \quad \text{with } s, s' \text{ in } S, b, b' \text{ in } B.$$

Each piece has 4 edges decorated by 2 elements in S and 2 elements in B as above. The decoration is determined by decorating any two adjacent edges freely. In other words, there are four canonical bijections between \mathcal{S} and $S \times B$. In this sense, we may drop decoration of some edges as follows:

$$\begin{array}{ccc} s & b \\ \diagdown & \diagup \\ b' & s' \end{array} = \begin{array}{ccc} s & b \\ \diagdown & \diagup \\ & \end{array} = \begin{array}{ccc} s & \\ \diagdown & \diagup \\ b' & \end{array} = \dots \quad \text{etc.}$$

Two pieces $\begin{matrix} s & b \\ & \diamond \\ b' & s' \end{matrix}$ and $\begin{matrix} t & c \\ & \diamond \\ c' & t' \end{matrix}$ are called *S-composable* if $s' = t$. If this is the case, $\begin{matrix} s & bc \\ & \diamond \\ b'c' & t' \end{matrix}$ is a piece in \mathcal{S} by (1.10), called the *S-composition*. Similarly, the *B-composition* of two *B-composable* pieces is defined by using (1.9).

Conversely, given a piece $\begin{matrix} s & b \\ & \diamond \\ b' & s' \end{matrix}$ in \mathcal{S} , we may consider the set of *B-composable* pairs of pieces whose *B-composition* is $\begin{matrix} s & b \\ & \diamond \\ b' & s' \end{matrix}$. Such a pair is called a *B-decomposition* of $\begin{matrix} s & b \\ & \diamond \\ b' & s' \end{matrix}$. A *B-decomposition* of $\begin{matrix} s & b \\ & \diamond \\ b' & s' \end{matrix}$ is in 1-1 correspondence with a decomposition $s = tu$ in S or a decomposition $s' = t'u'$ in S as follows. If $s = tu$, the pair of pieces in \mathcal{S}

$$\begin{matrix} t & \\ & \diamond \\ b' & \end{matrix}, \quad \begin{matrix} u & b \\ & \diamond \\ & \end{matrix}$$

is a *B-decomposition* of $\begin{matrix} s & b \\ & \diamond \\ b' & s' \end{matrix}$. Similarly, if $s' = t'u'$, then the pair

$$\begin{matrix} & \\ & \diamond \\ b' & t' \end{matrix}, \quad \begin{matrix} & b \\ & \diamond \\ & u' \end{matrix}$$

is a *B-decomposition*.

With these preliminaries, we describe the Hopf algebra structure of $H(S, B)$ as follows.

(1.12) $H(S, B)$ has a basis \mathcal{S} over k .

(1.13) *The algebra structure.*

$$\begin{matrix} s & b \\ & \diamond \\ b' & s' \end{matrix} \cdot \begin{matrix} t & c \\ & \diamond \\ c' & t' \end{matrix} = \begin{cases} \begin{matrix} s & bc \\ & \diamond \\ b'c' & t' \end{matrix} & \text{if } s' = t, \\ 0 & \text{otherwise,} \end{cases}$$

$$\text{the unit} = \sum_{s \in S} \begin{matrix} s & 1 \\ & \diamond \\ 1 & s \end{matrix}.$$

Note that $\begin{matrix} s & 1 \\ & \diamond \\ 1 & s \end{matrix}$, $s \in S$, give rise to orthogonal idempotents.

(1.14) *The coalgebra structure.*

$$\Delta \left(\begin{array}{c} s & b \\ \diamond & \\ b' & s' \end{array} \right) = \sum_{s=tu} \begin{array}{c} t \\ \diamond \\ b' \end{array} \otimes \begin{array}{c} u & b \\ \diamond & \\ & u' \end{array} = \sum_{s'=t'u'} \begin{array}{c} \diamond \\ b' & t' \end{array} \otimes \begin{array}{c} b \\ \diamond \\ u' \end{array},$$

the sum over all B -decompositions of $\begin{array}{c} s & b \\ \diamond & \\ b' & s' \end{array}$,

$$\varepsilon \left(\begin{array}{c} s & b \\ \diamond & \\ b' & s' \end{array} \right) = \delta_{s,1} = \delta_{s',1}.$$

(1.15) *The antipode.*

$$S \left(\begin{array}{c} s & b \\ \diamond & \\ b' & s' \end{array} \right) = \begin{array}{c} (s')^{-1} & (b')^{-1} \\ \diamond & \\ b^{-1} & s^{-1} \end{array}.$$

The above description will be used in §6.

2. Braided groups

DEFINITION 2.1. A *braided group* means a pair (G, σ) where G is a group and $\sigma : G \times G \rightarrow G \times G$ is a map such that

- (2.1) the triple (G, G, σ) forms a matched pair of groups,
- (2.2) if $(y', x') = \sigma(x, y)$, then $y'x' = xy$ for $x, y, x', y' \in G$.

Obviously, (2.2) is equivalent to saying that

$$\text{mult} : G \bowtie G \rightarrow G, \quad (x, y) \mapsto xy$$

is a group homomorphism.

REMARK 2.2 ([LYZ1], Theorem 1). (a) In order for the pair (G, σ) to be a braided group, conditions (1.1), (1.3) (for $S = B = G$) and (2.2) are sufficient, i.e., the rest conditions (1.2) and (1.4) follow from them.

(b) If (G, σ) is a braided group, then σ is a braid operator on $G \times G$. Thus (G, σ) forms a non-degenerate braided set in the sense of [ESS].

If the braided set (G, σ) is symmetric, we call (G, σ) a *symmetric group*. This condition is expressed diagrammatically:

$$(2.3) \quad \begin{array}{c} x & & y \\ & \diagdown & / \\ & x' & \\ & / & \diagdown \\ y' & & x' \end{array} \Rightarrow \begin{array}{c} y' & & x' \\ & \diagdown & / \\ & x & \\ & / & \diagdown \\ x & & y \end{array} \quad \text{or} \quad \begin{array}{c} x & & y \\ & \diagdown & / \\ & y' & \\ & / & \diagdown \\ y' & & x' \end{array}$$

for x, y, x', y' in G .

EXAMPLE 2.3 (of trivial braided groups). (a) G is arbitrary and σ is defined by

$$\begin{array}{c} x & & y \\ & \diagdown & / \\ & xyx^{-1} & \\ & / & \diagdown \\ & x & \end{array}, \quad x, y \in G.$$

(b) G is abelian and σ is defined by

$$\begin{array}{ccc} x & & y \\ & \diagdown & / \\ & & \\ & / & \diagdown \\ y & & x \end{array}, \quad x, y \in G.$$

PROPOSITION 2.4. *A braided group G is symmetric if and only if*

$$(2.4) \quad (x \leftarrow y)^{-1} = y^{-1} \rightarrow x^{-1} \text{ for all } x, y \text{ in } G.$$

Proof. By (1.8) and (2.3), G is symmetric if and only if

$$(2.5) \quad \begin{array}{ccc} x & & y \\ & \diagdown & / \\ & & \\ & / & \diagdown \\ y' & & x' \end{array} \Rightarrow \begin{array}{ccc} y^{-1} & & x^{-1} \\ & \diagdown & / \\ & & \\ & / & \diagdown \\ (x')^{-1} & & (y')^{-1} \end{array} \text{ for } x, y, x', y' \in G.$$

Under the assumption of (2.5), we have $x' = x \leftarrow y$ and y' is determined by data x, y, x' as $y'x' = xy$. This implies immediately the equivalence of (2.4) and (2.5). ■

DEFINITION 2.5 ([ESS], Def. 2.2). A *1-cocycle datum* means a triple (G, N, π) where G and N are groups such that G acts on N on the right as group automorphisms

$$N \times G \rightarrow N, \quad (a, x) \mapsto a \triangleleft x$$

and $\pi : G \rightarrow N$ is a bijective 1-cocycle, i.e.,

$$(2.6) \quad \pi(xy) = (\pi(x) \triangleleft y)\pi(y), \quad x, y \in G.$$

Braided groups and 1-cocycle data correspond categorically ([LYZ1], Theorem 2). If G is a braided group, we put

$$(2.7) \quad N = \text{Ker}(\text{mult} : G \bowtie G \rightarrow G)$$

We let G act on N by:

$$(2.8) \quad a \triangleleft x = (x^{-1}, 1)a(x, 1), \quad a \in N, \quad x \in G.$$

We define the 1-cocycle $\pi : G \rightarrow N$ by:

$$(2.9) \quad \pi(x) = (x^{-1}, x), \quad x \in G.$$

Then (G, N, π) is a 1-cocycle datum. We have

$$(2.10) \quad \pi(x \leftarrow y) = \pi(x) \triangleleft y, \quad x, y \in G,$$

as is easily checked.

Conversely, let (G, N, π) be a 1-cocycle datum. Then the following map is bijective:

$$(2.11) \quad G \times G \rightarrow G \times N, \quad (x, y) \mapsto (xy, \pi(y)).$$

Transport the group structure of $G \times N$ to $G \times G$ along this bijection. Then a matched pair structure on (G, G) is defined. Since we have a commutative diagram

$$(2.12) \quad \begin{array}{ccc} G \bowtie G & \xrightarrow{\sim} & G \times N \\ \swarrow \text{mult} & & \searrow \text{projection} \\ & G & \end{array}$$

the multiplication is a group homomorphism. Hence G becomes a braided group.

PROPOSITION 2.6 ([LYZ1], Prop. 4). *Under the above correspondence, the braided group G is symmetric if and only if N is abelian.*

Proof. Assume we have

$$\begin{array}{ccc}
 x & & y \\
 & \diagdown & / \\
 & x & y \\
 & / & \diagdown \\
 y' & & x'
 \end{array}
 , \quad x, y, x', y' \in G.$$

Since $xy = y'x'$, we have

$$(2.13) \quad \pi(xy) = \pi(y'x') = \pi(x \leftarrow y)\pi(y) = \pi(y' \leftarrow x')\pi(x').$$

Here, note that $x' = x \leftarrow y$. Hence, if N is abelian, we have $y = y' \leftarrow x'$. This implies we have

$$\begin{array}{ccc}
 y' & & x' \\
 & \diagdown & / \\
 & x & y \\
 & / & \diagdown \\
 x & & y
 \end{array}$$

hence G is symmetric by (2.3). Conversely, if G is symmetric, we have $y = y' \leftarrow x'$. Hence (2.13) implies

$$\pi(x')\pi(y) = \pi(y)\pi(x').$$

Since we can choose x', y arbitrarily, this implies N is abelian. ■

COROLLARY 2.7. *If G is symmetric, we have*

$$(x^{-1}, 1)a(x, 1) = (1, x^{-1})a(1, x), \quad x \in G, \quad a \in N.$$

The correspondence between symmetric groups and abelian 1-cocycle data is implicit in [ESS] and fully studied there.

Let G be a braided group. Let Γ_r (resp. Γ_l) be the kernel of the right action \leftarrow (resp. left action \rightarrow), i.e.,

$$(2.14) \quad \Gamma_r = \left\{ g \in G \mid \begin{array}{ccc} x & & g \\ & \diagdown & / \\ & xgx^{-1} & x \end{array} \quad \text{for all } x \in G \right\},$$

$$\Gamma_l = \left\{ g \in G \mid \begin{array}{ccc} g & & x \\ & \diagdown & / \\ x & & x^{-1}gx \end{array} \quad \text{for all } x \in G \right\}.$$

Put $\Gamma = \Gamma_r \cap \Gamma_l$. If G is symmetric, $\Gamma_r = \Gamma_l$ by Proposition 2.4.

LEMMA 2.8. $\Gamma_r \times \{1\}, \{1\} \times \Gamma_l \triangleleft G \bowtie G$.

Proof. (2.14) implies

$$(1, x)(g, 1) = (xgx^{-1}, x), \quad x \in G, \quad g \in \Gamma_r.$$

Hence

$$(1, x)(g, 1)(1, x^{-1}) = (xgx^{-1}, 1).$$

This implies $\Gamma_r \times \{1\} \triangleleft G \bowtie G$. Similarly, $\{1\} \times \Gamma_l \triangleleft G \bowtie G$. ■

PROPOSITION 2.9. (a) Γ is an abelian normal subgroup of G

(b) The matched pair structure $\sigma : G \times G \rightarrow G \times G$ induces a map $G/\Gamma \times G/\Gamma \rightarrow G/\Gamma \times G/\Gamma$ which makes G/Γ into a braided group, i.e., G/Γ is a quotient braided group of G .

Proof. (a) (2.14) implies we have

$$\begin{array}{ccc}
 x & & y \\
 & \searrow & / \\
 & x & \\
 & / & \searrow \\
 y & & x
 \end{array}
 \quad x, y \in \Gamma,$$

hence Γ is abelian.

(b) Similarly to Lemma 2.8, we have $\Gamma \times \{1\}, \{1\} \times \Gamma \triangleleft G \bowtie G$, hence $\Gamma \times \Gamma \triangleleft G \bowtie G$. The quotient $(G \bowtie G)/(\Gamma \times \Gamma)$ factors as a product of subgroups $G/\Gamma \times \{1\}, \{1\} \times G/\Gamma$ yielding a matched pair structure on $(G/\Gamma, G/\Gamma)$. This structure is obviously induced by σ . ■

Soloviev’s Theorem 2.6 [So], which is stated in terms of cocycle data, is equivalent to the above proposition.

COROLLARY 2.10. The braided group $\bar{G} = G/\Gamma$ corresponds to the 1-cocycle datum $(\bar{G}, \bar{N}, \bar{\pi})$ where $\bar{N} = N/N_\Gamma$ with

$$(2.15) \quad N_\Gamma = \{(g^{-1}, g) \mid g \in \Gamma\}$$

and $\bar{\pi}$ is induced by π . N_Γ is central in N .

Proof. If $g \in \Gamma, x \in G$, then

$$(x, 1)(g, 1)(x^{-1}, 1) = (1, x)(g, 1)(1, x^{-1})$$

by the proof of Lemma 2.8. Hence $(g, 1)$ commutes with (x^{-1}, x) . Similarly $(1, g)$ commutes with (x^{-1}, x) . Hence N_Γ is central in N . The rest is obvious. ■

3. The braided group G_X . Let (X, σ) be a non-degenerate braided set. We write

$$(3.1) \quad \sigma : X \times X \rightarrow X \times X, \quad (x, y) \mapsto (x \rightarrow y, x \leftarrow y).$$

This is bijective satisfying the braid relation, and the actions $x \rightarrow$ and $\leftarrow y$ are bijections of X onto itself. We use the symbol as in §1:

$$(3.2) \quad
 \begin{array}{ccc}
 x & & y \\
 & \searrow & / \\
 & x & \\
 & / & \searrow \\
 y' & & x'
 \end{array}
 \quad \text{or} \quad
 \begin{array}{ccc}
 y' & & x' \\
 & \searrow & / \\
 & x & \\
 & / & \searrow \\
 x & & y
 \end{array}$$

to mean the relation $(y', x') = \sigma(x, y)$.

DEFINITION 3.1 ([ESS], 2.1). Let G_X be the group defined by generators X and relations

$$(3.3) \quad y'x' = xy \text{ if } (y', x') = \sigma(x, y), \quad x, y \in X.$$

THEOREM 3.2 ([LYZ1], Theorem 9). G_X has a unique structure of a braided group such that the canonical map $X \rightarrow G_X$ preserves the braiding.

The matched actions $g \rightarrow h, g \leftarrow h, g, h \in G_X$ are constructed as follows (see [LYZ1] for details):

Step 1. The braid relation for σ implies

$$(3.4) \quad \begin{array}{ccc} x & & y \\ & \searrow & / \\ & x' & \\ & / & \searrow \\ y' & & \end{array} \Rightarrow \begin{cases} x \rightarrow (y \rightarrow z) = y' \rightarrow (x' \rightarrow z), \\ (u \leftarrow x) \leftarrow y = (u \leftarrow y') \leftarrow x' \end{cases}$$

where $x, y, x', y', z, u \in X$. Hence the actions \rightarrow and \leftarrow extend to group actions

$$(3.5) \quad \begin{aligned} G_X \times X &\rightarrow X, & (g, x) &\mapsto g \rightarrow x, \\ X \times G_X &\rightarrow X, & (x, g) &\mapsto x \leftarrow g. \end{aligned}$$

Step 2. By means of actions (3.5), we put

$$(3.6) \quad x \rightarrow g = xg(x \leftarrow g)^{-1}, \quad g \leftarrow x = (g \rightarrow x)^{-1}gx, \quad x \in X, g \in G_X.$$

One can prove that (i) the actions $x \rightarrow$ and $\leftarrow x$ are bijections of G_X onto itself, (ii) condition (3.4) is valid for these actions with $z, u \in G_X$. Hence these actions extend to left and right group actions of G_X on G_X . One can prove that the extended actions satisfy the compatibility condition

$$(3.7) \quad gh = (g \rightarrow h)(g \leftarrow h), \quad g, h \in G_X.$$

Thus G_X becomes a braided group by Remark 2.2.

Let (G_X, N_X, π_X) be the 1-cocycle datum corresponding to the braided group G_X , Soloviev [So], Theorem 2.5 has obtained a presentation of the group N_X by generators and relations. We review his presentation below.

If (G, N, π) is a 1-cocycle datum, it follows from (2.6) and (2.10) that we have

$$(3.8) \quad \begin{array}{ccc} x & & y \\ & \searrow & / \\ & x' & \\ & / & \searrow \\ y' & & \end{array} \Rightarrow \pi(xy) = \pi(x')\pi(y), \quad x, y, x', y' \in G.$$

This implies:

$$(3.9) \quad \begin{array}{ccc} x & & y \\ & \searrow & / \\ & x' & \\ & / & \searrow \\ y' & & \\ & / & \searrow \\ & x'' & \\ & / & \searrow \\ & y'' & \end{array} \text{ in } G \Rightarrow \pi(x')\pi(y) = \pi(y'')\pi(x').$$

Let A_X be the group defined by generators X and the following relation:

$$(3.10) \quad x' \cdot y = y'' \cdot x' \quad \text{if} \quad \begin{array}{ccc} x & & y \\ & \searrow & / \\ & y' & \\ & / & \searrow \\ & x'' & \\ & / & \searrow \\ & y'' & \end{array} \text{ in } X.$$

THEOREM 3.3 ([So], Theorem 2.5). *The map $\pi_X : X \rightarrow N_X$ induces a group isomorphism $A_X \xrightarrow{\cong} N_X$.*

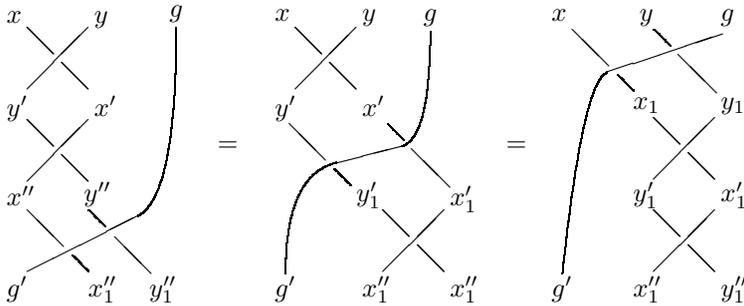
Comparison of (3.9) and (3.10) shows immediately that π_X induces a group homomorphism $\tilde{\pi}_X : A_X \rightarrow N_X$. We show that $\tilde{\pi}_X$ is an isomorphism.

LEMMA 3.4. *The right action $X \leftarrow G_X$ (3.5) extends to a right action $A_X \leftarrow G_X$ as group automorphisms.*

Proof. It is enough to show that

$$(x' \leftarrow g) \cdot (y \leftarrow g) = (y'' \leftarrow g) \cdot (x' \leftarrow g), \quad g \in G_X$$

with the assumption of (3.10). In fact, the braid relation implies that we have



This diagram means that

$$x'_1 \cdot y_1 = y''_1 \cdot x'_1 \quad \text{and} \quad x'_1 = x' \leftarrow g, \quad y_1 = y \leftarrow g, \quad y''_1 = y'' \leftarrow g.$$

Hence we are done. ■

Now, Theorem 3.3 is proved in several steps.

Step 1. We can form the semidirect product $G_X \rtimes A_X$. The map

$$(3.11) \quad X \rightarrow G_X \rtimes A_X, \quad x \mapsto (x, x)$$

extends to a group homomorphism

$$(3.12) \quad f : G_X \rightarrow G_X \rtimes A_X.$$

In fact, with the assumption of (3.10), we have in $G_X \rtimes A_X$

$$\begin{aligned} (x, x)(y, y) &= (xy, (x \leftarrow y) \cdot y) = (xy, x' \cdot y), \\ (y', y')(x', x') &= (y'x', (y' \leftarrow x') \cdot x') = (y'x', y'' \cdot x'). \end{aligned}$$

Hence they coincide.

Further, the map

$$(3.13) \quad \tilde{f} : G_X \rtimes G_X \rightarrow G_X \rtimes A_X, \quad (g, h) \mapsto (g, 1)f(h)$$

is a group homomorphism.

In fact, it is enough to show that

$$\begin{array}{ccc}
 g & & h \\
 & \searrow & / \\
 & & \times \\
 & / & \searrow \\
 h' & & g'
 \end{array}
 \quad \text{in } G_X \Rightarrow f(g)(h, 1) = (h', 1)f(g').$$

It is easy to see we can assume g, h, g', h' are in X . If this is the case, the claim follows directly from the definition of f .

Step 2. We have a commutative diagram

$$\begin{array}{ccc}
 G_X \rtimes G_X & \xrightarrow{\tilde{f}} & G_X \rtimes A_X \\
 \text{mult.} \searrow & & \swarrow \text{projection} \\
 & G_X &
 \end{array}$$

Hence \tilde{f} induces a homomorphism $\tilde{f} : N_X \rightarrow A_X$. On the other hand, we have a homomorphism $\tilde{\pi}_X : A_X \rightarrow N_X$. Since $\tilde{f}(x^{-1}, x) = (x^{-1}, 1)(x, x) = (1, x)$, $x \in X$, we have $\tilde{f} \circ \tilde{\pi}_X = \text{id}$. On the other hand, $\tilde{\pi}_X$ is surjective by the next lemma. Hence we have proved Theorem 3.3.

LEMMA 3.5. *Let G be a braided group with generators X such that $X \leftarrow G \subset X$. Then the corresponding group N is generated by (x^{-1}, x) , $x \in X$.*

Proof. Let M be the subgroup of N ($\subset G \rtimes G$) generated by (x^{-1}, x) , $x \in X$. The assumption implies that M is normalized by $G \times \{1\}$ and $G \rtimes M$ contains $\{1\} \times G$. Hence

$$G \rtimes M = G \rtimes G = G \rtimes N$$

yielding $M = N$. ■

COROLLARY 3.6 ([ESS], Proposition 2.5). *If (X, σ) is a symmetric set, then N_X is a free abelian group with basis (x^{-1}, x) , $x \in X$. In particular, the canonical map $X \rightarrow G_X$ is injective.*

One can refine the construction G/Γ in §2 in case of G_X . Let Γ_r (resp. Γ_l) be the kernel of the right action \leftarrow (resp. left action \rightarrow) of G_X on X (3.5). These are smaller than the Γ_r and Γ_l defined in §2. If (X, σ) is symmetric, they coincide since $X \subset G_X$. Put $\Gamma = \Gamma_l \cap \Gamma_r$. Similarly as Proposition 2.9, we have

- PROPOSITION 3.7. (a) Γ is an abelian normal subgroup of G_X .
 (b) G_X/Γ is a quotient braided group of G_X .

COROLLARY 3.8 ([So], Theorem 2.6). *If (X, σ) is a finite non-degenerate braided set, then G_X/Γ is a finite braided group.*

4. LYZ pairs. Let (S, B) be a matched pair of groups. If S is a finite group, we have the bi-smash product Hopf algebra $H(S, B)$ (§1). When $k = \mathbb{C}$, Lu-Yan-Zhu [LYZ2] describe all positive quasitriangular structures on $H(S, B)$ by means of homomorphisms

$$(4.1) \quad \xi, \eta : S \rightarrow B$$

satisfying some curious conditions. We would like to call such pairs LYZ pairs and study more in §§4–5.

DEFINITION 4.1. A pair of group homomorphisms (ξ, η) (4.1) is called an *LYZ pair* if the following conditions are satisfied:

$$(4.2) \quad \begin{array}{ccc} s & & b \\ & \searrow & / \\ & & s' \\ & / & \searrow \\ b' & & \end{array} \Rightarrow \begin{cases} \xi(s)b = b'\xi(s') \\ \eta(s)b = b'\eta(s') \end{cases}, \quad s, s' \in S, b, b' \in B,$$

(4.3) Let $s, t \in S$. Define $s', t' \in S$ by the diagrams

$$\begin{array}{ccc} \xi(s) & & t \\ & \searrow & / \\ & & t' \\ & / & \searrow \end{array}, \quad \begin{array}{ccc} s & & \eta(t) \\ & \searrow & / \\ & & s' \\ & / & \searrow \end{array}.$$

Then $t's' = st$.

Condition (4.2) implies ξ, η extend to group homomorphisms

$$(4.4) \quad \bar{\xi}, \bar{\eta} : B \bowtie S \rightarrow B$$

which are identity on B .

(4.2) and (4.3) imply

$$(4.5) \quad \begin{array}{ccc} \xi(s) & & t \\ & \searrow & / \\ & & \xi(s') \\ & / & \searrow \\ t' & & \end{array}, \quad \begin{array}{ccc} s & & \eta(t) \\ & \searrow & / \\ & & \eta(t') \\ & / & \searrow \\ s' & & \end{array}$$

with notations in (4.3) ([LYZ2], Lemma 2.4).

We put

$$(4.6) \quad \begin{aligned} N_\xi &= \text{Ker}(\bar{\xi}), \quad N_\eta = \text{Ker}(\bar{\eta}), \\ \pi_\xi(s) &= (\xi(s)^{-1}, s), \quad \pi_\eta(s) = (\eta(s)^{-1}, s), \quad s \in S. \end{aligned}$$

LEMMA 4.2. Under condition (4.2), we have

$$(4.3) \Leftrightarrow \pi_\xi(s)\pi_\eta(t^{-1}) = \pi_\eta(t^{-1})\pi_\xi(s).$$

Proof. With notations in (4.3), we have

$$\begin{array}{ccc} t^{-1} & & \xi(s)^{-1} \\ & \searrow & / \\ & & (t')^{-1} \\ & / & \searrow \end{array}, \quad \begin{array}{ccc} s & & \eta(t) \\ & \searrow & / \\ & & s' \\ & / & \searrow \end{array}.$$

Hence

$$\begin{aligned} \pi_\xi(s)\pi_\eta(t^{-1}) &= (\xi(s)^{-1}, s)(\eta(t), t^{-1}) = (, s't^{-1}), \\ \pi_\eta(t^{-1})\pi_\xi(s) &= (\eta(t), t^{-1})(\xi(s)^{-1}, s) = (, (t')^{-1}s). \end{aligned}$$

If these are equal, then $s't^{-1} = (t')^{-1}s$ or $t's' = st$ yielding (4.3). Conversely, if (4.3) is true, we have

$$\begin{array}{ccc} t^{-1} & \xi(s)^{-1} & \\ & \diagdown \quad \diagup & \\ & \xi(s')^{-1}(t')^{-1} & \end{array}, \quad \begin{array}{ccc} s & & \eta(t) \\ & \diagdown \quad \diagup & \\ & \eta(t') & s' \end{array}$$

by (4.5). Hence

$$\begin{aligned} \pi_\xi(s)\pi_\eta(t^{-1}) &= (\xi(s)^{-1}\eta(t'), s't^{-1}), \\ \pi_\eta(t^{-1})\pi_\xi(s) &= (\eta(t)\xi(s')^{-1}, (t')^{-1}s) \end{aligned}$$

which coincide since $\xi(s)\eta(t) = \eta(t')\xi(s')$ by (4.2). ■

Since $N_\xi = \{\pi_\xi(s) \mid s \in S\}$, we have

PROPOSITION 4.3. *A pair of group homomorphisms (ξ, η) (4.1) is an LYZ pair if and only if*

- (a) *they extend to homomorphisms $(\bar{\xi}, \bar{\eta})$ in (4.4),*
- (b) *every element in N_ξ commutes with every element in N_η .*

EXAMPLE 4.4. If G is a symmetric group, (id, id) is an LYZ pair for the matched pair (G, G) . This follows from Propositions 2.6 and 4.3.

Define a map

$$S \times S \rightarrow S \times S, \quad (s, t) \mapsto (t', s')$$

by condition (4.3). We illustrate this map as usual by diagram

$$(4.7) \quad \begin{array}{ccc} s & & t \\ & \diagdown \quad \diagup & \\ & t' & s' \end{array} .$$

THEOREM 4.5. *The above map makes S into a braided group.*

Proof. Since condition (2.2) is satisfied by (4.3), we check that (S, S) becomes a matched pair of groups by the above map. By Proposition 1.2, we have only to check conditions (1.9) and (1.10) for (S, S) . But they follow from the corresponding conditions for (S, B) through homomorphisms ξ and η , since (4.7) is equivalent to (4.5). ■

The equivalence of (4.5) and (4.7) means that

$$(\text{id}, \eta) : (S, S) \rightarrow (S, B), \quad (\xi, \text{id}) : (S, S) \rightarrow (B, S)$$

are homomorphisms of matched pairs of groups. This and an easy observation yield the following:

PROPOSITION 4.6. *Let (ξ, η) be an LYZ pair for (S, B) .*

(a) *We have the following group homomorphisms:*

$$(4.8) \quad \begin{aligned} \eta \bowtie \text{id} : S \bowtie S &\rightarrow B \bowtie S, & (s, t) &\mapsto (\eta(s), t), \\ \text{id} \bowtie \xi : S \bowtie S &\rightarrow B \bowtie S, & (s, t) &\mapsto (1, s)(\xi(t), 1). \end{aligned}$$

(b) We have commutative diagrams

$$(4.9) \quad \begin{array}{ccccc} B \rtimes S & \xleftarrow{\xi \rtimes \text{id}} & S \rtimes S & \xrightarrow{\text{id} \rtimes \xi} & B \rtimes S \\ \downarrow \bar{\eta} & & \downarrow \text{mult} & & \downarrow \bar{\xi} \\ B & \xleftarrow{\eta} & S & \xrightarrow{\xi} & B \end{array}$$

$$(4.10) \quad \begin{array}{ccc} & S \rtimes S & \\ \eta \rtimes \text{id} \swarrow & & \searrow \text{id} \rtimes \xi \\ B \rtimes S & & B \rtimes S \\ \bar{\xi} \searrow & B & \swarrow \bar{\eta} \end{array}$$

Note that the common homomorphism $S \rtimes S \rightarrow B$ in (4.10) maps (s, t) to $\eta(s)\xi(t)$.

COROLLARY 4.7. $\eta \rtimes \text{id}$ and $\text{id} \rtimes \xi$ induce the following isomorphisms:

$$(4.11) \quad \begin{array}{ccccc} N_\eta & \xleftarrow[\sim]{\eta \rtimes \text{id}} & N & \xrightarrow[\sim]{\text{id} \rtimes \xi} & N_\xi \\ (\eta(s)^{-1}, s) & \longleftarrow & (s^{-1}, s) & \longrightarrow & (1, s^{-1})(\xi(s), 1) \end{array}$$

PROPOSITION 4.8. Let (ξ, η) be an LYZ pair for (S, B) . There is a unique automorphism F of the group $B \rtimes S$ such that

$$(4.12) \quad F(\eta(s)^{-1}, s) = (1, s^{-1})(\xi(s), 1), \quad s \in S,$$

$$(4.13) \quad F(b, 1) = (b, 1), \quad b \in B.$$

Proof. By Corollary 4.7, there is a unique isomorphism $F : N_\eta \xrightarrow{\sim} N_\xi$ defined by (4.12). Since we have

$$B \rtimes S = B \rtimes N_\eta = B \rtimes N_\xi,$$

it is enough to show that F preserves the conjugate action by B . Assume that

$$\begin{array}{ccc} s & & b \\ & \searrow & \swarrow \\ & b' & s' \end{array}, \quad s, s' \in S, \quad b, b' \in B.$$

Then we have

$$(b^{-1}, 1)(\eta(s)^{-1}, s)(b, 1) = (b^{-1}\eta(s)^{-1}b', s') = (\eta(s')^{-1}, s').$$

Noting that

$$\xi(s)b = b'\xi(s') \quad \text{and} \quad \begin{array}{ccc} s^{-1} & & b' \\ & \searrow & \swarrow \\ b & & (s')^{-1} \end{array}$$

we see

$$\begin{aligned} (b^{-1}, 1)(1, s^{-1})(\xi(s), 1)(b, 1) &= (b^{-1}, s^{-1})(\xi(s)b, 1) \\ &= (b^{-1}, s^{-1})(b'\xi(s'), 1) = (1, (s')^{-1})(\xi(s'), 1). \end{aligned}$$

Hence F preserves the conjugate action by B . ■

This automorphism F was introduced in [LYZ2], Theorem 3.1.

PROPOSITION 4.9. *The automorphism F of $B \bowtie S$ has the following properties:*

$$(4.14) \quad F(1, s) = (\eta(s), 1)(1, s^{-1})(\xi(s), 1) = (\xi(s), 1)(1, s^{-1})(\eta(s), 1), \quad s \in S,$$

$$(4.15) \quad \bar{\eta} \circ F = \bar{\xi}, \quad \bar{\xi} \circ F = \bar{\eta},$$

$$(4.16) \quad F(N_\xi) = N_\eta, \quad F(N_\eta) = N_\xi,$$

$$(4.17) \quad F^2 = \text{id}.$$

Proof. The first half of (4.14) follows from (4.12) and (4.13). The latter half follows since $(\eta(s), s^{-1})$ commutes with $(\xi(s), s^{-1})$ by Proposition 4.3. Note that (4.14) means F stays invariant relative to interchange $\xi \leftrightarrow \eta$. (4.15) follows from (4.13) and (4.14), and this yields (4.16). We have

$$\begin{aligned} F^2(1, s) &= (\eta(s), 1)F(1, s^{-1})(\xi(s), 1) \\ &= (\eta(s), 1)(\eta(s^{-1}), 1)(1, s)(\xi(s^{-1}), 1)(\xi(s), 1) = (1, s) \end{aligned}$$

yielding (4.17). ■

5. The universal LYZ pair and minimal LYZ pairs. Let S be a braided group.

For $s, s' \in S$ and $(t, u), (t', u') \in S \bowtie S$, we write

$$(5.1) \quad \begin{array}{c} s & & (t, u) \\ & \diagdown & / \\ & & \\ & / & \diagdown \\ (t', u') & & s' \end{array} = \begin{array}{c} s & & t & & u \\ & \diagdown & / & & \\ & & & \diagdown & / \\ t' & & u' & & s' \end{array} .$$

This means a relation among relevant elements (or a subset of $(S \times S \bowtie S) \times (S \bowtie S \times S)$). If one has a pair $(s, (t, u))$, there is a unique pair $((t', u'), s')$ satisfying condition (5.1). Hence the correspondence $(s, (t, u)) \mapsto ((t', u'), s')$ may be viewed as a map $S \times S \bowtie S \rightarrow S \bowtie S \times S$.

PROPOSITION 5.1. (a) *The above map makes $(S, S \bowtie S)$ into a matched pair of groups.*

(b) *The injections $\text{in}_2, \text{in}_1 : S \rightarrow S \bowtie S, s \mapsto (1, s), (s, 1)$ form an LYZ pair for $(S, S \bowtie S)$.*

(c) *The braided structure on S induced by the LYZ pair $(\text{in}_2, \text{in}_1)$ coincides with the original one.*

Proof. (a) We check conditions (1.9) and (1.10). (1.9) becomes

$$(5.2) \quad \begin{array}{c} r & & s & & t & & u \\ & \diagdown & / & & & \diagdown & / \\ & & & & & & \\ & / & \diagdown & / & \diagdown & / & \\ t' & & u' & & r' & & s' \end{array} \Rightarrow \begin{array}{c} rs & & t & & u \\ & \diagdown & / & & \\ & & & \diagdown & / \\ t' & & u' & & r's' \end{array}$$

which holds obviously. As for (1.10), we have to choose b, c from $S \bowtie S$. Then we can assume b, c belong to $S \times \{1\}$ or $\{1\} \times S$. If b is in $S \times \{1\}$ (resp. $\{1\} \times S$), we can assume b' is also in $S \times \{1\}$ (resp. $\{1\} \times S$). Thus there are 4 possibilities of the choice of b, c (and b', c'). Here we use the notations of (1.10). Among them, the only nontrivial choice

is the case $b = (1, t)$ and $c = (u, 1)$, hence $b' = (1, t')$ and $c' = (u', 1)$. In this case, (1.10) becomes

$$(5.3) \quad \begin{array}{ccc} s & & t & & u \\ & \diagdown & / & & \\ t' & & u' & & s' \end{array} \Rightarrow \begin{array}{ccc} s & & u_1 & & t_1 \\ & \diagdown & / & & \\ u'_1 & & t'_1 & & s'_1 \end{array}$$

if $(1, t)(u, 1) = (u_1, t_1)$ and $(1, t')(u', 1) = (u'_1, t'_1)$. Now we have

$$\begin{array}{ccc} t & & u \\ & \diagdown & / \\ u_1 & & t_1 \end{array} \quad \text{and} \quad \begin{array}{ccc} t' & & u' \\ & \diagdown & / \\ u'_1 & & t'_1 \end{array} .$$

Hence the assertion follows from the braid relation

$$(5.4) \quad \begin{array}{ccc} s & & t & & u \\ & \diagdown & / & & \\ u'_1 & & t'_1 & & s' \end{array} = \begin{array}{ccc} s & & t & & u \\ & \diagdown & / & & \\ u'_1 & & t'_1 & & s' \end{array} .$$

(b), (c). First we check condition (4.2). This means (5.1) implies

$$(5.5) \quad (1, s)(t, u) = (t', u')(1, s'), \quad (s, 1)(t, u) = (t', u')(s', 1).$$

In fact, (5.1) implies there is $s^\circ \in S$ such that

$$\begin{array}{ccc} s & & t \\ & \diagdown & / \\ t' & & s^\circ \end{array} \quad \text{and} \quad \begin{array}{ccc} s^\circ & & u \\ & \diagdown & / \\ u' & & s' \end{array} .$$

Then we have

$$(1, s)(t, u) = (t', s^\circ u) = (t', u's'),$$

$$(st, u) = (t's^\circ, u) = (t', u')(s', 1).$$

To prove (b), (c), it is enough to show

$$(5.6) \quad \begin{array}{ccc} v & & w \\ & \diagdown & / \\ w' & & v' \end{array} \Rightarrow \begin{array}{ccc} (1, v) & & w \\ & \diagdown & / \\ w' & & (1, v') \end{array} \quad \text{and} \quad \begin{array}{ccc} v & & (w, 1) \\ & \diagdown & / \\ (w', 1) & & v' \end{array}$$

where $v, w, v', w' \in S$. This follows directly from definition (5.1). ■

The above LYZ pair has the following universality.

PROPOSITION 5.2. *Let (ξ, η) be an LYZ pair for a matched pair of groups (S, B) .*

- (a) *The map $\eta * \xi : S \bowtie S \rightarrow B, (s, t) \mapsto \eta(s)\xi(t)$ is a group homomorphism.*
- (b) *$(\text{id}, \eta * \xi) : (S, S \bowtie S) \rightarrow (S, B)$ is a homomorphism of matched pairs of groups.*
- (c) *The above homomorphism transforms the LYZ pair $(\text{in}_2, \text{in}_1)$ to (ξ, η) .*

Proof. (a) See (4.10).

(b) Since (4.7) implies (4.5), it follows that we have

$$(5.7) \quad \begin{array}{c} s & & t & & u \\ & \diagdown & / & \diagdown & / \\ t' & & u' & & s' \end{array} \Rightarrow \begin{array}{c} s & & \eta(t) & & \xi(u) \\ & \diagdown & / & \diagdown & / \\ \eta(t') & & \xi(u') & & s' \end{array} \Rightarrow \begin{array}{c} s & & \eta(t)\xi(u) \\ & \diagdown & / \\ \eta(t')\xi(u') & & s' \end{array} .$$

(c) is obvious. ■

EXAMPLE 5.3. Let (X, σ) be a finite non-degenerate braided set. We have a finite braided group $S = G_X/\Gamma$ by Corollary 3.8. Hence we have a quasitriangular Hopf algebra $H(S, S \bowtie S)$.

We turn to minimal LYZ pairs. A quasitriangular Hopf algebra (H, R) is called *minimal* if H is the only Hopf subalgebra containing R .

PROPOSITION 5.4. *Let (ξ, η) be an LYZ pair for a matched pair of finite groups (S, B) . If ξ and η are isomorphisms $S \xrightarrow{\sim} B$, then $H(S, B)$ is a minimal quasitriangular Hopf algebra.*

This follows immediately from the description of the quasitriangular structure R in [LYZ2], Theorem 2.3 (see (6.4)).

EXAMPLE 5.5. Let G be a finite symmetric group. Then (id, id) is an LYZ pair for (G, G) by Example 4.4. Hence it gives a minimal quasitriangular structure on $H(G, G)$. Since we have

$$G \bowtie G = G \rtimes A \quad \text{with} \quad A = \text{Ker}(\text{mult}),$$

the Hopf algebra $H(G, G)$ is quasi-isomorphic to $H(A, G) = (kA)^* \# kG$ [LYZ2, Prop. 4.1], [EG, Thm. 4.2]. If k is an algebraically closed field of characteristic 0, then $(kA)^* \simeq kA^*$, so that $(kA)^* \# kG$ is isomorphic to the group Hopf algebra $k(A^* \rtimes G)$. Thus $H(G, G)$ is a twist of the group Hopf algebra $k(A^* \rtimes G)$. Minimal quasitriangular Hopf algebras of this form are studied in [EG].

We may call the LYZ pair (ξ, η) *minimal* if ξ and η are group isomorphisms $S \xrightarrow{\sim} B$. In this case, we can assume $S = B$ and $\eta = \text{id}$ by the following:

PROPOSITION 5.6. (a) *Let S be a braided group and ξ a group automorphism of S . Then (ξ, id) is an LYZ pair for (S, S) if and only if we have*

$$(5.8) \quad \begin{array}{c} s & & t \\ & \diagdown & / \\ t' & & s' \end{array} \Rightarrow \begin{array}{c} \xi(s) & & t \\ & \diagdown & / \\ t' & & \xi(s') \end{array} , \quad s, t, s', t' \in S.$$

(b) *Let (ξ, η) be a minimal LYZ pair for the matched pair of groups (S, B) . Then $(\xi\eta^{-1}, \text{id})$ is a minimal LYZ pair for the pair (S, S) .*

Proof. (a) (5.8) is part of (4.5). Condition (4.2) is automatically satisfied.

(b) This is obvious, since we have an isomorphism of matched pairs $(\text{id}, \eta) : (S, S) \xrightarrow{\sim} (S, B)$. ■

DEFINITION 5.7. A pair of a braided group S and its group automorphism ξ is called a ξ -braided group if condition (5.8) is satisfied.

If (S, ξ) is a finite ξ -braided group, we have a minimal quasitriangular Hopf algebra $H(S, S)$ with structure induced by the LYZ pair (ξ, id) .

PROPOSITION 5.8. *Let (S, ξ) be a ξ -braided group.*

- (a) ξ is an automorphism of the braided group S .
- (b) We have $\Gamma_l = \Gamma_r = \Gamma$ and $\Gamma = \xi(\Gamma)$ with the notations in (2.14) (for $G = S$).
- (c) Every element in Γ commutes with $\xi(s)s^{-1}$, $s^{-1}\xi(s)$, $s \in S$.
- (d) S/Γ is a ξ -braided group.

Proof. (a) (5.8) yields

$$\begin{array}{ccc}
 \begin{array}{c} s \quad t \\ \diagdown \quad / \\ t' \quad s' \end{array} & \Rightarrow & \begin{array}{c} t' \quad \xi(s') \\ \diagdown \quad / \\ \xi(s) \quad t \end{array} & \Rightarrow & \begin{array}{c} \xi(s) \quad \xi(t) \\ \diagdown \quad / \\ \xi(t') \quad \xi(s') \end{array}
 \end{array}$$

hence ξ preserves the braiding.

(b) If $g \in \Gamma_r$ and $x \in S$, we have

$$\begin{array}{c}
 x \quad x^{-1}gx \\
 \diagdown \quad / \\
 g \quad x
 \end{array}$$

since $x^{-1}gx \in \Gamma_r$. By (5.8), this yields

$$(5.9) \quad \begin{array}{c} g \quad \xi(x) \\ \diagdown \quad / \\ \xi(x) \quad x^{-1}gx \end{array} .$$

Since ξ is bijective, this means $g \in \Gamma_l$. Hence $\Gamma_r \subset \Gamma_l$. If $g \in \Gamma_l$ and $x \in S$, we have similarly

$$(5.10) \quad \begin{array}{c} x \quad \xi(g) \\ \diagdown \quad / \\ \xi(xgx^{-1}) \quad x \end{array} .$$

This means $\xi(g) \in \Gamma_r$. Hence $\xi(\Gamma_l) \subset \Gamma_r$. On the other hand, we have $\xi(\Gamma_r) = \Gamma_r$ and $\xi(\Gamma_l) = \Gamma_l$, since ξ preserves the braid structure by (a). Hence $\Gamma_l = \Gamma_r = \Gamma$.

(c) (5.9) and (5.10) imply

$$g\xi(x) = \xi(x)x^{-1}gx \quad \text{and} \quad x\xi(g) = \xi(x)\xi(g)\xi(x)^{-1}x$$

if $g \in \Gamma$ and $x \in S$. The assertion follows from this.

(d) is obvious. ■

We consider the set version of ξ -braided groups.

DEFINITION 5.9. A ξ -braided set means a triple (X, σ, ξ) where (X, σ) is a non-degenerate braided set and ξ is a bijection of X onto itself satisfying condition (5.8) for $S = X$.

THEOREM 5.10. *Let (X, σ, ξ) be a ξ -braided set. Then ξ extends to a group automorphism $\bar{\xi}$ of G_X . $(G_X, \bar{\xi})$ is a ξ -braided group.*

Proof. Similarly to Proposition 5.8 (a), ξ is an automorphism of the braided set (X, σ) . Hence it induces an automorphism $\bar{\xi}$ of the braided group G_X . Condition (5.8) for $S = G_X$ can be deduced easily from (5.8) for $S = X$ by using Proposition 1.2. ■

COROLLARY 5.11. *We have $\Gamma_l = \Gamma_r = \Gamma$ and $\bar{\xi}(\Gamma) = \Gamma$ with the notations of §3 (above Proposition 3.5).*

This can be proved similarly to Proposition 5.8 (b).

If (X, σ, ξ) is a finite ξ -braided set, we have a finite ξ -braided group G_X/Γ yielding a minimal quasitriangular Hopf algebra $H(G_X/\Gamma, G_X/\Gamma)$.

6. Quasitriangular structures on $H(S, B)$. Let H be a Hopf algebra over a field k . Recall that a quasitriangular structure on H is given by an invertible element R in $H \otimes H$ satisfying the following conditions:

$$\begin{aligned}
 (6.1) \quad & (\Delta \otimes \text{id})(R) = R_{13}R_{23}, \\
 (6.2) \quad & (\text{id} \otimes \Delta)(R) = R_{13}R_{12}, \\
 (6.3) \quad & \Delta^{\text{op}}(x) = R\Delta(x)R^{-1}, \quad x \in H.
 \end{aligned}$$

If (H, R) is a quasitriangular Hopf algebra, the category of right H modules \mathcal{M}_H has the following structure of a braided category. For two right H modules V, W , the map

$$\tau : V \otimes W \rightarrow W \otimes V, \quad \tau(v \otimes w) = (w \otimes v)R$$

is a right H linear isomorphism. This natural isomorphism τ satisfies the hexagon axiom making \mathcal{M}_H into a braided category.

Let (S, B) be a matched pair of groups where S is finite. Let (ξ, η) be an LYZ pair for (S, B) . We define an element in $H(S, B) \otimes H(S, B)$:

$$(6.4) \quad R_{\xi, \eta} = \sum_{s, t \in S} \eta(t')^{-1} \begin{array}{c} s' \\ \diagdown \\ \text{ } \\ \diagup \\ s \end{array} \otimes \begin{array}{c} t' \\ \diagdown \\ \text{ } \\ \diagup \\ \xi(s) \end{array} \xi(s')$$

where we use the braided structure $\begin{array}{c} s & t \\ \diagdown & / \\ t' & s' \end{array} \quad (4.7)$ on S . Note that

$$(6.4.1) \quad \begin{array}{c} s & t \\ \diagdown & / \\ t' & s' \end{array} \Rightarrow \begin{array}{c} s & \eta(t) \\ \diagdown & / \\ \eta(t') & s' \end{array} \quad \text{and} \quad \begin{array}{c} t' & \xi(s') \\ \diagdown & / \\ \xi(s) & t \end{array}, \quad \text{hence} \quad \begin{array}{c} s' & \eta(t)^{-1} \\ \diagdown & / \\ \eta(t')^{-1} & s \end{array}.$$

THEOREM 6.1 ([LYZ2], Theorem 2.3). *$R_{\xi, \eta}$ is a quasitriangular structure on $H(S, B)$, and we have*

$$R_{\eta, \xi} = \text{tw}(R_{\xi, \eta}^{-1})$$

where $\text{tw}(a \otimes b) = b \otimes a$.

In fact, Lu, Yan and Zhu characterize these quasitriangular structures as positive ones when $k = \mathbb{C}$. It is possible to check that the $R_{\xi, \eta}$ (6.4) satisfies conditions (6.1)–(6.3) by direct calculations. But in the following, we would like to give a natural categorical explanation of this fact, suggested by Masuoka [Ms3].

We begin by describing the category of right $H(S, B)$ modules $\mathcal{M}_{H(S, B)}$ explicitly.

Define the category ${}^S\mathcal{M}_B$ as follows. An object is an S -graded vector space over k , $V = (V_s)_{s \in S}$ which is also a right kB module in such a way that

$$(6.5) \quad V_s b \subset V_{s \leftarrow b}, \quad s \in S, \quad b \in B,$$

where we use the right action $S \leftarrow B$. Morphisms in ${}^S\mathcal{M}_B$ are kB linear maps preserving the S -gradation. If V and W are two objects in ${}^S\mathcal{M}_B$, the tensor product $V \otimes W$ has S -gradation

$$(6.6) \quad (V \otimes W)_s = \bigoplus_{s=tu} V_t \otimes W_u.$$

Define a right B action on $V \otimes W$ as follows:

$$(6.7) \quad (v \otimes w_u)b = v(u \rightarrow b) \otimes w_u b, \quad v \in V, \quad w_u \in W_u, \quad b \in B,$$

where we use the left action $S \rightarrow B$. This structure makes $V \otimes W$ into an object in ${}^S\mathcal{M}_B$, and ${}^S\mathcal{M}_B$ becomes a tensor category with this tensor product.

PROPOSITION 6.2. *The tensor categories $\mathcal{M}_{H(S, B)}$ and ${}^S\mathcal{M}_B$ are identified with each other as tensor categories.*

Proof. Let V be a right $H(S, B)$ module. We put

$$(6.8) \quad V_s = V \cdot \begin{array}{c} s & 1 \\ \diamond & \\ 1 & s \end{array}, \quad s \in S.$$

Since $\begin{array}{c} s & 1 \\ \diamond & \\ 1 & s \end{array}$, $s \in S$ are orthogonal idempotents, we have $V = \bigoplus_{s \in S} V_s$. Thus V is S -graded. Define a right B action by

$$(6.9) \quad v_s b = v_s \cdot \begin{array}{c} s & b \\ \diamond & \\ b' & s' \end{array}, \quad v_s \in V_s, \quad s \in S, \quad b \in B,$$

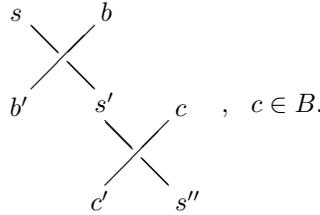
where $\begin{array}{c} s & b \\ \times & \\ b' & s' \end{array}$. We claim V is an object in ${}^S\mathcal{M}_B$. Since

$$\begin{array}{c} s & b \\ \diamond & \\ b' & s' \end{array} \cdot \begin{array}{c} s' & 1 \\ \diamond & \\ 1 & s' \end{array} = \begin{array}{c} s & b \\ \diamond & \\ b' & s' \end{array}$$

we have

$$(v_s b) \cdot \begin{array}{c} s' & 1 \\ \diamond & \\ 1 & s' \end{array} = v_s b.$$

This means (6.5), since $s' = s \leftarrow b$. Assume we have



Then we have

$$(v_s b)c = v_s \cdot \begin{array}{|c|} \hline s \quad b \\ \hline b' \quad s' \\ \hline \end{array} \cdot \begin{array}{|c|} \hline s' \quad c \\ \hline c' \quad s'' \\ \hline \end{array} = v_s \cdot \begin{array}{|c|} \hline s \quad bc \\ \hline b'c \quad s'' \\ \hline \end{array} = v_s(bc)$$

and $v_s 1 = v_s$. Hence V becomes an object in ${}^S\mathcal{M}_B$. Conversely, if V is an object in ${}^S\mathcal{M}_B$, we define a right $H(S, B)$ action on V as follows. Let $v = (v_s)_{s \in S}$ be an element in $V = \bigoplus_{s \in S} V_s$. We put

$$(6.10) \quad v \cdot \begin{array}{|c|} \hline s \quad b \\ \hline b' \quad s' \\ \hline \end{array} = v_s b.$$

we leave the reader to check that V becomes indeed a right $H(S, B)$ module. In this way, we can identify $\mathcal{M}_{H(S, B)} = {}^S\mathcal{M}_B$ as categories. We also leave it the reader to check that the diagonal action on $V \otimes W$ is described by (6.6) and (6.7). ■

Let G be a group and B a subgroup of G . Define a category ${}^G_B\mathcal{M}_B$ as follows. An object is a G -graded vector space $M = (M_g)_{g \in G}$ which is a kB bimodule in such a way that

$$(6.11) \quad bM_g c \subset M_{bgc}, \quad b, c \in B, \quad g \in G.$$

Morphisms are kB bimodule maps preserving the G -gradation. If M and N are objects in ${}^G_B\mathcal{M}_B$, we have a kB bimodule $M \otimes_{kB} N$, which has the following G -gradation:

$$(M \otimes_{kB} N)_g = \text{the span of } m_f \otimes n_h \text{ for all } m_f \in M_f, n_h \in N_h \text{ with } fh = g.$$

It is easy to check that $M \otimes_{kB} N$ becomes an object in ${}^G_B\mathcal{M}_B$. Thus ${}^G_B\mathcal{M}_B$ is a tensor category.

PROPOSITION 6.3. *The tensor categories ${}^S\mathcal{M}_B$ and ${}^{B \bowtie S}_B\mathcal{M}_B$ are canonically equivalent as tensor categories.*

Proof. Let V be an object in ${}^S\mathcal{M}_B$. We make $kB \otimes V$ into an object in ${}^{B \bowtie S}_B\mathcal{M}_B$. Define the $B \bowtie S$ -gradation by

$$(6.12) \quad (kB \otimes V)_{(b, s)} = b \otimes V_s, \quad (b, s) \in B \bowtie S.$$

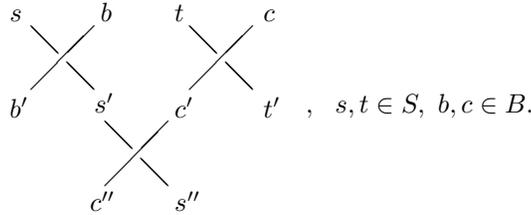
Define the kB bimodule action by

$$a(b \otimes v_s)c = ab(s \rightarrow c) \otimes v_s c, \quad a, b, c \in B, \quad v_s \in V_s, \quad s \in S.$$

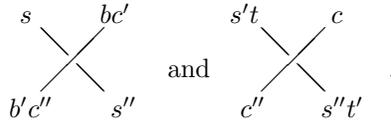
One can easily check that the above structures make $kB \otimes V$ into an object in ${}^B_{B \bowtie S} \mathcal{M}_B$. If $V, W \in {}^S \mathcal{M}_B$, we have a left kB linear isomorphism

$$(6.13) \quad \begin{aligned} (kB \otimes V) \otimes_{kB} (kB \otimes W) &\simeq kB \otimes V \otimes W \\ (a \otimes v_s) \otimes (b \otimes w_t) &\leftrightarrow (a \otimes v_s)b \otimes w_t. \end{aligned}$$

Both elements above have grade $(a, s)(b, t)$ in $B \bowtie S$. Hence the isomorphism preserves the $B \bowtie S$ -graduation. We claim that it is right kB linear. We write



Then we have



It follows from the left diagram above that the element

$$(6.13.1) \quad (a \otimes v_s) \otimes (b \otimes w_t)c = (a \otimes v_s) \otimes (bc' \otimes w_t)c$$

corresponds to

$$(6.13.2) \quad (a \otimes v_s)bc' \otimes w_t c = ab'c'' \otimes v_s bc' \otimes w_t c.$$

It follows from the right diagram that we have

$$(6.13.3) \quad \begin{aligned} ((a \otimes v_s)b \otimes w_t)c &= (ab' \otimes v_s b \otimes w_t)c \\ &= ab'c'' \otimes (v_s b \otimes w_t)c = ab'c'' \otimes v_s bc' \otimes w_t c. \end{aligned}$$

Hence the isomorphism (6.13) is right kB linear.

We have established a monoidal functor

$$(6.14) \quad V \mapsto kB \otimes V, \quad {}^S \mathcal{M}_B \rightarrow {}^B_{B \bowtie S} \mathcal{M}_B.$$

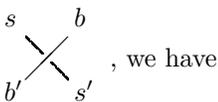
We show this is a categorical equivalence. Let M be in ${}^B_{B \bowtie S} \mathcal{M}_B$. Through the projection $B \bowtie S \rightarrow B$, we may view M as a left kB Hopf module. Hence, if we put

$$(6.15) \quad V = {}^{\text{co}B} M = \bigoplus_{s \in S} M_{(1,s)},$$

we have an isomorphism

$$(6.16) \quad kB \otimes V \rightarrow M, \quad b \otimes v \mapsto bv.$$

If we give the S -graduation on V by $V_s = M_{(1,s)}$, then it follows that $M_{(b,s)} = b \otimes V_s$. If



$$M_{(1,s)}b \subset M_{(b',s')},$$

since $(1, s)(b, 1) = (b', s')$. Hence $V_s b \subset b' \otimes V_{s'}$. We define a new multiplication $\cdot b : V_s \rightarrow V_{s'}$ by putting

$$(6.17) \quad v_s b = b' \otimes v_s \cdot b, \quad v_s \in V_s.$$

We leave it to the reader to check that these structures make V into an object in ${}^S \mathcal{M}_B$, and that the isomorphism (6.16) is a morphism in ${}^{B \bowtie S} \mathcal{M}_B$. Hence the functor $M \mapsto V = {}^{\text{co}B} M$ gives a quasi-inverse to the functor (6.14). ■

Let B be a subgroup of a group G , and let $\xi, \eta : G \rightarrow B$ be group homomorphisms which are identity on B and such that

$$(6.18) \quad \text{Ker}(\xi) \text{ and } \text{Ker}(\eta) \text{ commute with each other element-wise.}$$

Masuoka [Ms3] has constructed a braiding $\bar{\tau} = \bar{\tau}_{\xi, \eta}$ on the tensor category ${}^G_B \mathcal{M}_B$ as follows.

PROPOSITION 6.4 ([Ms3], cf. also [Sch], 6.3 Theorem). (a) *Let M, N be two objects in ${}^G_B \mathcal{M}_B$. There is an isomorphism $\bar{\tau}_{M, N} : M \otimes_{kB} N \xrightarrow{\sim} N \otimes_{kB} M$ in ${}^G_B \mathcal{M}_B$ such that*

$$\bar{\tau}_{M, N}(m_f \otimes n_g) = \eta(f)n_g \xi(g)^{-1} \otimes \eta(f)^{-1} m_f \xi(g), \quad m_f \in M_f, \quad n_g \in N_g \text{ with } f, g \in G.$$

(b) *The natural isomorphism $\bar{\tau} = (\bar{\tau}_{M, N})_{M, N}$ satisfies the hexagon condition.*

(c) *If we write $\bar{\tau} = \bar{\tau}_{\xi, \eta}$, then we have*

$$(\bar{\tau}_{\xi, \eta})_{M, N}^{-1} = (\bar{\tau}_{\eta, \xi})_{N, M}.$$

Proof. We show briefly that the map $\bar{\tau}_{M, N}$ is well-defined and that it is a morphism in ${}^G_B \mathcal{M}_B$. We leave it to the reader to verify the other properties. If $b \in B$, then

$$\bar{\tau}_{M, N}(m_f b \otimes n_g) = \eta(fb)n_g \xi(g)^{-1} \otimes \eta(fb)^{-1} m_f b \xi(g),$$

$$\bar{\tau}_{M, N}(m_f \otimes b n_g) = \eta(f) b n_g \xi(bg)^{-1} \otimes \eta(f)^{-1} m_f \xi(bg).$$

Since $\eta(fb) = \eta(f)b$ and $\xi(bg) = b\xi(g)$, these elements coincide in $N \otimes_{kB} M$. Hence $\bar{\tau}_{M, N}$ is well-defined. We have

$$\begin{aligned} \bar{\tau}_{M, N}(b m_f \otimes n_g) &= \eta(bf)n_g \xi(g)^{-1} \otimes \eta(bf)^{-1} b m_f \xi(g) \\ &= b \eta(f)n_g \xi(g)^{-1} \otimes \eta(f)^{-1} m_f \xi(g) \end{aligned}$$

implying that $\bar{\tau}_{M, N}$ is left kB linear. Similarly it is right kB linear. Finally, the element $\bar{\tau}_{M, N}(m_f \otimes n_g)$ has grade

$$\eta(f)g\xi(g)^{-1} \cdot \eta(f)^{-1}f\xi(g) = \eta(f)\eta(f)^{-1}f \cdot g\xi(g)^{-1}\xi(g) = fg$$

by (6.18), since $g\xi(g)^{-1} \in \text{Ker}(\xi)$ and $\eta(f)^{-1}f \in \text{Ker}(\eta)$. Hence $\bar{\tau}_{M, N}$ preserves the G gradation, and we conclude it is a morphism in ${}^G_B \mathcal{M}_B$. ■

We get back to the matched pair of groups (S, B) with S finite. Let (ξ, η) be an LYZ pair for it. Let $\bar{\xi}, \bar{\eta} : B \bowtie S \rightarrow B$ be the extended group maps (4.4). The pair $\bar{\xi}, \bar{\eta}$ satisfies (6.18) by Proposition 4.3. Hence we have the Masuoka braiding $\bar{\tau} = \bar{\tau}_{\bar{\xi}, \bar{\eta}}$ on the tensor category ${}^{B \bowtie S} \mathcal{M}_B$. Since we have monoidal equivalences

$$\mathcal{M}_{H(S, B)} \approx {}^S \mathcal{M}_B \approx {}^{B \bowtie S} \mathcal{M}_B$$

we can transport the braiding $\bar{\tau}$ onto the category $\mathcal{M}_{H(S, B)}$. Let τ be the transported braiding structure on $\mathcal{M}_{H(S, B)}$.

PROPOSITION 6.5 ([Ms3]). *Let V, W be right $H(S, B)$ modules. Then we have*

$$(6.19) \quad \tau_{V,W}(v \otimes w) = (w \otimes v)R_{\xi,\eta}, \quad v \in V, \quad w \in W,$$

where $R_{\xi,\eta}$ is the LYZ element (6.4).

Proof. We may identify V, W as objects in ${}^S\mathcal{M}_B$ (Prop. 6.2). We use the notation of (6.4) and (6.4.1). We only have to prove

$$\tau_{V,W}(v_{t'} \otimes w_{s'}) = w_{s'}\eta(t)^{-1} \otimes v_{t'}\xi(s'), \quad v_{t'} \in V_{t'}, \quad w_{s'} \in W_{s'}.$$

In fact, taking $M = kB \otimes V, N = kB \otimes W, f = (1, t'), g = (1, s')$ in Proposition 6.4 (a), we have

$$\bar{\tau}_{M,N}((1 \otimes v_{t'}) \otimes (1 \otimes w_{s'})) = \eta(t')(1 \otimes w_{s'})\xi(s')^{-1} \otimes \eta(t')^{-1}(1 \otimes v_{t'})\xi(s').$$

Since $\begin{array}{c} t' \quad \xi(s') \\ \diagdown \quad \diagup \\ \xi(s) \quad t \end{array}$ (6.4.1), we have $\eta(t')\xi(s') = \xi(s)\eta(t)$ and

$$\eta(t')^{-1}(1 \otimes v_{t'})\xi(s') = \eta(t')^{-1}\xi(s) \otimes v_{t'}\xi(s') = \xi(s')\eta(t)^{-1} \otimes v_{t'}\xi(s').$$

Hence

$$\begin{aligned} \bar{\tau}_{M,N}((1 \otimes v_{t'}) \otimes (1 \otimes w_{s'})) &= \eta(t')(1 \otimes w_{s'})\xi(s')^{-1} \otimes (\xi(s')\eta(t)^{-1} \otimes v_{t'}\xi(s')) \\ &= \eta(t')(1 \otimes w_{s'})\eta(t)^{-1} \otimes (1 \otimes v_{t'}\xi(s')) \\ &= (\eta(t')\eta(t)^{-1} \otimes w_{s'}\eta(t)^{-1}) \otimes (1 \otimes v_{t'}\xi(s')) \\ &= (1 \otimes w_{s'}\eta(t)^{-1}) \otimes (1 \otimes v_{t'}\xi(s')), \end{aligned}$$

since we have $\begin{array}{c} s' \quad \eta(t)^{-1} \\ \diagdown \quad \diagup \\ \eta(t')^{-1} \quad s \end{array}$ (6.4.1). This implies that the map $\tau_{V,W}$ (6.19) corresponds to

$\bar{\tau}_{M,N}$ through the isomorphism (6.13). ■

This gives a categorical proof to Theorem 6.1.

Let G be a group with a subgroup B . Assume there are two finite subgroups S, T of G such that

$$G = B \bowtie S = B \bowtie T.$$

Proposition 4.1 of [LYZ2] claims that the Hopf algebras $H(S, B)$ and $H(T, B)$ are quasi-isomorphic. The above approach admits the following naive categorical explanation of this fact, as noted in [Ms3].

We view $T \subset B \bowtie S$ and write $t = (t_1, t_2)$ for $t \in T$. Then the map $t \mapsto t_2, T \rightarrow S$ is bijective. If $t, u \in T$, then

$$(6.20) \quad (tu)_1 = t_1u'_1, \quad (tu)_2 = t'_2u_2, \quad \text{where} \quad \begin{array}{c} t_2 \quad u_1 \\ \diagdown \quad \diagup \\ u'_1 \quad t'_2 \end{array} .$$

We denote the jigsaw puzzle basis of $H(T, B)$ by $\begin{matrix} t & b \\ \diamond & \\ c & u \end{matrix}$ with $t, u \in T, b, c \in B$ such that $tb = cu$.

PROPOSITION 6.6 ([LYZ2], 4.1). *There is an algebra isomorphism $\phi : H(T, B) \rightarrow H(S, B)$ such that*

$$\phi \left(\begin{matrix} t & b \\ \diamond & \\ c & u \end{matrix} \right) = \begin{matrix} t_2 & b \\ \diamond & \\ t_1^{-1}cu_1 & u_2 \end{matrix} .$$

This is easily verified.

For an object V in ${}^S\mathcal{M}_B$, let V^ϕ be the object in ${}^T\mathcal{M}_B$ obtained by viewing V as a right $H(T, B)$ module through ϕ , i.e., we have

$$(V^\phi)_t = V_{t_2}, \quad \text{with the same } B \text{ action.}$$

PROPOSITION 6.7. *We have a commutative diagram of functors up to a natural isomorphism:*

$$(6.21) \quad \begin{array}{ccc} {}^S\mathcal{M}_B & \xrightarrow{(\)^\phi} & {}^T\mathcal{M}_B \\ \text{cano} \searrow & & \swarrow \text{cano} \\ & & {}^G_B\mathcal{M}_B \end{array}$$

Proof. It is enough to define the left kB isomorphism

$$kB \otimes V \simeq kB \otimes V^\phi \quad \text{by} \quad t_1 \otimes v_t \leftrightarrow 1 \otimes v_t, \quad t \in T, \quad v_t \in V_{t_2}.$$

One can easily check that this is right kB linear, too, preserving the G gradation. ■

The commutative diagram (6.21) yields a monoidal structure on the equivalence $(\)^\phi$ as follows. If V, W are two objects in ${}^S\mathcal{M}_B$, we have isomorphisms in ${}^G_B\mathcal{M}_B$:

$$\begin{aligned} kB \otimes V^\phi \otimes W^\phi &\simeq (kB \otimes V^\phi) \otimes_{kB} (kB \otimes W^\phi) \simeq (kB \otimes V) \otimes_{kB} (kB \otimes W) \\ &\simeq kB \otimes V \otimes W \simeq kB \otimes (V \otimes W)^\phi. \end{aligned}$$

This induces the isomorphism in ${}^T\mathcal{M}_B$:

$$(6.22) \quad V^\phi \otimes W^\phi \simeq (V \otimes W)^\phi, \quad v_t \otimes w_u \leftrightarrow v_t u_1 \otimes w_u, \quad t, u \in T, \quad v_t \in V_{t_2}, \quad w_u \in W_{u_2}.$$

If we put

$$(6.23) \quad J = \sum_{t, u \in T} \begin{matrix} t_2 & u_1 \\ \diamond & \\ u_1 & t_2 \end{matrix} \otimes \begin{matrix} u_2 & 1 \\ \diamond & \\ 1 & u_2 \end{matrix} \in H(S, B) \otimes H(S, B)$$

with the notation in (6.20), then the isomorphism (6.22) is precisely the multiplication $\cdot J$. It follows immediately that J is a Harrison cocycle on $H(S, B)$, and the fact that $\cdot J$ is right $H(S, B)$ linear means we have

$$J\Delta\phi(x) = \sum (\phi(x_1) \otimes \phi(x_2))J, \quad x \in H(T, B).$$

Hence if we twist the Δ of $H(S, B)$ by J , it follows that ϕ is an isomorphism of Hopf algebras $H(T, B) \xrightarrow{\sim} H(S, B)^J$.

References

- [EG] P. Etingof and S. Gelaki, *A method of construction of finite dimensional triangular semisimple Hopf algebras*, Math. Res. Letters 5 (1998), 551–561.
- [ESS] P. Etingof, T. Schedler and A. Soloviev, *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. 100 (1999), 169–209.
- [H] I. Hofstetter, *Extensions of Hopf algebras and their cohomological description*, J. Algebra 164 (1994), 264–298.
- [K] G. I. Kac, *Extensions of groups to ring groups*, Math. USSR Sbornik 5 (1968), 451–474.
- [LYZ1] J. Lu, M. Yan and Y. Zhu, *On the set-theoretical Yang-Baxter equation*, Duke Math. J. 104 (2000), 1–18.
- [LYZ2] —, —, —, *Quasi-triangular structures on Hopf algebras with positive bases*, Contemp. Math. 267 (2000), 339–356.
- [Mj] S. Majid, *Foundations of Quantum Group Theory*, Cambridge Univ. Press, 1995.
- [Ms1] A. Masuoka, *Calculations of some groups of Hopf algebra extensions*, J. Algebra 191 (1997), 568–588.
- [Ms2] —, *Faithfully flat forms and cohomology of Hopf algebra extensions*, Comm. Algebra 25 (1997), 1169–1197.
- [Ms3] —, *Joy of Hopf-Galois theory*, Annual Meeting of the Math. Society of Japan, Keio Univ., 2001 (lecture in Japanese).
- [Sch] P. Schauenburg, *Hopf modules and Yetter-Drinfeld modules*, J. Algebra 169 (1994), 874–890.
- [Si] W. M. Singer, *Extension theory for connected Hopf algebras*, J. Algebra 21 (1972), 1–16.
- [So] A. Soloviev, *Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation*, Math. Res. Letters 7 (2000), 577–596.
- [T] M. Takeuchi, *Matched pairs of groups and bismash products of Hopf algebras*, Comm. Algebra 9 (1981), 841–882.