CHAPTER 1

A quick introduction to Nichols algebras

The structure theory of Nichols algebras is a central theme throughout the book. In this chapter we introduce the concepts which are needed to deal with Nichols algebras of group type and also in the general case later in Chapters 6 and 7.

In Section 1.3 we study \( \mathbb{N}_0 \)-graded connected coalgebras which are strictly graded, that is, the only primitive elements are in degree 1. For any \( \mathbb{N}_0 \)-graded connected coalgebra \( C \), let \( I_C(n) \) be the kernel of
\[
C(n) \subseteq C \xrightarrow{\Delta^{n-1}} C^\otimes n \xrightarrow{\pi_1^\otimes n} C(1)^\otimes n.
\]
Then \( I_C = \bigoplus_{n \geq 2} I_C(n) \) is the largest coideal of \( C \) in degree \( \geq 2 \), and \( B(C) = C/I_C \) is a universally defined strictly graded coalgebra quotient of \( C \) which coincides with \( C \) in degree 0 and 1.

The tensor algebra of a Yetter-Drinfeld module \( V \) (over a group algebra or in the general case in Chapter 7) is a braided Hopf algebra, where the elements in \( V \) are primitive. In Section 1.6 we define the Nichols algebra of \( V \) by
\[
B(V) = B(T(V)) = T(V)/I_{T(V)}.
\]
This is a braided Hopf algebra quotient of the tensor algebra. In Section 1.9 we describe the comultiplication of the tensor algebra \( T(V) \) by braided shuffle maps, and the relations of the Nichols algebra as the kernels of the braided symmetrizer maps.

In the last section we will discuss several important examples and mention others with reference to a proof.

1.1. Algebras, coalgebras, modules and comodules

Convention. The ground field is denoted by \( \mathbb{k} \). This is an arbitrary field. If we use additional assumptions on the field, we will say so explicitly.

We write \( \mathbb{k}^\times \) for the subgroup of non-zero elements of \( \mathbb{k} \). Vector spaces are vector spaces over \( \mathbb{k} \), and linear maps between vector spaces are \( \mathbb{k} \)-linear maps. If \( V, W \) are vector spaces, then \( \text{Hom}(V, W) \) is the set of all linear maps from \( V \) to \( W \), and \( V \otimes W = V \otimes_\mathbb{k} W \) is the tensor product over \( \mathbb{k} \). In this book we will use the following convention. If \( U, V, W \) are vector spaces, then we will identify
\[
(U \otimes V) \otimes W = U \otimes (V \otimes W)
\]
using the natural isomorphism
\[
(U \otimes V) \otimes W \xrightarrow{\cong} U \otimes (V \otimes W), \ (u \otimes v) \otimes w \mapsto u \otimes (v \otimes w).
\]
Hence we will omit the brackets in tensor products of several vector spaces. Occa-
sionally we will also suppress the natural isomorphisms
\[ k \otimes V \cong V, \quad \alpha \otimes v \mapsto \alpha v, \quad V \otimes k \cong V, \quad v \otimes \alpha \mapsto \alpha v. \]
Thus we will write \( V = k \otimes V \) and \( V = V \otimes k \).

The dual of a vector space \( V \) is denoted by \( V^* = \text{Hom}(V, k) \).

Let \( A \) be a vector space, and \( \mu : A \times A \to A \) a map (called multiplication) whose images will be denoted by \( \mu(a, b) = ab \) for all \( a, b \in A \). Then \( A \) together with \( \mu \) is an algebra (with unit element) if there exists an element \( 1_A = 1 \in A \) such that for all \( a, b, c \in A \) and \( \alpha \in k \),
\[
\begin{align*}
a(bc) &= (ab)c, \\
a(b + c) &= ab + ac, \quad (a + b)c = ac + bc, \\
\alpha(ab) &= (\alpha a)b = a(\alpha b), \\
1a &= a = a1.
\end{align*}
\]
The unit element \( 1_A \) of an algebra is uniquely determined. It defines a linear map \( \eta : k \to A, \quad \alpha \mapsto \alpha 1_A \). The multiplication map \( \mu \) is a \( k \)-bilinear map. Hence it is given by a linear map
\[ \mu : A \otimes A \to A, \quad a \otimes b \mapsto ab. \]

Let \( V, W \) be vector spaces. The linear map \( \tau_{V, W} : V \otimes W \to W \otimes V, \quad v \otimes w \mapsto w \otimes v, \)
is called the flip map of \( V \) and \( W \).

Let \( A, B \) be algebras. The tensor product of vector spaces \( A \otimes B \) is an algebra with unit \( 1 \otimes 1 \) and multiplication given by
\[
(a \otimes b)(a' \otimes b') = aa' \otimes bb'
\]
for all \( a, a' \in A, b, b' \in B \). Thus the multiplication map of \( A \otimes B \) is the composition
\[
(A \otimes B) \otimes (A \otimes B) \xrightarrow{\text{id}_A \otimes \tau_{B, A} \otimes \text{id}_B} (A \otimes A) \otimes (B \otimes B) \xrightarrow{\mu_A \otimes \mu_B} A \otimes B.
\]
This algebra structure on \( A \otimes B \) is called the tensor product of the algebras \( A \) and \( B \). Note that for algebras \( A, B, C \), the canonical isomorphism
\[
(A \otimes B) \otimes C \cong A \otimes (B \otimes C)
\]
is an isomorphism of algebras, and following our convention, we will identify these algebras.

The opposite algebra \( A^{\text{op}} \) is \( A \) as a vector space, where the elements are denoted by \( a^{\text{op}} = a \in A \), and where the multiplication is given by
\[ a^{\text{op}}b^{\text{op}} = (ba)^{\text{op}} \]
for all \( a, b \in A \).

An algebra homomorphism (or algebra map) \( \rho : A \to B \) is a linear map satisfying \( \rho(1) = 1 \) and \( \rho(ab) = \rho(a)\rho(b) \) for all \( a, b \in A \). An algebra anti-
homomorphism \( \rho : A \to B \) is an algebra homomorphism \( \rho : A \to B^{\text{op}} \). We write \( \text{Alg}(A, B) \) for the set of algebra homomorphisms from \( A \) to \( B \).
An algebra can equivalently be defined as a triple \((A, \mu, \eta)\), where \(A\) is a vector space and \(\mu : A \otimes A \to A\) and \(\eta : \mathbb{k} \to A\) are linear maps such that the following diagrams commute.

\[
\begin{array}{ccc}
A \otimes A \otimes A & \xrightarrow{\mu \otimes \text{id}_A} & A \otimes A \\
\downarrow \id_A \otimes \mu & & \downarrow \mu \\
A \otimes A & \xrightarrow{\mu} & A
\end{array}
\]

(associativity)

\[
\begin{array}{ccc}
A \otimes \mathbb{k} & \xrightarrow{\eta \otimes \text{id}_A} & A \otimes A \\
\downarrow \mu & & \downarrow \mu \\
A & \xrightarrow{\text{id}_A \otimes \eta} & A \otimes \mathbb{k}
\end{array}
\]

(unit)

Let \(A\) and \(B\) be algebras. An algebra homomorphism \(\rho : A \to B\) is a linear map such that the following diagrams commute.

\[
\begin{array}{ccc}
A \otimes A & \xrightarrow{\rho \otimes \rho} & B \otimes B \\
\downarrow \mu_A & & \downarrow \mu_B \\
A & \xrightarrow{\rho} & B
\end{array}
\]

(1.1.5)

We introduce coalgebras by formally inverting the arrows in the definition of an algebra.

**Definition 1.1.1.** Let \(C\) be a vector space, and let \(\Delta : C \to C \otimes C\), \(\varepsilon : C \to \mathbb{k}\) be linear maps called comultiplication and counit. Then \((C, \Delta, \varepsilon)\) or simply \(C\) is a **coalgebra** if the following diagrams commute.

\[
\begin{array}{ccc}
C & \xrightarrow{\Delta} & C \otimes C \\
\downarrow \Delta & & \downarrow \text{id}_C \otimes \Delta \\
C \otimes C & \xrightarrow{\Delta \otimes \text{id}_C} & C \otimes C \otimes C
\end{array}
\]

(coassociativity)

\[
\begin{array}{ccc}
C & \xrightarrow{\Delta} & C \otimes C \\
\downarrow \Delta & & \downarrow \varepsilon \otimes \text{id}_C \\
C \otimes \mathbb{k} & \xrightarrow{\text{id}_C \otimes \varepsilon} & \mathbb{k} \otimes C
\end{array}
\]

(counit)

A subspace \(D\) of a coalgebra \(C\) is called a **subcoalgebra** if \(\Delta(D) \subseteq D \otimes D\).

Let \(C, D\) be coalgebras. The vector space \(C \otimes D\) is a coalgebra with counit \(\varepsilon_C \otimes \varepsilon_D\) and comultiplication

\[
\begin{array}{ccc}
C \otimes D & \xrightarrow{\Delta_C \otimes \Delta_D} & C \otimes C \otimes D \otimes D \\
\downarrow \text{id}_C \otimes \tau_{C,D} \otimes \text{id}_D & & \downarrow \text{id}_C \otimes \tau_{C,D} \otimes \text{id}_D \\
(C \otimes D) \otimes (C \otimes D)
\end{array}
\]

(1.1.9)
This coalgebra structure on $C \otimes D$ is called the **tensor product of the coalgebras** $C$ and $D$.

A linear map $\varphi : C \to D$ is a **coalgebra homomorphism** or a **coalgebra map** if the following diagrams commute.

\[
\begin{array}{ccc}
C & \xrightarrow{\varphi} & D \\
\downarrow{\Delta_C} & & \downarrow{\Delta_D} \\
C \otimes C & \xrightarrow{\varphi \otimes \varphi} & D \otimes D
\end{array}
\]

(1.1.10)

\[
\begin{array}{ccc}
C & \xrightarrow{\varphi} & D \\
\downarrow{\varepsilon_C} & & \downarrow{\varepsilon_D} \\
\mathbb{k} & & \\
\end{array}
\]

(1.1.11)

We denote by $\text{Coalg}(C, D)$ the set of all coalgebra homomorphisms from $C$ to $D$.

The coalgebra $C$ is called **cocommutative** if the diagram

\[
\begin{array}{ccc}
C & \xrightarrow{\Delta} & C \otimes C \\
\downarrow{\Delta} & & \downarrow{\tau_{C,C}} \\
C \otimes C & & \\
\end{array}
\]

(cocommutativity)

(1.1.12)

commutes.

The **coopposite coalgebra** $C^{\text{cop}}$ is $C$ as a vector space with comultiplication $\tau_{C,C} \Delta$ and counit $\varepsilon$. A **coalgebra anti-homomorphism** $f : C \to D$ is a coalgebra homomorphism $f : C \to D^{\text{cop}}$.

**Example 1.1.2.** Let $\Gamma$ be a set and $\mathbb{k}\Gamma$ the vector space with basis $\Gamma$. Then $\mathbb{k}\Gamma$ is a coalgebra with $\Delta(g) = g \otimes g$, $\varepsilon(g) = 1$ for all elements $g \in \Gamma$.

**Example 1.1.3.** Let $C$ be a 3-dimensional vector space with basis $g, h, x$. Define linear maps $\Delta : C \to C \otimes C$ and $\varepsilon : C \to \mathbb{k}$ on the basis of $C$ by

\[
\Delta(g) = g \otimes g, \quad \Delta(h) = h \otimes h, \quad \Delta(x) = g \otimes x + x \otimes h,
\]

\[
\varepsilon(g) = 1, \quad \varepsilon(h) = 1, \quad \varepsilon(x) = 0.
\]

It is easily checked by direct computation that $C$ is a coalgebra.

**Definition 1.1.4.** Let $C$ be a coalgebra.

1. An element $g \in C$ is called **group-like** if $\Delta(g) = g \otimes g$ and $\varepsilon(g) = 1$. Let $G(C) = \{ g \in C \mid g \text{ is group-like} \}$.

2. Let $g, h \in G(C)$. Let $P_{g,h}(C) = \{ x \in C \mid x \text{ is } (g, h)\text{-primitive} \}$, where $x \in C$ is called **$(g, h)$-primitive** if $\Delta(x) = g \otimes x + x \otimes h$.

3. An element $x \in C$ is called **skew-primitive** if there are group-like elements $g, h \in G(C)$ with $x \in P_{g,h}(C)$.

Note that $g \in C$ is group-like if $\Delta(g) = g \otimes g$ and $g \neq 0$, since $g = \varepsilon(g) g$. The sets $P_{g,h}(C)$ with $g, h \in G(C)$ are subspaces of $C$. If $x \in P_{g,h}(C)$, then $\varepsilon(x) = 0$, since $x = \varepsilon(g)x + \varepsilon(x)h$ because of the counit axiom.

**Example 1.1.5.** Let $n \in \mathbb{N}$ and let $C = M_n(\mathbb{k})^*$ denote the dual space of the vector space of $n$ by $n$ matrices. Let $(u_{ij})_{1 \leq i,j \leq n}$ denote the dual basis of the standard basis $(E_{ij})_{1 \leq i,j \leq n}$ of $M_n(\mathbb{k})$, where $E_{ij}$ is a matrix having entry 1 in the
i-th row and j-th column, and zeros elsewhere. Then C together with the linear maps \( \Delta : C \to C \otimes C \) and \( \varepsilon : C \to k \),

\[
\Delta(u_{ij}) = \sum_{k=1}^{n} u_{ik} \otimes u_{kj}, \quad \varepsilon(u_{ij}) = \delta_{ij}
\]

for all \( i, j \in \{1, \ldots, n\} \), is a coalgebra.

The next result is a version of Dedekind’s Lemma in Galois theory on the linear independency of characters.

**Proposition 1.1.6.** Let \( C \) be a coalgebra. Then \( G(C) \) is a linearly independent subset of \( C \).

**Proof.** We show by induction on \( n \) that each subset of \( G(C) \) of \( n \) elements is linearly independent. This is clear for \( n = 1 \). Assume that each subset of \( G(C) \) of \( n \) elements is linearly independent. Let \( g_1, \ldots, g_{n+1} \in G(C) \) be pairwise distinct elements. Assume that there are non-zero scalars \( \alpha_1, \ldots, \alpha_{n+1} \in k \) with \( \sum_{i=1}^{n+1} \alpha_i g_i = 0 \). Then \( g_{n+1} = \sum_{i=1}^{n} \beta_i g_i \), where \( \beta_i = -\frac{\alpha_i}{\alpha_{n+1}} \) for all \( 1 \leq i \leq n \). By applying \( \Delta \) to this equation we get

\[
\sum_{1 \leq i \leq n} \beta_i g_i \otimes g_i = \Delta \left( \sum_{1 \leq i \leq n} \beta_i g_i \right) = \Delta(g_{n+1}) = g_{n+1} \otimes g_{n+1} = \sum_{1 \leq i, j \leq n} \beta_i \beta_j g_i \otimes g_j.
\]

Hence \( n = 1 \) and \( \beta_1 = 1 \) by linear independency of \( g_1, \ldots, g_n \). This is a contradiction to \( g_1 \neq g_2 \). Hence \( g_1, \ldots, g_{n+1} \) are linearly independent. \( \square \)

**Lemma 1.1.7.** Let \( C, D \) be vector spaces and let \( A \subseteq C, B \subseteq D \) be subspaces. Then

\[
A \otimes B = \{ t \in C \otimes D \mid (\text{id}_C \otimes g)(t) \in A \text{ for all } g \in D^*, \quad (f \otimes \text{id}_D)(t) \in B \text{ for all } f \in C^* \}.
\]

**Proof.** The inclusion \( \subseteq \) is clear. Conversely, any \( t \in C \otimes D \) can be written as \( t = \sum_{i=1}^{n} c_i \otimes d_i \) with \( n \in \mathbb{N}_0, c_1, \ldots, c_n \in C, \) and \( d_1, \ldots, d_n \in D \). Take such a presentation of \( t \) for a minimal \( n \). Then both \( c_1, \ldots, c_n \) and \( d_1, \ldots, d_n \) are linearly independent. If \( (f \otimes \text{id}_D)(t) \in B \) for all \( f \in C^* \), then \( d_i \in B \) for all \( i \in \{1, \ldots, n\} \). Similarly, if \( (\text{id}_C \otimes g)(t) \in A \) for all \( g \in D^* \) then \( c_i \in A \) for all \( i \). This implies the inclusion \( \supseteq \). \( \square \)

**Lemma 1.1.8.** A subspace \( D \) of a coalgebra \( C \) is a subcoalgebra if and only if \( (\text{id}_C \otimes f)\Delta(x) \in D, \quad (f \otimes \text{id}_C)\Delta(x) \in D \text{ for all } x \in D, \quad f \in C^* \).

**Proof.** The subspace \( D \) of \( C \) is a subcoalgebra if and only if \( \Delta(x) \in D \otimes D \) for all \( x \in D \). Thus the claim follows from Lemma 1.1.7. \( \square \)

**Proposition 1.1.9.** The intersection of subcoalgebras of a given coalgebra is a subcoalgebra.

**Proof.** Apply Lemma 1.1.8 with \( D \) the intersection of subcoalgebras. \( \square \)

If \( X \subseteq C \) is a subspace of a coalgebra \( C \), by Proposition 1.1.9 we can define the **subcoalgebra of \( C \) generated by \( X \)** as the intersections of all subcoalgebras of \( C \) containing \( X \).
REMARK 1.1.10. For all elements $c$ in a coalgebra $C$ it is useful to symbolically write
\[ \Delta(c) = c_{(1)} \otimes c_{(2)}. \] (Sweedler notation)

In this notation the axioms of a coalgebra are equivalent to the equations
\begin{align*}
(1.1.13) \quad & \Delta(c_{(1)}) \otimes c_{(2)} = c_{(1)} \otimes \Delta(c_{(2)}), \quad \text{(coassociativity)} \\
(1.1.14) \quad & \varepsilon(c_{(1)})c_{(2)} = c = c_{(1)}\varepsilon(c_{(2)}) \quad \text{(counit)}
\end{align*}

for all $c \in C$. Let $c \in C$. Choose finitely many elements $c_{1i}, c_{2i} \in C$, $1 \leq i \leq n$, with $\Delta(c) = \sum_{i=1}^{n} c_{1i} \otimes c_{2i}$. Then the symbolic equations (1.1.13) and (1.1.14) say that
\[ \sum_{i=1}^{n} \Delta(c_{1i}) \otimes c_{2i} = \sum_{i=1}^{n} c_{1i} \otimes \Delta(c_{2i}), \]
\[ \sum_{i=1}^{n} \varepsilon(c_{1i})c_{2i} = c = \sum_{i=1}^{n} c_{1i}\varepsilon(c_{2i}). \]

Let $C$ be a coalgebra. The iterations $\Delta^n$, $n \geq 0$, of $\Delta$ are defined inductively by
\[ \Delta^0 = \text{id}_C : C \to C, \quad \Delta^n = (\text{id}_C \otimes \Delta^{n-1})\Delta : C \to C^\otimes(n+1) \]
for all $n \geq 1$. We extend the symbolic notation above to the iterations of $\Delta$. For all $c \in C$ and $n \geq 1$, we write
\[ \Delta(c) = c_{(1)} \otimes c_{(2)}, \]
\[ \Delta^2(c) = c_{(1)} \otimes c_{(2)} \otimes c_{(3)}, \quad \ldots \]
\[ \Delta^n(c) = c_{(1)} \otimes \cdots \otimes c_{(n+1)}. \]

This notation is useful since implicitly it expresses the axiom of coassociativity. Thus for an element $c$ in a coalgebra,
\[ \Delta(c_{(1)}) \otimes c_{(2)} = c_{(1)} \otimes \Delta(c_{(2)}) = c_{(1)} \otimes c_{(2)} \otimes c_{(3)}. \]

Note that $c_{(1)}$ alone does not make sense. But if $F : C \times \cdots \times C \to V$ is an $n$-fold multilinear function to a vector space $V$, where $n \geq 2$, then
\[ F(c_{(1)}, \ldots, c_{(n)}) = f(\Delta^{n-1}(c)) \]
is a well-defined expression, where $f : C^\otimes^n \to V$ is the linear map defined by $F$.

Let $C, D$ be coalgebras. The formulas for the comultiplication and counit of the tensor product coalgebra $C \otimes D$ are
\begin{align*}
(1.1.16) \quad & \Delta(c \otimes d) = (c_{(1)} \otimes d_{(1)}) \otimes (c_{(2)} \otimes d_{(2)}), \quad \varepsilon(c \otimes d) = \varepsilon(c)\varepsilon(d) \quad \text{for all } c \in C, \; d \in D.
\end{align*}

Quotients of algebras are described by ideals. We define coideals to describe coalgebra quotients.

We first note a lemma on the tensor product of linear maps.

**LEMMA 1.1.11.** Let $f : V \to X$, $g : W \to Y$ be linear maps between vector spaces $V, W, X, Y$. Then $\ker(f \otimes g) = V \otimes \ker(g) + \ker(f) \otimes W$. 
Proof. Choose subspaces \( V' \subseteq V \), \( W' \subseteq W \) such that \( V = \ker(f) \oplus V' \) and \( W = \ker(g) \oplus W' \). Then
\[
V \otimes W = (V \otimes \ker(g)) \oplus (\ker(f) \otimes W') \oplus (V' \otimes W'),
\]
and the restriction of \( f \otimes g \) to \( V' \otimes W' \) is injective. \( \square \)

Definition 1.1.12. Let \( C \) be a coalgebra. A vector subspace \( I \subseteq C \) is a coideal if
\[
\Delta(I) \subseteq I \otimes C + C \otimes I, \quad \varepsilon(I) = 0.
\]

Proposition 1.1.13. Let \( C, D \) be coalgebras, \( f : C \to D \) a coalgebra map.

1. If \( I \subseteq C \) is a coideal, then \( f(I) \subseteq D \) is a coideal, and the quotient vector space \( C/I \) is a coalgebra with
\[
\Delta(x) = \overline{x(1)} \otimes \overline{x(2)}, \quad \varepsilon(x) = \varepsilon(x)
\]
for all \( x \in C \), where \( \overline{x} = x + I \) is the residue class of \( x \) in \( C/I \). The quotient map \( C \to C/I \) is a coalgebra homomorphism.

2. Let \( I = \ker(f) \), and let \( \overline{f} : C/I \to D \) be the map induced by \( f \). Then \( I \) is a coideal of \( C \), and \( \overline{f} \) is an injective coalgebra homomorphism.

3. If \( J \subseteq D \) is a coideal, then \( f^{-1}(J) \subseteq C \) is a coideal.

Proof. (1) is clear from the definition, and (2) follows from Lemma 1.1.11, since \( \Delta(\ker(f)) \subseteq \ker(f \otimes f) \). (3) follows from (2) applied to the composition \( C \xrightarrow{f} D \to D/J \). \( \square \)

The next lemma demonstrates another setting in which coideals appear naturally.

Lemma 1.1.14. Let \( C \) be a coalgebra and let \( B \subseteq C \) be a subspace satisfying \( \Delta(B) \subseteq B \otimes C \) or \( \Delta(B) \subseteq C \otimes B \). Then \( B^+ = \ker(\varepsilon : B \to \mathbb{k}) \) is a coideal of \( C \), and \( B \neq B^+ \) if \( B \neq 0 \).

Proof. Assume that \( B \neq 0 \) and \( \Delta(B) \subseteq B \otimes C \). By the counit axiom there exists \( b \in B \) with \( \varepsilon(b) = 1 \). Hence \( B = \mathbb{k}b \oplus B^+ \). Let \( x \in B^+ \). Then
\[
\Delta(x) \in b \otimes y + B^+ \otimes C
\]
for some \( y \in C \), and \( y = x \) by applying \( \varepsilon \otimes \text{id}_C \) to the above formula. Thus \( \Delta(B^+) \subseteq C \otimes B^+ + B^+ \otimes C \). If \( \Delta(B) \subseteq C \otimes B \), then the claim is shown similarly. \( \square \)

Let \( V \) be a vector space, \( (A, \mu, \eta) \) an algebra, and \( \lambda : A \otimes V \to V \) a linear map. The pair \( (V, \lambda) \) is a left \( A \)-module if the following diagrams commute.

\[
\begin{array}{ccc}
A \otimes A \otimes V & \xrightarrow{\mu \otimes \text{id}_V} & A \otimes V \\
\downarrow \text{id}_A \otimes \lambda & & \downarrow \lambda \\
A \otimes V & \xrightarrow{\lambda} & V
\end{array}
\]

(1.1.17)
Let $V,W$ be left $A$-modules. An $A$-module homomorphism $f : V \to W$ is a linear map such that the following diagram commutes.

\[
\begin{array}{ccc}
A \otimes V & \overset{\text{id}_A \otimes f}{\longrightarrow} & A \otimes W \\
\downarrow^{\lambda_V} & & \downarrow^{\lambda_W} \\
V & \overset{f}{\longrightarrow} & W
\end{array}
\]

(1.1.18)

We denote the category of left $A$-modules with $A$-linear maps by $A\mathcal{M}$. The category of right $A$-modules, defined analogously, is denoted by $\mathcal{M}_A$.

We introduce comodules over a coalgebra by formally inverting the diagrams defining a module over an algebra.

**Definition 1.1.15.** Let $(C, \Delta, \varepsilon)$ be a coalgebra, $V$ a vector space, and let $\delta : V \to C \otimes V$ be a linear map. Then $(V, \delta)$ or simply $V$ is a left $C$-comodule if the following diagrams commute.

\[
\begin{array}{ccc}
V & \overset{\delta}{\longrightarrow} & C \otimes V \\
\downarrow^{\delta} & & \downarrow^{\Delta \otimes \text{id}_V} \\
C \otimes V & \overset{\text{id}_C \otimes \delta}{\longrightarrow} & C \otimes C \otimes V
\end{array}
\]  

(coassociativity)

\[
\begin{array}{ccc}
V & \overset{\delta}{\longrightarrow} & C \otimes V \\
\downarrow^{\delta} & & \downarrow^{\varepsilon \otimes \text{id}_V} \\
\mathbb{k} \otimes V & \overset{\varepsilon \otimes \text{id}_V}{\longrightarrow} & \mathbb{k} \otimes V
\end{array}
\]  

(counit)

If $(V, \delta_V)$ and $(W, \delta_W)$ are left $C$-comodules, and $f : V \to W$ is a linear map, then $f$ is a left $C$-comodule homomorphism or a left $C$-colinear map if the following diagram commutes.

\[
\begin{array}{ccc}
V & \overset{f}{\longrightarrow} & W \\
\downarrow^{\delta_V} & & \downarrow^{\delta_W} \\
C \otimes V & \overset{\text{id}_C \otimes f}{\longrightarrow} & C \otimes W
\end{array}
\]

(1.1.21)

Let $(V, \delta)$ be a left $C$-comodule. A subcomodule of $V$ is a subspace $U \subseteq V$ with $\delta(U) \subseteq C \otimes U$.

The category of left $C$-comodules with $C$-colinear maps as morphisms is denoted by $\mathcal{C}\mathcal{M}$. Right $C$-comodules and right $C$-colinear maps are defined similarly. Their category is denoted by $\mathcal{M}^C$.

We write $\text{Hom}^C(V, W)$ for the set of all left (or right) $C$-colinear maps between two left (or right) $C$-comodules $V, W$.

**Remark 1.1.16.** Comodules over a coalgebra $C$ form an abelian category like modules over an algebra. In particular, let $(V, \delta_V) \in \mathcal{C}\mathcal{M}$, and let $U \subseteq V$ be a subcomodule. Let $V/U$ be the quotient vector space, and let $\pi : V \to V/U$ be the quotient map. Then $(V/U, \delta_{V/U})$ is a left $C$-comodule, where the comodule
structure is uniquely defined by the commutative diagram

\[
\begin{array}{ccc}
V & \xrightarrow{\delta_V} & C \otimes V \\
\downarrow{\pi} & & \downarrow{\text{id} \otimes \pi} \\
V/U & \xrightarrow{\delta_{V/U}} & C \otimes V/U
\end{array}
\]

If \( V, W \in C\mathcal{M} \), and \( f : V \to W \) is left \( C \)-colinear, then \( \ker(f) \subseteq V \) and \( \text{im}(f) \subseteq W \) are subcomodules, and \( V/\ker(f) \xrightarrow{\cong} \text{im}(f), \overline{v} \mapsto f(v) \), is an isomorphism in \( C\mathcal{M} \).

Let \( \Gamma \) be a set. Comodules over \( k\Gamma \) are given by \( \Gamma \)-graded vector spaces. A \( \Gamma \)-\textbf{grading} of a vector space \( V \) is a family \( \mathcal{V} = (V(g))_{g \in \Gamma} \) of subspaces of \( V \) such that

\[ V = \bigoplus_{g \in \Gamma} V(g). \]

A \( \Gamma \)-\textbf{graded vector space} is a pair \((V, \mathcal{V})\), where \( V \) is a vector space with a grading (or a \textbf{gradation}) \( \mathcal{V} \). For a graded vector space \( V = (V, \mathcal{V}) \) we denote by \( \pi^V_g : V \to V(g), \ g \in \Gamma \), the canonical projection. An element \( v \in V \) is called \textbf{homogeneous of degree} \( g \in \Gamma \) if \( v \in V(g) \). We write \( \text{deg}(v) = g \), if \( v \in V(g) \).

We also use the notation \( V_g = V(g) \), in particular, when \( G \) is a monoid or a group.

Let \( \Gamma\text{-Gr} \mathcal{M}_k \) be the category of \( \Gamma \)-graded vector spaces, where a morphism \( f : (V, \mathcal{V}) \to (W, \mathcal{W}) \) is a \textbf{graded map} or a \textbf{homogeneous map} (of degree 0), that is a \( k \)-linear map with \( f(V(g)) \subseteq W(g) \) for all \( g \in \Gamma \).

**Proposition 1.1.17.** Let \( \Gamma \) be a set. The functor

\[ F : \Gamma\text{-Gr} \mathcal{M}_k \to k\Gamma \mathcal{M}, (V, (V(g))_{g \in \Gamma}) \mapsto \left( \bigoplus_{g \in \Gamma} V(g), \delta \right), \]

where \( \delta(v) = g \otimes v \) for all \( v \in V(g), \ g \in \Gamma \), and where morphisms \( f \) are mapped onto \( f \), is an isomorphism of categories. The inverse functor maps a comodule \((V, \delta)\) onto \( V \) with grading \( V(g) = V_g = \{ v \in V | \delta(v) = g \otimes v \} \) for all \( g \in \Gamma \).

**Proof.** Let \((V, \delta)\) be a left \( k\Gamma \)-comodule. We prove that \( V = \bigoplus_{g \in \Gamma} V_g \), where

\[ V_g = \{ v \in V | \delta(v) = g \otimes v \} \]

for all \( g \in \Gamma \).

For any \( v \in V \) there are elements \( v_g \in V, \ g \in \Gamma \), such that \( v_g \neq 0 \) only for finitely many \( g \in \Gamma \) and such that \( \delta(v) = \sum_{g \in \Gamma} g \otimes v_g \). By coassociativity,

\[ \sum_{g \in \Gamma} g \otimes \delta(v_g) = \sum_{g \in \Gamma} g \otimes g \otimes v_g. \]

Hence \( \delta(v_g) = g \otimes v_g \) for all \( g \in \Gamma \). Moreover, \( v = \sum_{g \in \Gamma} \varepsilon(g)v_g = \sum_{g \in \Gamma} v_g \). Hence \( V = \sum_{g \in \Gamma} V_g \). Let now \((v_g)_{g \in \Gamma}\) be a family of elements of \( V \), where \( v_g \in V(g) \) for all \( g \in \Gamma \) and \( v_g \neq 0 \) only for finitely many \( g \in \Gamma \). Assume that \( \sum_{g \in \Gamma} v_g = 0 \).

Applying \( \delta \) gives \( \sum_{g \in \Gamma} g \otimes v_g = 0 \), hence \( v_g = 0 \) for all \( g \in \Gamma \).

The isomorphism of categories now follows easily. \( \square \)

**Remark 1.1.18.** If \((V, \delta)\) is a right \( C \)-comodule, we define inductively

\[ \delta^n : V \to V \otimes C^\otimes n \text{ for all } n \geq 0 \]
by $\delta^0 = \text{id}_V$, $\delta^1 = \delta_V$, and $\delta^n = (\delta \otimes \text{id}_{C \otimes (n-1)})\delta^{n-1}$ for all $n \geq 2$. Extending the Sweedler notation to comodules we write

$$
\begin{align*}
\delta(v) &= v(0) \otimes v(1), \\
\delta^2(v) &= v(0) \otimes \Delta(v(1)) = v(0) \otimes v(1) \otimes v(2), \ldots \\
\delta^n(v) &= v(0) \otimes v(1) \otimes \cdots \otimes v(n)
\end{align*}
$$

for all $v \in V$. For left $C$-comodules $(V, \delta)$ we use negative indices.

$$
\begin{align*}
\delta(v) &= v(-1) \otimes v(0), \\
\delta^2(v) &= \Delta(v(-1)) \otimes v(0) = v(-2) \otimes v(-1) \otimes v(0), \ldots \\
\delta^n(v) &= v(-n) \otimes \cdots \otimes v(-1) \otimes v(0)
\end{align*}
$$

for all $v \in V$.

### 1.2. Bialgebras and Hopf algebras

We continue with the introduction of bialgebras, Hopf algebras, quotients of them, and their graded versions.

**Definition 1.2.1.** Let $H$ be a vector space, and let

$$
\begin{align*}
\mu : H \otimes H &\rightarrow H, \quad \eta : \mathbb{k} \rightarrow H, \\
\Delta : H &\rightarrow H \otimes H, \quad \varepsilon : H \rightarrow \mathbb{k}
\end{align*}
$$

be linear maps. Then $(H, \mu, \eta, \Delta, \varepsilon)$ is a **bialgebra** if $(H, \mu, \eta)$ is an algebra, $(H, \Delta, \varepsilon)$ is a coalgebra, and $\Delta$ and $\varepsilon$ are algebra maps.

Let $H, H'$ be bialgebras. A **bialgebra homomorphism** $\varphi : H \rightarrow H'$ is an algebra and a coalgebra homomorphism. A **subbialgebra** of a bialgebra is a subalgebra and a subcoalgebra.

**Proposition 1.2.2.** Let $H$ be a vector space, and let

$$
\begin{align*}
\mu : H \otimes H &\rightarrow H, \quad \eta : \mathbb{k} \rightarrow H, \\
\Delta : H &\rightarrow H \otimes H, \quad \varepsilon : H \rightarrow \mathbb{k}
\end{align*}
$$

be linear maps. Assume that $(H, \mu, \eta)$ is an algebra and $(H, \Delta, \varepsilon)$ is a coalgebra. Then the following are equivalent.

1. $\Delta$ and $\varepsilon$ are algebra maps.
2. $\mu$ and $\eta$ are coalgebra maps.

**Proof.** By definition, (1) is equivalent to the commutativity of the diagrams (1.1.5) and (1.1.6) for $\Delta$ and $\varepsilon$, and (2) is equivalent to the commutativity of the diagrams (1.1.10) and (1.1.11) for $\mu$ and $\eta$.

Let $\tau = \tau_{H,H} : H \otimes H \rightarrow H \otimes H$ be the flip map. Then

$$
\mu_{H \otimes H}(\Delta \otimes \Delta) = (\mu \otimes \mu)(\text{id} \otimes \tau \otimes \text{id})(\Delta \otimes \Delta) = (\mu \otimes \mu)\Delta_{H \otimes H}.
$$

Hence (1.1.5) for $\Delta$ and (1.1.10) for $\mu$ coincide. Obviously, the diagrams (1.1.6) for $\Delta$ and (1.1.10) for $\eta$, (1.1.5) for $\varepsilon$ and (1.1.11) for $\mu$, as well as (1.1.6) for $\varepsilon$ and (1.1.11) for $\eta$ coincide. \qed

**Example 1.2.3.** Let $G$ be a monoid, that is a set $G$ together with an associative map $G \times G \rightarrow G$ and a unit element $e$. The **monoid algebra** $\mathbb{k}G$ (or **group algebra**, if $G$ is a group) is the vector space with basis $G$. Its algebra structure $\mu : \mathbb{k}G \otimes \mathbb{k}G \rightarrow \mathbb{k}G$, $\eta : \mathbb{k} \rightarrow \mathbb{k}G$, is given by $\mu(g, h) = gh$ (the product of $g$ and $h$ in $G$) for all $g, h \in G$ and by $\eta(1) = e$. Then $\mathbb{k}G$ is a bialgebra where the elements of $G$ are group-like. The bialgebra axioms are trivially verified on the basis.
1.2. BIALGEBRAS AND HOPF ALGEBRAS

Definition 1.2.4. Let $H$ be a bialgebra.

(1) Let $V,W \in _H \mathcal{M}$. The map

$$H \otimes V \otimes W \to V \otimes W, \quad h \otimes v \otimes w \mapsto h_{(1)} v \otimes h_{(2)} w,$$

is called the diagonal action of $H$ on $V \otimes W$. The trivial action of $H$ on $k$ is defined by $H \otimes k \to k, \quad h \otimes 1 \mapsto \varepsilon(h)$.

(2) Let $V,W \in _H \mathcal{M}$. The map

$$V \otimes W \to H \otimes V \otimes W, \quad v \otimes w \mapsto v_{(-1)} w_{(-1)} \otimes v_{(0)} \otimes w_{(0)},$$

is called the diagonal coaction of $H$ on $V \otimes W$. The trivial coaction of $H$ on $k$ is defined by $k \to H \otimes k, \quad 1 \mapsto \eta(1) \otimes 1$.

For modules over $kG, G$ a monoid, the diagonal action is given by the familiar formulas from representation theory of groups:

$$g(v \otimes w) = gv \otimes gw, \quad g\alpha = \alpha,$$

for all $v \in V, w \in W, \alpha \in k$.

It is a fundamental consequence of the axioms of a bialgebra that modules and comodules over a bialgebra can be multiplied in the sense of the following proposition.

Proposition 1.2.5. Let $H$ be a bialgebra. The tensor product of two left $H$-(co)modules is a left $H$-(co)module with diagonal (co)action. Moreover, for all $U,V,W \in _H \mathcal{M}$ (for all $U,V,W \in _H \mathcal{M}$, respectively) the canonical isomorphisms

$$(U \otimes V) \otimes W \to U \otimes (V \otimes W), \quad k \otimes V \to V, \quad V \otimes k \to V,$$

are left $H$-(co)linear.

Proof. This is easily checked using the Sweedler notation. \qed

Of course, the same result holds for right modules and right comodules where the diagonal action and coaction is defined in a similar way.

The next remark shows that in fact the last proposition gives a natural explanation of the axioms of a bialgebra.

Remark 1.2.6. Let $H$ be an algebra together with algebra maps

$$\Delta : H \to H \otimes H, \quad \varepsilon : H \to k.$$ 

We will again write $\Delta(h) = h_{(1)} \otimes h_{(2)}$ for all $h \in H$.

The trivial one-dimensional left $H$-module is the vector space $k$ with $H$-action $h1_k = \varepsilon(h)$ for all $h \in H$.

Let $V,W$ be left $H$-modules. Then $V \otimes W$ is a left $H \otimes H$-module by

$$(x \otimes y)(v \otimes w) = xv \otimes yw$$

for all $x,y \in H, v \in V, w \in W$. Hence $V \otimes W$ is a left $H$-module induced by the algebra map $\Delta$. Thus

$$h(v \otimes w) = h_{(1)} v \otimes h_{(2)} w$$

for all $h \in H, v \in V, w \in W$.

The coalgebra axioms in the definition of a bialgebra can now be explained in a very natural way.
(1) The map $\Delta$ satisfies (1.1.7) if and only if for all left $H$-modules $U,V,W$ the canonical isomorphism
\[(U \otimes V) \otimes W \to U \otimes (V \otimes W)\]
is left $H$-linear.

(2) The map $\varepsilon$ satisfies (1.1.8) if and only if for all left $H$-modules $V$ the canonical isomorphisms $V \otimes k \to V$ and $k \otimes V \to V$ are left $H$-linear.

**Definition 1.2.7.** Let $\Gamma$ be a monoid and let $V, W$ be $\Gamma$-graded vector spaces. Then $V \otimes W$ is a $\Gamma$-graded vector space by
\[(V \otimes W)(g) = \bigoplus_{(a,b) \in \Gamma^2 \mid ab = g} V(a) \otimes W(b), \quad \text{for all } g \in \Gamma.\]
This grading on $V \otimes W$ is called the **diagonal $\Gamma$-grading**. The **trivial grading** on a vector space $V$ is defined by $V(e) = k$, $e$ the unit element of $\Gamma$, that is, $V(g) = 0$ for all $e \neq g \in \Gamma$.

**Remark 1.2.8.** Let $\Gamma$ be a monoid.
(1) For all $\Gamma$-graded vector spaces $U, V, W$ the canonical isomorphisms
\[(U \otimes V) \otimes W \to U \otimes (V \otimes W), \quad k \otimes V \to V, \quad V \otimes k \to V,\]
are $\Gamma$-graded. The flip maps $\tau_{V,W} : V \otimes W \to W \otimes V$ are only graded for all $V, W$ if $\Gamma$ is commutative.

(2) The category isomorphism $F : \Gamma\-Gr \mathcal{M}_k \to k^\Gamma \mathcal{M}$ of Proposition 1.1.17 preserves the trivial objects and the tensor product with diagonal structure, that is, $F(k) = k$, and for all $\Gamma$-graded vector spaces $V, W$,
\[F(V \otimes W) = F(V) \otimes F(W) \text{ in } k^\Gamma \mathcal{M}.\]
The following algebra structure on $\text{Hom}(C, A)$ for a coalgebra $C$ and an algebra $A$ will be an important tool to study the existence of the antipode of a bialgebra.

**Definition 1.2.9.** Let $C$ be a coalgebra, $A$ an algebra, and $f, g \in \text{Hom}(C, A)$ linear maps. The **convolution** $f * g \in \text{Hom}(C, A)$ of $f$ and $g$ is defined by
\[(f * g)(c) = f(c_{(1)})g(c_{(2)})\]
for all $c \in C$, that is by the composition
\[f * g = \left( C \xrightarrow{\Delta} C \otimes C \xrightarrow{f \otimes g} A \otimes A \xrightarrow{\mu} A \right).\]

The coassociativity of the comultiplication $\Delta$ of $C$ and the associativity of the multiplication map $\mu$ of $A$ imply that the convolution product of $\text{Hom}(C, A)$ is associative. Thus $\text{Hom}(C, A)$ is an algebra with unit element $\eta \varepsilon$.

In the next proposition we will identify $\text{Hom}(C, A)$ with an algebra of endomorphisms. This will give very useful information about the structure of the inverse of an element in $\text{Hom}(C, A)$. We define
\[\text{End}_C^A(A \otimes C) = \{ f : A \otimes C \to A \otimes C \mid f \text{ left } A\text{-linear and right } C\text{-colinear} \},\]
where $A \otimes C$ is a left $A$-module by $\mu \otimes id_C$, and a right $C$-comodule by $id_A \otimes \Delta$. Then $\text{End}_A^C(A \otimes C)$ becomes an algebra with composition of maps as multiplication.
Lemma 1.2.10. Let $C$ be a coalgebra, and $X$ a vector space. For any right $C$-comodule $V$, the map

$$\Hom^C(V, X \otimes C) \xrightarrow{\sim} \Hom(V, X), \quad f \mapsto (\id \otimes \varepsilon)f,$$

is bijective with inverse given by $\varphi \mapsto (\varphi \otimes \id)V$. Here, $X \otimes C$ is a right $C$-comodule with comodule structure $\id_X \otimes \Delta$.

Proof. Let $f \in \Hom^C(V, X \otimes C)$. Then $f(v_{(0)}) \otimes v_{(1)} = (\id_X \otimes \Delta)f(v)$ for all $v \in V$, since $f$ is $C$-colinear. By applying $\id \otimes \varepsilon \otimes \id$ to this equation we obtain $\varphi(v_{(0)}) \otimes v_{(1)} = f(v)$, where $\varphi = (\id \otimes \varepsilon)f$. Conversely, let $\varphi \in \Hom(V, X)$ and define $f = (\varphi \otimes \id)V$. Then $f \in \Hom^C(V, X \otimes C)$ by coassociativity of $\delta_V$. Moreover, $((\id \otimes \varepsilon)f)(v) = \varphi(v_{(0)})\varepsilon(v_{(1)}) = \varphi(v)$ for all $v \in V$. \qed

Lemma 1.2.10 implies that the functor $\mathcal{M}_k \to \mathcal{M}^C$, $X \mapsto X \otimes C$, is right adjoint to the forgetful functor $\mathcal{M}^C \to \mathcal{M}_k$.

Proposition 1.2.11. Let $C$ be a coalgebra and $A$ an algebra.

(1) The map $\Phi : \Hom(C, A) \xrightarrow{\sim} \End_A^C(A \otimes C)$ given by

$$f \mapsto (A \otimes C \xrightarrow{\id \otimes \Delta} A \otimes C \otimes C \xrightarrow{\id \otimes f \otimes \id} A \otimes A \otimes C \xrightarrow{\mu \otimes \id} A \otimes C)$$

is an algebra anti-isomorphism, where $\Hom(C, A)$ is an algebra with convolution as multiplication.

(2) Let $f \in \Hom(C, A)$. Then $f$ is invertible if and only if $\Phi(f)$ is an isomorphism. If $\Phi(f)$ is an isomorphism with inverse map $\Phi(f)^{-1}$, then

$$f^{-1} = (C = k \otimes C \xrightarrow{\eta \otimes \id_C} A \otimes C \xrightarrow{\Phi(f)^{-1}} A \otimes C \xrightarrow{\id \otimes \varepsilon} A)$$

is the inverse of $f$ in $\Hom(C, A)$.

Proof. (1) Let $V = A \otimes C$ and $X = A$ in Lemma 1.2.10. Since the comodule structure $\delta_V = \id \otimes \Delta$ of $V$ is left $A$-linear, the isomorphism in Lemma 1.2.10 restricts to an isomorphism $\Phi_1 : \Hom_A^C(A \otimes C, A \otimes C) \to \Hom_A(A \otimes C, A)$. Let

$$\Phi : \Hom(C, A) \xrightarrow{\sim} \Hom_A(A \otimes C, A) \xrightarrow{\Phi_1^{-1}} \Hom_A^C(A \otimes C, A \otimes C)$$

be the composition of $\Phi_1^{-1}$ with the isomorphism

$$\Hom(C, A) \xrightarrow{\sim} \Hom_A(A \otimes C, A), \quad f \mapsto (a \otimes c \mapsto af(c)).$$

Then

$$\Phi(f)(a \otimes c) = af(c_{(1)}) \otimes c_{(2)} \quad \text{for all } f \in \Hom(C, A), \quad a \in A, \quad c \in C.$$\nto.

Hence for all $f, f' \in \Hom(C, A)$ and $a \in A, \ c \in C$,

$$(\Phi(f)\Phi(f'))(a \otimes c) = \Phi(f)(af'(c_{(1)}) \otimes c_{(2)})$$

$$= af'(c_{(1)})f(c_{(2)}) \otimes c_{(3)} = \Phi(f' \ast f)(a \otimes c).$$

The inverse of $\Phi$ is given by

$$\Phi^{-1} : \End_A^C(A \otimes C) \to \Hom(C, A), \quad F \mapsto (\id \otimes \varepsilon)F(\eta_A \otimes \id_C).$$

(2) follows from (1). \qed

Let $C$ be a coalgebra. The algebra $C^* = \Hom(C, k)$ in Definition 1.2.9 with $A = k$ is called the dual algebra of $C$. It is easy to see that for any coalgebra map $\varphi : C \to D$ the map $\varphi^* : D^* \to C^*, \ f \mapsto f \circ \varphi$, is an algebra homomorphism.
Example 1.2.12. Let $G = \{g_1, \ldots, g_n\}$ be a finite set of $n$ elements. The vector space $kG$ with basis $G$ is a coalgebra with $\Delta(g) = g \otimes g$, $\varepsilon(g) = 1$ for all $g \in G$. Let $(e_i)_{1 \leq i \leq n}$ be the dual basis of $(g_i)_{1 \leq i \leq n}$. Then $e_i e_j = \delta_{ij} e_i$ for all $i, j$, and $\sum_{i=1}^{n} e_i = 1$. Hence $C^* \cong k^n$ as algebras.

Example 1.2.13. Let $C = M_n(k)^*$ be the coalgebra in Example 1.1.5. For all $i, j \in \{1, \ldots, n\}$ consider $E_{ij} \in M_n(k)$ as an element in $C^*$ via the natural isomorphism $M_n(k)^* \cong M_n(k)$, that is, $E_{ij}(u_{kl}) = \delta_{ik}\delta_{jl}$ for all $i, j, k, l \in \{1, \ldots, n\}$. Then

$$(E_{ij} * E_{kl})(u_{rs}) = \sum_{m=1}^{n} E_{ij}(u_{rm})E_{kl}(u_{ms}) = \delta_{ir}\delta_{js} = \delta_{jk}E_{il}(u_{rs})$$

for all $i, j, k, l, r, s \in \{1, 2, \ldots, n\}$. Hence the natural isomorphism

$$C^* \rightarrow M_n(k)$$

is an algebra isomorphism, where the multiplication in $C^*$ is the convolution product.

Definition 1.2.14. A Hopf algebra $H$ is a bialgebra such that $\text{id}_H$ is invertible in the convolution algebra $\text{Hom}(H, H)$. The inverse $S$ (or $S_H$) of $\text{id}_H$ is called the antipode of $H$. A Hopf algebra homomorphism between two Hopf algebras is a bialgebra homomorphism. A Hopf subalgebra of a Hopf algebra $H$ is a subbialgebra $H' \subseteq H$ such that $S(H') \subseteq H'$.

Remark 1.2.15. Let $H$ be a bialgebra. Then $H$ is a Hopf algebra (with antipode $S$) if there is a linear map $S : H \rightarrow H$ such that

$$(1.2.1) \quad h_{(1)}S(h_{(2)}) = \varepsilon(h)1 = S(h_{(1)})h_{(2)} \quad \text{(antipode)}$$

for all $h \in H$, or equivalently such that the following diagrams commute.

$$(1.2.2) \quad \begin{array}{ccc}
H & \xrightarrow{\Delta} & H \otimes H \\
\downarrow{\eta} & & \downarrow{\eta} \\
H & \xleftarrow{\mu} & H \otimes H
\end{array} \quad \text{and} \quad \begin{array}{ccc}
H & \xrightarrow{\Delta} & H \otimes H \\
\downarrow{\delta} & & \downarrow{\delta} \\
H & \xleftarrow{\mu} & H \otimes H
\end{array} \quad \text{and} \quad \begin{array}{ccc}
H & \xrightarrow{\Delta} & H \otimes H \\
\downarrow{\eta} & & \downarrow{\eta} \\
H & \xleftarrow{\mu} & H \otimes H
\end{array}$$

By uniqueness of inverses, each bialgebra has at most one antipode.

Example 1.2.16. Let $G$ be a group. Then the bialgebra $kG$ of the monoid $G$ in Example 1.2.3 is a Hopf algebra with antipode defined by $S(g) = g^{-1}$ for all $g \in G$.

Proposition 1.2.17. Let $H$ be a Hopf algebra with antipode $S$.

1. The antipode $S$ is an algebra anti-homomorphism and a coalgebra anti-homomorphism, that is, for all $x, y \in H$

(a) $S(xy) = S(y)S(x)$, $S(1) = 1$, 
(b) $\Delta(S(x)) = S(x_{(2)}) \otimes S(x_{(1)})$, $\varepsilon(S(x)) = \varepsilon(x)$.

2. Let $H'$ be a Hopf algebra, and let $\varphi : H \rightarrow H'$ be a bialgebra map. Then $S_{H'} \varphi = \varphi S_H$.

Proof. (1) (a) Define $F, G \in \text{Hom}(H \otimes H, H)$ by

$$F(x \otimes y) = S(xy), \quad G(x \otimes y) = S(y)S(x)$$

for all $x, y \in H$. Then

$$F(x \otimes y) = S(xy), \quad G(x \otimes y) = S(y)S(x)$$

for all $x, y \in H$. Then
for all \( x, y \in H \). Then both \( F \) and \( G \) are convolution inverses of \( \mu_H \). Indeed, 
\[
\mu_H * F = \eta \varepsilon \quad \text{and} \quad \mu_H * G = \eta \varepsilon
\]
since
\[
x_{(1)}y_{(1)}S(x_{(2)}y_{(2)}) = \varepsilon(x)\varepsilon(y), \quad x_{(1)}y_{(1)}S(y_{(2)})S(x_{(2)}) = \varepsilon(x)\varepsilon(y)
\]
for all \( x, y \in H \). Similarly, \( F * \mu_H = G * \mu_H = \eta \varepsilon \). Hence \( F = G \). Further, \( S(1) = 1 \) since \( 1 S(1) = \varepsilon(1)1 \).

(b) Define \( F, G \in \text{Hom}(H, H \otimes H) \) by
\[
F(x) = \Delta(S(x)), \quad G(x) = S(x_{(2)}) \otimes S(x_{(1)})
\]
for all \( x \in H \). Then both \( F \) and \( G \) are convolution inverses of \( \Delta_H \). Indeed, 
\[
\Delta \ast F = (\eta \otimes \eta)\varepsilon \quad \text{and} \quad \Delta \ast G = (\eta \otimes \eta)\varepsilon
\]
since \( 1 \Delta = \varepsilon \) for all elements \( x, y \in H \). Similarly, \( F \ast \Delta = G \ast \Delta = (\eta \otimes \eta)\varepsilon \). Hence \( F = G \). Further, \( \varepsilon \circ S = \varepsilon \), since both are convolution inverses of \( \varepsilon \).

(2) Both \( S_{H'} \circ \varphi \) and \( \varphi S_H \) are convolution inverses of \( \varphi \in \text{Hom}(H, H') \). \( \square \)

**Remark 1.2.18.** Let \( H \) be a bialgebra, and \( \mathcal{S} : H \to H \) an algebra anti-homomorphism. For any left \( H \)-module \( V \), the dual space \( V^* = \text{Hom}(V, \kappa) \) is a right \( H \)-module in the natural way by \( (fh)(v) = f(hv) \) for all \( h \in H \), \( f \in V^* \), \( v \in V \). Since \( \mathcal{S} \) is an algebra anti-homomorphism, \( V^* \) becomes a left \( H \)-module by
\[
(hf)(v) = f(S(h)v)
\]
for all \( h \in H \), \( f \in V^* \), \( v \in V \). If \( V \) is a right \( H \)-module, then the dual vector space \( V^* \) is a right \( H \)-module by
\[
(fh)(v) = f(vS(h))
\]
for all \( h \in H \), \( f \in V^* \), \( v \in V \).

The map \( \mathcal{S} \) satisfies (1.2.1) if and only if for all left \( H \)-modules \( V \) and all right \( H \)-modules \( W \) the evaluation maps
\[
V^* \otimes V \to \kappa, \quad p \otimes v \mapsto p(v), \quad W \otimes W^* \to \kappa, \quad w \otimes q \mapsto q(w),
\]
are left \( H \)-linear and right \( H \)-linear, respectively.

Bialgebras are generalizations of monoids and Hopf algebras are generalizations of groups. Proposition 1.2.17(1) says that \( (gh)^{-1} = h^{-1}g^{-1} \) for all elements \( g, h \) of a group. By Proposition 1.2.17(2), a monoid homomorphism between groups preserves inverses.

However, the rule \( (g^{-1})^{-1} = g \) does not generalize to Hopf algebras. In general, the antipode \( S \) of a Hopf algebra does not satisfy \( S^2 = \text{id} \). There are (rather pathological) Hopf algebras whose antipode is not bijective. If the antipode is bijective, then its order as a vector space automorphism could be infinite.

A monoid \( M \) is a group if and only if the canonical map
\[
M \times M \to M \times M, \quad (x, y) \mapsto (xy, y),
\]
is bijective. We note the corresponding characterization for Hopf algebras.
Proposition 1.2.19. Let $H$ be a bialgebra. We denote the “Galois map” by

$$G = (H \otimes H \xrightarrow{\text{id} \otimes \Delta} H \otimes H \otimes H \xrightarrow{\mu \otimes \text{id}} H \otimes H).$$

(1) The following are equivalent.
(a) $H$ is a Hopf algebra.
(b) $G : H \otimes H \to H \otimes H$ is an isomorphism.
(2) If $G$ is an isomorphism with inverse $G^{-1}$, then

$$S = (H \xrightarrow{\eta \otimes \text{id}} H \otimes H \xrightarrow{G^{-1}} H \otimes H \xrightarrow{\text{id} \otimes \varepsilon} H)$$

is the antipode of $H$.

Proof. Note that $G \in \text{End}_H^H(H \otimes H)$. The isomorphism

$$\Phi : \text{Hom}(H, H) \cong \text{End}_H^H(H \otimes H)$$

of Proposition 1.2.11 maps the identity onto $G$. Hence the claim follows from Proposition 1.2.11(2). \qed

By slight altering of the multiplication or comultiplication one can get new bialgebras and Hopf algebras. We will discuss this phenomenon in a more general setting in Proposition 3.2.15.

Definition 1.2.20. Let $H$ be a bialgebra. Then $H^\text{op}$ with comultiplication $\Delta_H$ and counit $\varepsilon_H$ is called the **opposite bialgebra**. Similarly, $H^\text{cop}$ with multiplication $\mu_H$ and unit $\eta_H$ is called the **coproposite bialgebra**.

It is easy to check that for any bialgebra $H$, $H^\text{op}$ and $H^\text{cop}$ are again bialgebras. Moreover, if $H$ is a Hopf algebra then $H^\text{op}$ and $H^\text{cop}$ are Hopf algebras if and only if $S$ is bijective. In this case, $S^{-1}$ is the antipode of $H^\text{op}$ and of $H^\text{cop}$.

To define quotients of bialgebras and Hopf algebras we introduce the subobjects which are the kernels of the corresponding quotient maps.

An **ideal** or **two-sided ideal** $I$ in an algebra $A$ is a linear subspace $I \subseteq A$ such that $ax \in I$ and $xa \in I$ for all $x \in I$ and $a \in A$.

Definition 1.2.21. Let $H$ be a bialgebra. A subspace $I \subseteq H$ is a **bi-ideal** of $H$ if $I \subseteq H$ is an ideal and a coideal.

Let $H$ be a Hopf algebra. A **Hopf ideal** of $H$ is a bi-ideal $I$ of $H$ with $S(I) \subseteq I$.

Proposition 1.2.22. Let $H$ and $H'$ be bialgebras, $I \subseteq H$ a bi-ideal, and let $\varphi : H \to H'$ a morphism of bialgebras.

(1) The quotient coalgebra and quotient algebra $\overline{H} = H/I$ is a bialgebra. If $H$ is a Hopf algebra, and $I \subseteq H$ is a Hopf ideal, then $\overline{H}$ is a Hopf algebra with antipode $S_{\overline{H}}(\overline{x}) = S_H(x)$ for all $x \in H$.

(2) $\ker(\varphi) \subseteq H$ is a bi-ideal, and the natural map $\overline{\varphi} : H/\ker(\varphi) \to H'$ is an injective bialgebra homomorphism. If $H$ and $H'$ are Hopf algebras, then $\ker(\varphi)$ is a Hopf ideal of $H$.

Proof. (1) follows directly from the definitions, and (2) follows from Proposition 1.1.13 and 1.2.17(2). \qed

It can be quite difficult or impossible to verify the axioms of a Hopf algebra on a vector space basis, since usually there is no easy formula for the comultiplication on all elements of a basis.
However, it is sufficient to check the axioms on algebra generators. We say that a subset \( M \) of an algebra \( A \) is a set of algebra generators, or that \( M \) generates \( A \) as an algebra, if any element of \( A \) is a \( k \)-linear combination of products of elements of \( M \). We write \( A = k[M] \) if \( M \) is a set of algebra generators.

**Proposition 1.2.23.** Let \( H \) be an algebra and \( M \subseteq H \) a set of algebra generators. Let

\[
\Delta : H \to H \otimes H, \quad \varepsilon : H \to k, \quad S : H \to H^{\text{op}}
\]

be algebra maps. Assume that the diagrams (1.1.7), (1.1.8) and (1.2.2) commute for all \( h \in M \). Then \((H, \Delta, \varepsilon, S)\) is a Hopf algebra.

**Proof.** In the diagrams in (1.1.7) and (1.1.8) for \((H, \Delta, \varepsilon)\) all maps are algebra maps. Hence the diagrams commute, since they commute when applied to elements of \( M \).

But the maps in the diagrams in (1.2.2) are in general not algebra maps. Let \( H' \) be the subset of all elements of \( H \) on which the first diagram in (1.2.2) commutes. Thus \( H' = \{ h \in H \mid S(h(1))h(2) = \varepsilon(h)1 \} \) is a subspace of \( H \) containing the unit element 1 of \( H \). Let \( x, y \in H' \). Then \( xy \in H' \), since

\[
S((xy)_1)(xy)_2 = S(x_1y_1)x_2y_2 \quad \text{(\( \Delta \) is an algebra map)}
\]

\[
= S(y_1)x_1S(x_1)x_2y_2 \quad \text{(since } x \in H')
\]

\[
= S(y_1)\varepsilon(x)y_2 \quad \text{(since } y \in H')
\]

\[
= \varepsilon(x)\varepsilon(y) \quad \text{(}\varepsilon\text{ is an algebra map)}
\]

where the second equality holds since \( S \) is an algebra anti-homomorphism.

Hence \( H' \) is a subalgebra of \( H \). This shows that \( H' = H \), since \( M \subseteq H' \). In the same way it follows that the second diagram in (1.2.2) commutes. \( \square \)

For the next example we need the notion of shuffle permutations. We will study them in more detail in Section 1.8.

Let \( n \) be a natural number, and \( i \in \{0,1,\ldots,n\} \). A permutation \( w \in \mathcal{S}_n \) is called an \((i, n-i)\)-shuffle or simply an \( i \)-shuffle if

\[
w(1) < \cdots < w(i), \text{ and } w(i+1) < \cdots < w(n).
\]

Note that any \((0,n)\)- or \((n,0)\)-shuffle is the identity.

**Example 1.2.24.** Let \( X \) be a set which we view as an alphabet. Let \( k\langle X \rangle \) be the free algebra in the alphabet \( X \). If \( X = \{a_1, \ldots, a_m\} \) is a finite set of \( m \) elements, we write \( k\langle X \rangle = k\langle a_1, \ldots, a_m \rangle \).

The formal words

\[
x_1 \cdots x_n, \text{ where } x_1, \ldots, x_n \in X, \text{ } n \in \mathbb{N}_0,
\]

form a basis of the vector space \( k\langle X \rangle \), and the multiplication is defined by concatenation of words. By definition, the length of the word \( x_1 \cdots x_n \) is \( n \), where \( x_1, \ldots, x_n \in X, n \in \mathbb{N}_0 \). The empty word is the unit element.

The free algebra has the following universal property: Let \( A \) be an algebra and \( (a_x)_{x \in X} \) a family of elements \( a_x \in A \). Then there is exactly one algebra map \( \varphi : k\langle X \rangle \to A \) such that \( \varphi(x) = a_x \) for all \( x \in X \).
Using the universal property, we define algebra maps
\[ \Delta : \mathbb{k}\langle X \rangle \to \mathbb{k}\langle X \rangle \otimes \mathbb{k}\langle X \rangle, \quad \varepsilon : \mathbb{k}\langle X \rangle \to \mathbb{k}, \quad S : \mathbb{k}\langle X \rangle \to \mathbb{k}\langle X \rangle^\text{op} \]
with
\[ \Delta(x) = 1 \otimes x + x \otimes 1, \quad \varepsilon(x) = 0, \quad S(x) = -x \]
for all \( x \in X \). It follows from Proposition 1.2.23 that \((\mathbb{k}\langle X \rangle, \Delta, \varepsilon, S)\) is a Hopf algebra. Explicitly, one obtains for all \( x_1, \ldots, x_n \in X, n \geq 1 \),
\[ \Delta(x_1 \cdots x_n) = (1 \otimes x_1 + x_1 \otimes 1) \cdots (1 \otimes x_n + x_n \otimes 1) \]
\[ = \sum_{i=0}^{n} \sum_{w \text{-shuffle}} x_{w(1)} \cdots x_{w(i)} \otimes x_{w(i+1)} \cdots x_{w(n)}. \]
This formula follows easily since the elements \( 1 \otimes x_i \) and \( x_j \otimes 1 \) commute for all \( i, j \).

**Example 1.2.25.** Let \( V \) be a vector space. For all natural numbers \( n \geq 0 \) let \( V^\otimes n = \underbrace{V \otimes \cdots \otimes V}_n \), where \( V^\otimes 0 = \mathbb{k} \). The tensor algebra of \( V \) is the vector space \( T(V) = \bigoplus_{n \geq 0} V^\otimes n \) with multiplication given by
\[ V^\otimes m \otimes V^\otimes n \to V^\otimes (m+n), \quad x \otimes y \mapsto x \otimes y, \]
for all \( m, n \geq 0 \). We also write \( T^n(V) \) for \( V^\otimes n \) for all \( n \geq 0 \). Up to an isomorphism depending on the choice of a basis \( (x_i)_{i \in I} \) of \( V \), the tensor algebra is the free algebra in \( X = \{ x_i \mid i \in I \} \). The algebra map
\[ \mathbb{k}\langle X \rangle \to T(V), \quad x_i \mapsto x_i, \quad i \in I, \]
is an isomorphism.

As in Example 1.2.24, \( T(V) \) is a Hopf algebra with
\[ \Delta(v) = 1 \otimes v + v \otimes 1, \quad \varepsilon(v) = 0, \quad S(v) = -v \]
for all \( v \in V \).

We end this section with some general definitions.

**Definition 1.2.26.**

1. An \( \mathbb{N}_0 \)-graded coalgebra is a pair \((C, C)\), where \( C \) is a coalgebra, \((C, C)\) is an \( \mathbb{N}_0 \)-graded vector space, and
\[ \Delta(C(n)) \subseteq \bigoplus_{r+s=n} C(r) \otimes C(s) \quad \text{for all } n \geq 0, \]
(1.2.3)
\[ \varepsilon(C(n)) = 0 \quad \text{for all } n > 0. \]
(1.2.4)

We write
\[ \Delta_{m,n} : C(m + n) \subseteq C \xrightarrow{\Delta} C \otimes C \xrightarrow{\pi_m^C \otimes \pi_n^C} C(m) \otimes C(n), \quad m, n \in \mathbb{N}_0, \]
for the components of the comultiplication \( \Delta \).

2. An \( \mathbb{N}_0 \)-graded algebra is a pair \((A, A)\), where \( A \) is an algebra, \((A, A)\) is an \( \mathbb{N}_0 \)-graded vector space, and
\[ A(m)A(n) \subseteq A(m + n) \quad \text{for all } m, n \geq 0, \]
(1.2.5)
\[ 1_A \in A(0). \]
(1.2.6)
The components of the multiplication are
\[ \mu_{m,n} : A(m) \otimes A(n) \rightarrow A(m + n), \ x \otimes y \mapsto xy, \ m, n \geq 0. \]

(3) An \( \mathbb{N}_0 \)-graded bialgebra \( H \) is a bialgebra and an \( \mathbb{N}_0 \)-graded vector space \( (H, \mathcal{H}) \) such that \( H \) is an \( \mathbb{N}_0 \)-graded algebra and an \( \mathbb{N}_0 \)-graded coalgebra with respect to \( \mathcal{H} \). An \( \mathbb{N}_0 \)-graded Hopf algebra is an \( \mathbb{N}_0 \)-graded bialgebra which is a Hopf algebra.

**Corollary 1.2.27.** Let \( C \) be an \( \mathbb{N}_0 \)-graded coalgebra, and \( A \) an \( \mathbb{N}_0 \)-graded algebra. If \( f \in \text{Hom}(C, A) \) is an invertible graded map, then its inverse \( f^{-1} \) is graded.

**Proof.** By Proposition 1.2.11, \( \Phi(f) \) and \( f^{-1} \) are graded. \( \Box \)

By Corollary 1.2.27, the antipode of an \( \mathbb{N}_0 \)-graded Hopf algebra is graded.

We note that in Example 1.2.25, \( T(V) \) is an \( \mathbb{N}_0 \)-graded Hopf algebra with grading \( (T^n(V))_{n \geq 0} \).

### 1.3. Strictly graded coalgebras

**Definition 1.3.1.** An \( \mathbb{N}_0 \)-filtered coalgebra is a pair \((C, \mathcal{F}(C))\), where \( C \) is a coalgebra and \( \mathcal{F}(C) = (F_n(C))_{n \geq 0} \) is a family of subspaces \( F_n(C) \subseteq C, \ n \geq 0, \) such that

\begin{align*}
(1.3.1) \quad & F_m(C) \subseteq F_n(C) \text{ for all } 0 \leq m \leq n, \\
(1.3.2) \quad & C = \bigcup_{n \geq 0} F_n(C), \\
(1.3.3) \quad & \Delta(F_n(C)) \subseteq \sum_{r+s \leq n} F_r(C) \otimes F_s(C) \text{ for all } n \geq 0.
\end{align*}

Note that the subspaces \( F_n(C) \subseteq C, \ n \geq 0, \) of a filtered coalgebra are subcoalgebras. If \( (C, (C(n))_{n \geq 0}) \) is an \( \mathbb{N}_0 \)-graded coalgebra, then \( (C, \mathcal{F}(C)) \) is an \( \mathbb{N}_0 \)-filtered coalgebra with \( F_n(C) = \bigoplus_{m=0}^n C(m) \) for all \( n \geq 0 \).

We want to prove two useful results about filtered coalgebras. We first look at their simple subcoalgebras. A coalgebra \( C \) is called **simple** if \( C \neq 0 \), and if \( 0 \) and \( C \) are the only subcoalgebras of \( C \).

**Proposition 1.3.2.** Let \((C, \mathcal{F}(C))\) be an \( \mathbb{N}_0 \)-filtered coalgebra. Then any simple subcoalgebra of \( C \) is contained in \( F_0(C) \).

**Proof.** Let \( D \subseteq C \) be a simple subcoalgebra. Since \( F_0(C) \cap D \) is a subcoalgebra of \( C \) by Proposition 1.1.9, it is enough to prove that \( F_0(C) \cap D \) is non-zero. Let \( n \geq 0 \) be minimal such that \( F_n(C) \cap D \neq 0 \), and let \( x \in F_n(C) \cap D \) with \( x \neq 0 \). If \( \Delta(x) \in F_0(C) \otimes D \), then \( x = (\text{id} \otimes \varepsilon) \Delta(x) \in F_0(C) \), and we are done. If \( \Delta(x) \notin F_0(C) \otimes D \), then there exists \( f \in C^* = \text{Hom}(C, k) \) such that \( f(x(1))x(2) \neq 0 \) and \( f(F_0(C)) = 0 \). Since \( f(x(1))x(2) \in F_{n-1}(C) \cap D \), we obtain a contradiction to the minimality of \( n \).

We introduce at this point a basic coalgebra notion.

**Definition 1.3.3.** A coalgebra \( C \) is called **pointed** if every simple subcoalgebra of \( C \) is one-dimensional.
If \( C \) is a one-dimensional coalgebra, then there is a unique group-like element \( 1_C \) in \( C \), and \( C = k1_C \). In this section we study pointed coalgebras with a unique group-like element.

The main examples of coalgebras and Hopf algebras which appear in this book are pointed. We will say more on pointed coalgebras and Hopf algebras in Sections 2.4 and 5.4.

**Corollary 1.3.4.** Let \( (C, \mathcal{F}(C)) \) be an \( \mathbb{N}_0 \)-filtered coalgebra. If \( F_0(C) \) is one-dimensional, then \( F_0(C) \) is the unique simple subcoalgebra of \( C \). The coalgebra \( C \) then has a unique group-like element which spans \( F_0(C) \).

**Proof.** The subcoalgebra \( F_0(C) \) is one-dimensional, hence simple. Thus the claim follows from Proposition 1.3.2. \( \square \)

We prove Takeuchi’s criterion for invertibility in \( \text{Hom}(C, A) \).

**Proposition 1.3.5.** Let \( (C, \mathcal{F}) \) be a filtered coalgebra and assume that \( F_0(C) \) is one-dimensional with unique group-like element \( 1_C \). Let \( A \) be an algebra and \( f : C \to A \) a linear map with \( f(1_C) = 1 \). Then \( f \) is invertible in \( \text{Hom}(C, A) \) with respect to convolution, and its inverse is

\[
f^{-1} = \sum_{n \geq 0} (\varepsilon - f)^n.
\]

**Proof.** Let \( g = \varepsilon - f \). We first show that \( \sum_{n \geq 0} g^n \) is well-defined. Let \( m \geq 0 \), and \( x \in F_m(C) \). Then for all \( n > m \),

\[
g^n(x) = \sum_{k_1 + \ldots + k_n \leq m} g(F_{k_1}(C)) \cdots g(F_{k_n}(C)) = 0,
\]

since \( g(F_0(C)) = 0 \). Hence \( \sum_{n \geq 0} g^n(x) = \sum_{n=0}^m g^n(x) \). Then in the algebra \( \text{Hom}(C, A) \),

\[
(f \sum_{n \geq 0} (\varepsilon - f)^n)(x) = (\varepsilon - g) \sum_{n \geq 0} g^n(x)
\]

\[
= (\varepsilon(x(1)) - g(x(1))) \sum_{n=0}^m g^n(x(2))
\]

\[
= \sum_{n=0}^m g^n(x) - \sum_{n=0}^m g^{n+1}(x)
\]

\[
= \varepsilon(x).
\]

The equation \( (\sum_{n \geq 0} (\varepsilon - f))^f = \varepsilon \) follows in the same way. \( \square \)

Let \( C \) be a coalgebra with exactly one group-like element, which we call \( 1_C = 1 \).

The space of **primitive elements** of \( C \) is defined by

\[
P(C) = P_{1,1}(C) = \{ x \in C \mid \Delta(x) = 1 \otimes x + x \otimes 1 \}.
\]

Note that \( \varepsilon(x) = 0 \) for each \( x \in P(C) \) by the counit axiom.

The **primitive elements of a bialgebra** \( H \) are the elements in

\[
P(H) = P_{1,1}(H) = \{ x \in H \mid \Delta(x) = 1 \otimes x + x \otimes 1 \}.
\]

Let \( C \) be an \( \mathbb{N}_0 \)-graded coalgebra. We call \( C \) **connected** if \( C(0) \) is one-dimensional. Then \( F_n(C) = \bigoplus_{i=0}^n C(i), \ n \geq 0, \) is a coalgebra filtration of \( C \).
with one-dimensional $F_0(C) = k1$, and 1 is the unique group-like element of $C$. If $C$ is connected, then $P(C) \subseteq C$ is a graded subspace, since $P(C)$ is the kernel of the graded map $C \to \bigotimes C$, $x \mapsto \Delta(x) - 1 \otimes x - x \otimes 1$.

**Lemma 1.3.6.** (1) Let $(C, F(C))$ be an $\mathbb{N}_0$-filtered coalgebra. Assume that $F_0(C) = k1$ is one-dimensional. Let $n \geq 1$ and $x \in F_n(C)$. Then

$$\Delta(x) \in 1 \otimes x + x \otimes 1 + F_{n-1}(C) \otimes F_{n-1}(C).$$

(2) Let $C$ be a connected $\mathbb{N}_0$-graded coalgebra. Then

$$\Delta(x) \in 1 \otimes x + x \otimes 1 + \bigoplus_{i=1}^{n-1} C(i) \otimes C(n-i)$$

for all $n \geq 1$ and $x \in C(n)$. In particular, $C(1) \subseteq P(C)$.

(3) Let $C$ be an $\mathbb{N}_0$-graded coalgebra. Then the maps $\Delta_{0,n}$ and $\Delta_{n,0}$ are injective for all $n \geq 0$.

**Proof.** (1) Since $F(C)$ is a coalgebra filtration with $F_0(C) = k1$, there exist $y, z \in F_n(C)$ such that $\Delta(x) - 1 \otimes y - z \otimes 1 \in F_{n-1}(C) \otimes F_{n-1}(C)$. Then

$$\Delta(x) - 1 \otimes x - x \otimes 1 - 1 \otimes (y-x) - (z-x) \otimes 1 \in F_{n-1}(C) \otimes F_{n-1}(C).$$

By the counit axioms, $x - y - \varepsilon(z)1 \in F_{n-1}(C)$ and $x - z - \varepsilon(y)1 \in F_{n-1}(C)$. Since $n \geq 1$, this implies (1).

(2) Let $n \geq 1$ and $x \in C(n)$. Since $C$ is a connected graded coalgebra, there exist $y, z \in C(n), w \in \bigoplus_{i=1}^{n-1} C(i) \otimes C(n-i)$ such that $\Delta(x) = 1 \otimes y + z \otimes 1 + w$. By applying $\text{id} \otimes \varepsilon$ and $\varepsilon \otimes \text{id}$ to this equation we see that $x = y = z$. In particular, $C(1) \subseteq P(C)$.

(3) Let $n \geq 0$ and $x \in C(n)$. Then $\Delta(x) = \sum_{i=0}^{n} \Delta_{i,n-i}(x)$, hence

$$x = (\text{id}_C \otimes \varepsilon)\Delta(x) = (\text{id}_C \otimes \varepsilon)(\Delta_{n,0}(x)) = (\varepsilon \otimes \text{id}_C)(\Delta_{0,n}(x))$$

since $\varepsilon(C(i)) = 0$ for all $i \geq 1$. This implies the claim. $\square$

In general, a connected $\mathbb{N}_0$-graded coalgebra has non-zero primitive elements in degrees $\geq 2$.

**Example 1.3.7.** If $H$ is a bialgebra, then for all $x, y \in P(H)$, the commutator $[x, y] = xy - yx$ is a primitive element in $H$. In particular, in the free algebra in Example 1.2.24 iterated commutators of the primitive generators are primitive.

**Example 1.3.8.** Let $H = k[x]$ be the polynomial algebra in one variable $x$. Then $H$ is an $\mathbb{N}_0$-graded coalgebra (and bialgebra) with

$$H(n) = kx^n, \quad \Delta(x^n) = \sum_{i=0}^{n} \binom{n}{x^i} \otimes x^{n-i}, \quad \varepsilon(x^n) = \delta_{0n} \quad \text{for all } n \geq 0.$$ 

Note that $H$ is the universal enveloping algebra of the one-dimensional abelian Lie algebra. Assume that the characteristic of $k$ is 0. Then it is easy to see (and follows from the Theorem of Poincaré, Birkhoff, Witt) that $P(H) = H(1)$. But if the characteristic of $k$ is $p > 0$, then for all $m \geq 1$ the binomial coefficients $\binom{p^n}{i}$ are zero for all $1 \leq i \leq p^n - 1$, hence $x^p$ is primitive.

**Definition 1.3.9.** ([Swe69, Section 11.2]) An $\mathbb{N}_0$-graded coalgebra is called **strictly graded** if it is connected with $P(C) = C(1)$. 
The next proposition is a very special case of the following theorem of Heynemann and Radford: If \( f : C \to D \) is a homomorphism of coalgebras such that the restriction of \( f \) to the first part \( C_1 \) of the coradical filtration is injective, then \( f \) is injective. See [Mon93, Theorem 5.3.1] for a proof of this result.

**Proposition 1.3.10.** Let \((C, \mathcal{F}(C))\) be an \( \mathbb{N}_0 \)-filtered coalgebra and assume that \( F_0(C) = k1 \) is one-dimensional.

1. Let \( 0 \neq I \subseteq C \) be a coideal. Then \( I \cap P(C) \neq 0 \).
2. Let \( D \) be a coalgebra, and \( f : C \to D \) a coalgebra homomorphism such that \( f|P(C) \) is injective. Then \( f \) is injective.

**Proof.** The homomorphism theorem for coalgebras, Proposition 1.1.13, implies that (1) and (2) are equivalent. We prove (2). We show by induction on \( n \) that \( f|F_n(C) \) is injective for all \( n \). If \( n = 0 \), then \( f|F_0(C) \) is injective, since \( 1 = \varepsilon(f(1)) \). Let \( n \geq 1 \) and assume that \( f|F_{n-1}(C) \) is injective. Let \( x \in F_n(C) \) with \( f(x) = 0 \). By Lemma 1.3.6(1) there is an element \( w \in F_{n-1}(C) \otimes F_{n-1}(C) \) such that \( \Delta(x) = 1 \otimes x + x \otimes 1 + w \). Then

\[
0 = \Delta(f(x)) = f(1) \otimes f(x) + f(x) \otimes f(1) + (f \otimes f)(w).
\]

Thus \((f \otimes f)(w) = 0\), and hence \( w = 0 \) by Lemma 1.1.11 and by induction. Therefore \( x \in P(C) \) and then \( x = 0 \) by the injectivity of \( f|P(C) \).

**Corollary 1.3.11.** Let \( C \) be a strictly graded coalgebra.

1. Let \( 0 \neq I \subseteq C \) be a coideal. Then \( I \cap C(1) \neq 0 \).
2. Let \( D \) be a coalgebra, and \( f : C \to D \) a coalgebra homomorphism such that \( f(C(1)) \) is injective. Then \( f \) is injective.
3. Let \( 0 \neq E \subseteq C \) be a subspace with \( E \cap C(1) = 0 \). Assume \( \Delta(E) \subseteq E \otimes C \) or \( \Delta(E) \subseteq C \otimes E \). Then \( E = k1_C \).

**Proof.** (1) and (2) follow from Proposition 1.3.10 using the coalgebra filtration \( \mathcal{F}(C) \) with \( F_n(C) = \bigoplus_{i=0}^{n} C(n) \) for all \( n \geq 0 \), since \( P(C) = C(1) \).

(3) By Lemma 1.1.14, \( E \cap \ker(\varepsilon) \) is a coideal of \( C \) and \( E \not\subseteq \ker(\varepsilon) \). Then \( E \cap \ker(\varepsilon) = 0 \) by (1), and hence \( E \) is one-dimensional. Since \( C \) is connected, we conclude that \( E = k1_C \).

We will characterize strictly graded coalgebras in terms of the components of the graded map \( \Delta \) and of its iterations.

**Definition 1.3.12.** Let \( C = \bigoplus_{n \in \mathbb{N}_0} C(n) \) be a graded coalgebra with projections \( \pi_n = \pi_n^C \) for all \( n \geq 0 \). For all \( n \geq 1 \) we denote the \((1, \ldots, 1)\)-th component of \( \Delta^{n-1} \) by

\[
\Delta_{1^n} : C(n) \subseteq C \xrightarrow{\Delta^{n-1}} C^{\otimes n} \xrightarrow{\pi_1^{\otimes n}} C(1)^{\otimes n}.
\]

Let \( I_C(n) = \ker(\Delta_{1^n}) \) for all \( n \geq 1 \), and

\[
I_C = \bigoplus_{n \geq 1} I_C(n) = \bigoplus_{n \geq 2} I_C(n).
\]

Note that \( I_C(1) = 0 \) since \( \Delta_1 = \text{id} \).

**Lemma 1.3.13.** Let \( C \) be an \( \mathbb{N}_0 \)-graded coalgebra.
Lemma 1.1.11. Therefore

\[ \Delta H \]

Hence

\[ \text{where the last equality holds by (1)(a).} \]

Thus

\[ 1 \leq i \leq n - 1. \text{ Then } \Delta_{1^n} = (\Delta_{1^i} \otimes \Delta_{1^{n-i}})\Delta_{i,n-i}. \]

(2) Assume that \( C \) is connected. Then \( I_C \subseteq C \) is a coideal of \( C \).

Proof. (1)(a) Since \( \Delta \) is graded,

\[ \Delta^{n-1}(C(m)) \subseteq \bigoplus_{i_1 + \cdots + i_n = m} C(i_1) \otimes \cdots \otimes C(i_n). \]

Thus \( \pi_1^{\otimes n} \Delta^{n-1}|C(m) = 0 \) if \( m \neq n \).

To prove (1)(b) let \( n \geq 2 \) and \( x \in C(n) \). Then

\[ \Delta(x) = \sum_{j=0}^{n} \Delta_{j,n-j}(x) \]

definition of the components of \( \Delta \). Note that \( \Delta^{n-1} = (\Delta^{i-1} \otimes \Delta^{n-i-1})\Delta \) for all \( 1 \leq i \leq n - 1 \) by coassociativity. Hence

\[ \Delta_{1^n}(x) = \pi_1^{\otimes n} \Delta^{n-1}(x) \]

\[ = \pi_1^{\otimes n} (\Delta^{i-1} \otimes \Delta^{n-i-1}) \left( \sum_{j=0}^{n} \Delta_{j,n-j}(x) \right) \]

\[ = \sum_{j=0}^{n} \left( \pi_1^{\otimes i} \Delta^{i-1} \otimes \pi_1^{\otimes (n-i)} \Delta^{n-i-1} \right)(\Delta_{j,n-j}(x)) \]

\[ = (\Delta_{1^i} \otimes \Delta_{1^{n-i}})\Delta_{i,n-i}(x), \]

where the last equality holds by (1)(a).

(2) Let \( n \geq 2, \ x \in I_C(n) \) and \( i \in \{1, \ldots, n - 1\} \). By (1)(b),

\[ 0 = \Delta_{1^n}(x) = (\Delta_{1^i} \otimes \Delta_{1^{n-i}})\Delta_{i,n-i}(x). \]

Hence \( \Delta_{i,n-i}(x) \in \ker(\Delta_{1^i} \otimes \Delta_{1^{n-i}}) = C(i) \otimes I_C(n - i) + I_C(i) \otimes C(n - i) \) by Lemma 1.1.11. Therefore

\[ \Delta(x) = 1 \otimes x + x \otimes 1 + \sum_{i=1}^{n-1} \Delta_{i,n-i}(x) \in C \otimes I_C + I_C \otimes C \]

by Lemma 1.3.6(2). \( \square \)

Proposition 1.3.14. Let \( C \) be an \( \mathbb{N}_0 \)-graded coalgebra.

(1) The following are equivalent.

(a) For all \( n \geq 2, \ \Delta_{1^n} : C(n) \to C(1)^{\otimes n} \) is injective.

(b) For all \( i, j \geq 0, \ \Delta_{i,j} : C(i + j) \to C(i) \otimes C(j) \) is injective.

(c) For all \( n \geq 2, \ \Delta_{n-1,1} : C(n) \to C(n - 1) \otimes C(1) \) is injective.

(d) For all \( n \geq 2, \ \Delta_{1,n-1} : C(n) \to C(1) \otimes C(n - 1) \) is injective.

(2) Assume that \( C \) is connected. Then the following are equivalent.

(a) \( C \) is strictly graded.

(b) Conditions (a) – (d) in (1).

(c) \( I_C = 0 \).

Proof. (1) (a) \( \Rightarrow \) (b): By Lemma 1.3.13(1b), \( \Delta_{i,j} \) is injective for all \( i, j \geq 1 \). This proves (b) by Lemma 1.3.6(3).

(b) \( \Rightarrow \) (c) and (b) \( \Rightarrow \) (d) are trivial.
(d) $\Rightarrow$ (a) follows by induction on $n$, since by Lemma 1.3.13(1b),
\[
\Delta_{1^n} = (\text{id}_{C(1)} \otimes \Delta_{1^{n-1}}) \Delta_{1,n-1}
\]
for all $n \geq 2$. The implication (c) $\Rightarrow$ (a) is shown similarly.

(2) By definition of $I_C$, (1a) holds if and only if $I_C = 0$. Assume that $C$ is
strictly graded. By Lemma 1.3.13(2), $I_C$ is a coideal of $C$. Hence $I_C = 0$ by
Corollary 1.3.11(1). Conversely, assume that $I_C = 0$. Then for all $n \geq 2$
and $x \in C(n) \cap P(C)$, $\Delta_{n-1,1}(x) = 0$, and $x = 0$ by (1c). Thus $C$ is strictly graded. \(\square\)

**Definition 1.3.15.** Let $C$ be a connected $\mathbb{N}_0$-graded coalgebra. The coalgebra
$B(C) = C/I_C$ is called the **associated strictly graded coalgebra** to $C$. Let
$\pi_C : C \rightarrow B(C)$ denote the canonical graded coalgebra map.

The next theorem gives a characterization of the coalgebra $B(C)$.

**Theorem 1.3.16.** Let $C$ be a connected $\mathbb{N}_0$-graded coalgebra.

1. The coideal $I_C$ is the only graded coideal $I$ of $C$ such that
   (a) $C/I$ is strictly graded, and
   (b) $\pi(1) : (1) \rightarrow (C/I)(1)$ is bijective, where $\pi : C \rightarrow C/I$ is the
      canonical map.

2. The coideal $I_C$ is the largest coideal of $C$ contained in $\bigoplus_{n \geq 2} C(n)$.

3. The coideal $I_C$ is the only coideal $I$ of $C$ contained in $\bigoplus_{n \geq 2} C(n)$ such
   that $P(C/I) = C(1)$.

4. Let $D$ be an $\mathbb{N}_0$-graded coalgebra and $\pi : C \rightarrow D$ a surjective graded
   coalgebra map such that $\pi(1) : (1) \rightarrow D(1)$ is bijective. Then there is
   exactly one graded coalgebra map $\tilde{\pi} : D \rightarrow B(C)$ with $\pi_C = \tilde{\pi} \pi$.

**Proof.** We first show that $I_C$ satisfies (1)(a) and (1)(b). By Lemma 1.3.13(2),
$I_C \subseteq C$ is a graded coideal of $C$. By definition, the grading of $B(C)$ is given by
$B(C) = \mathbb{K}1 \oplus C(1) \oplus \bigoplus_{n \geq 2} C(n)/I_C(n)$. Thus (1)(b) holds. To prove that $B(C)$ is
strictly graded we use Proposition 1.3.14(2). We show that $\Delta^{B(C)}_{1^n}$ is injective for all $n \geq 2$. Let $n \geq 2$. Since $\pi_C : C \rightarrow B(C) = C/I_C$ is a graded coalgebra map and
$C(1) = B(C)(1)$,
\[
\Delta^{B(C)}_{1^n} = \left( C(n) \xrightarrow{\pi_C(n)} C(n)/I_C(n) \xrightarrow{\Delta^{B(C)}_{1^n}} C(1)^{\otimes n} \right).
\]
Hence $\Delta^{B(C)}_{1^n}$ is injective, since by definition, $I_C(n) = \ker(\Delta^{C}_{1^n})$.

(2) Let $J \subseteq C$ be the sum of all coideals of $C$ contained in $\bigoplus_{n \geq 2} C(n)$. Then $J$
is the largest coideal of $C$ contained in $\bigoplus_{n \geq 2} C(n)$. Hence $I_C \subseteq J$, and the induced
map $f : C/I_C \rightarrow C/J$ is a coalgebra map which is injective when restricted to
$C/I_C(1) = C(1)$. Since $C/I_C$ is strictly graded, $f$ is injective by Corollary 1.3.11(2). Thus $I_C = J$.

(3) By the first paragraph of the proof, $P(C/I_C) = C(1)$. Let $I$ be a coideal of $C$
contained in $\bigoplus_{n \geq 2} C(n)$ with $P(C/I) = C(1)$. Then $I \subseteq I_C$ by (2). The induced
coalgebra homomorphism $C/I \rightarrow C/I_C$ is injective by Proposition 1.3.10(2), since
it is injective on $P(C/I)$. Note that the image of the natural filtration of $C$ is a
coalgebra filtration of $C/I$ with one-dimensional $F_0(C/I)$.

(4) Let $I = \ker(\pi)$. Then $I \subseteq C$ is a graded coideal. By assumption, $I(1) = 0$. Further, $I(0) = 0$ since $C$ is connected and $\varepsilon(1_C) = 1$. Hence $I \subseteq I_C$ by (2). This
proves existence and the uniqueness of $\tilde{\pi}$, since $\pi$ is surjective.
To finish the proof of (1), we have to show that each coideal \( I \) of \( C \) satisfying (a) and (b) coincides with \( I_C \). Let \( I \subseteq C \) be such a coideal. Then \( I \subseteq I_C \) by (2), and the induced map \( C/I \to C/I_C \) is bijective by Corollary 1.3.11(2). Hence \( I = I_C \). 

We finally note a useful property of the tensor product of strictly graded coalgebras.

**Proposition 1.3.17.** Let \( C, D \) be strictly \( \mathbb{N}_0 \)-graded coalgebras. Assume that the tensor product \( C \otimes D \) of the vector spaces \( C, D \) has a coalgebra structure with comultiplication \( \Delta_{C \otimes D} \) and counit \( \varepsilon_{C \otimes D} = \varepsilon_C \otimes \varepsilon_D \) such that

1. \((C \otimes D, \Delta_{C \otimes D}, \varepsilon_{C \otimes D})\) is an \( \mathbb{N}_0 \)-graded coalgebra with grading 
\[
(C \otimes D)(n) = \bigoplus_{i+j=n} C(i) \otimes D(j) \quad \text{for all } n \geq 0,
\]
2. \((\text{id}_C \otimes \varepsilon_D \otimes \varepsilon_C \otimes \text{id}_D)\Delta_{C \otimes D} = \text{id}_{C \otimes D},
3. \((\text{id}_C \otimes \varepsilon_D : C \otimes D \to C \otimes \mathbb{k} \cong C \) and \( \varepsilon_C \otimes \text{id}_D : C \otimes D \to \mathbb{k} \otimes D \cong D \) are coalgebra maps.

Then \( C \otimes D \) is a strictly graded coalgebra.

**Proof.** Let \( n \geq 2 \) and \( x \in (C \otimes D)(n) \) a primitive element. We write
\[
x = 1_C \otimes d + y + c \otimes 1_D, \quad c \in C(n), \quad d \in D(n), \quad y \in \bigoplus_{i=1}^{n-1} C(i) \otimes D(n-i).
\]

By assumption,
\[
\Delta(x) = x \otimes 1_C \otimes 1_D + 1_C \otimes y \otimes 1_D + c \otimes 1_D \otimes x \in C \otimes D \otimes C \otimes D.
\]

We apply \( f = \text{id}_C \otimes \varepsilon_D \otimes \varepsilon_C \otimes \text{id}_D \) to both sides of this equation. Then by (2), \( f\Delta(x) = x \). Hence \( x = 1_C \otimes d + c \otimes 1_D \). Moreover, \( c = (\text{id}_C \otimes \varepsilon_D)(x) \in P(C) \) and \( d = (\varepsilon_C \otimes \text{id}_D)(x) \in P(C) \) by (3). Hence \( c = 0 \), \( d = 0 \) and \( x = 0 \), since \( C \) and \( D \) are strictly graded. 

Proposition 1.3.17 can be applied to the usual tensor product of coalgebras, but also to more general “braided tensor products”.

### 1.4. Yetter-Drinfeld modules over a group algebra

In this section, let \( G \) be a group. We write \( g \triangleright h = ghg^{-1}, \ g, h \in G \), for the adjoint action of \( G \) on itself. The center of \( G \) is denoted by \( Z(G) \).

If \( V \) is a left \( \mathbb{k}G \)-module, and \( \chi \in \hat{G} = \text{Gr}(G, \mathbb{k}^\times) \) is a character of \( G \), we define \( V^\chi = \{ v \in V \mid g \cdot v = \chi(g)v \ \text{for all} \ g \in G \} \).

**Definition 1.4.1.** A **Yetter-Drinfeld module over the group algebra** \( \mathbb{k}G \) is a \( \mathbb{Z} \)-graded vector space \( V = \bigoplus_{g \in G} V_g \), and a left \( \mathbb{k}G \)-module with module structure \( \mathbb{k}G \otimes V \to V, \ g \otimes v \mapsto g \cdot v \), where \( g \in G \), such that

\[
(1.4.1) \quad g \cdot V_h \subseteq V_{g \triangleright h} \quad \text{for all } g, h \in G.
\]

We denote the category of Yetter-Drinfeld modules over the group algebra \( \mathbb{k}G \) by \( \underline{\mathbb{G}YD} \). Objects of \( \underline{\mathbb{G}YD} \) are the Yetter-Drinfeld modules over \( \mathbb{k}G \), morphisms are the \( G \)-graded and \( G \)-linear maps. Let \( \underline{\mathbb{G}YD}^{\text{fin}} \) be the full subcategory of \( \underline{\mathbb{G}YD} \) of finite-dimensional objects.
If $V$ is a Yetter-Drinfeld module over $\mathbb{k}G$, then $g \cdot V_h = V_{g \cdot h}$ for all $g, h \in G$, since $g \cdot V_h \subseteq V_{g \cdot h}$ and $g^{-1} \cdot V_{g \cdot h} \subseteq V_h$. If $G$ is abelian, then Yetter-Drinfeld modules over $\mathbb{k}G$ are $G$-graded vector spaces and $G$-modules such that each homogeneous component is stable under the action of $G$.

**Example 1.4.2.** Assume that $G$ is abelian. Let $h \in G$. Then any $\mathbb{k}G$-module $U$ is a Yetter-Drinfeld module over $\mathbb{k}G$ with $U = U_h$. On the other hand, let $V$ be a non-zero Yetter-Drinfeld module over $\mathbb{k}G$. Then there is an $h \in G$ such that $V_h \neq 0$. Moreover, for any $h \in G$ the subspace $V_h$ is a Yetter-Drinfeld submodule of $V$ and any subspace of $V_h$ is a $\mathbb{k}G$-submodule of $V_h$ if and only if it is a Yetter-Drinfeld submodule. In particular, the set of isomorphism classes of irreducible Yetter-Drinfeld modules over $\mathbb{k}G$ is in bijection to $G \times \text{Irrep } G$, where $\text{Irrep } G$ is the set of isomorphism classes of simple $\mathbb{k}G$-modules.

**Example 1.4.3.** Let us determine one-dimensional Yetter-Drinfeld modules $V = kx \in \mathcal{G}_Y^D$. The action on $V$ and the degree of $x$ are given by a character $\chi \in \hat{G} = \text{Gr}(G, \mathbb{k}^\times)$ and an element $g \in G$ with

$$h \cdot x = \chi(h)x, \quad x \in V_g,$$

for all $h \in G$. The Yetter-Drinfeld condition (1.4.1) holds if and only if for all $h \in G$, $hgh^{-1} = \deg(h \cdot x) = \deg(\chi(h)x) = g$, that is, if and only if $g \in Z(G)$. Thus there is a bijection between the set of isomorphism classes of one-dimensional Yetter-Drinfeld modules in $\mathcal{G}_Y^D$ and $Z(G) \times \hat{G}$.

**Example 1.4.4.** Assume that $G$ is abelian, and $\mathbb{k}$ is algebraically closed. Let $V$ be a finite-dimensional irreducible $\mathbb{k}G$-module, and let $\rho : \mathbb{k}G \to \text{End}(V)$ be the representation of $V$. Then there is a common eigenvector for the set $\rho(\mathbb{k}G)$ of pairwise commuting endomorphisms. Hence $V$ is one-dimensional.

It follows from the two previous examples that the finite-dimensional irreducible objects in $\mathcal{G}_Y^D$ are one-dimensional and given by elements in $G \times \hat{G}$.

**Lemma 1.4.5.** Let $G$ be an abelian group and $V \in \mathcal{G}_Y^D$. Then the following are equivalent:

1. $V$ is a direct sum of one-dimensional Yetter-Drinfeld modules in $\mathcal{G}_Y^D$.
2. $V$ is a direct sum of one-dimensional $G$-modules.

**Proof.** Clearly, (1) implies (2). Assume now (2). Since $G$ is abelian, the comodule decomposition $V = \bigoplus_{g \in G} V_g$ is a decomposition of $G$-modules. By (2), all direct summands $V_g$, $g \in G$, are direct sums of one-dimensional Yetter-Drinfeld modules. \qed

**Proposition 1.4.6.** Let $G$ be a finite abelian group and $V \in \mathcal{G}_Y^D^{\text{fd}}$. Assume that $\mathbb{k}$ is algebraically closed and that char($\mathbb{k}$) does not divide the order of $G$.

1. Any finite-dimensional $\mathbb{k}G$-module is a direct sum of one-dimensional $\mathbb{k}G$-modules.
2. Any $V \in \mathcal{G}_Y^D^{\text{fd}}$ is the direct sum of one-dimensional Yetter-Drinfeld modules.

**Proof.** (1) is well-known (and follows from the Theorem of Maschke and Example 1.4.4), and (2) follows from (1) and Lemma 1.4.5. \qed
Example 1.4.7. We denote the symmetric group of $n$ elements $\{1, \ldots, n\}$ by $S_n$. Let $O_2 = \{(i, j) \mid 1 \leq i < j \leq n\}$ be the set of all transpositions in $S_n$, $n \geq 3$. Let $V_n$ be the Yetter-Drinfeld module in $S_n \mathcal{YD}$ with basis $x_t$, $t \in O_2$, and

$$\deg(x_t) = t, \quad s \cdot x_t = \text{sign}(s)x_{st}$$

for all $t \in O_2$, $s \in S_n$.

Note that $V_n$ is irreducible in $S_n \mathcal{YD}$, since any non-zero subobject contains $x_t$ for some $t$, and the elements $g \cdot x_t$ with $g \in S_n$ span $V_n$, since $O_2$ is a conjugacy class of $S_n$.

Remark 1.4.8. Yetter-Drinfeld modules $V$ in $G \mathcal{YD}$ can equivalently be defined as left $kG$-modules with a left $kG$-comodule structure

$$\delta : V \to kG \otimes V, \quad v \mapsto v_{(-1)} \otimes v_{(0)},$$

such that

$$\delta(g \cdot v) = gv_{(-1)}g^{-1} \otimes g \cdot v_{(0)}$$

for all $v \in V$, $g \in G$. This follows from the category isomorphism between $G$-graded vector spaces and $kG$-comodules in Proposition 1.1.17.

Let $V, W \in G \mathcal{YD}$. Note that $V \otimes W$ is an object in $G \mathcal{YD}$ with diagonal action and diagonal coaction of $G$. The trivial object $k$ with grading $k = k_0$ and $G$-action $g \cdot 1 = 1$ for all $g \in G$ is an object in $G \mathcal{YD}$.

Proposition 1.4.9. (1) Let $V, W, V', W' \in G \mathcal{YD}$. Then for all morphisms $f : V \to V'$ and $g : W \to W'$ in $G \mathcal{YD}$, the tensor product $f \otimes g : V \otimes W \to V' \otimes W'$ is a morphism in $G \mathcal{YD}$.

(2) For all $U, V, W \in G \mathcal{YD}$ the canonical isomorphisms

$$(U \otimes V) \otimes W \xrightarrow{\sim} U \otimes (V \otimes W), \quad k \otimes V \xrightarrow{\sim} V, \quad V \otimes k \xrightarrow{\sim} V$$

are morphisms in $G \mathcal{YD}$.

Proof. (1) is clear from the definition, and (2) is a special case of Proposition 1.2.5.

Let $H$ be a bialgebra. Suppose that the canonical isomorphism of vector spaces

$$\tau_{V,W} : V \otimes W \xrightarrow{\sim} W \otimes V, \quad v \otimes w \mapsto w \otimes v,$$

is $H$-linear for all left $H$-modules $V, W$ and the diagonal action. Then $H$ is co-commutative. Similarly, $H$ is commutative, if $\tau_{V,W}$ is $H$-colinear for all left $H$-comodules $V, W$ with the diagonal coaction.

Hence it is quite remarkable that a commutativity rule for objects in $G \mathcal{YD}$ does exist. It is not the flip map $\tau_{V,W}$, but it is a natural isomorphism in $G \mathcal{YD}$ which behaves like a commutativity law.

Definition 1.4.10. For all $V, W \in G \mathcal{YD}$ the linear map

$$(1.4.2) \quad c_{V,W} : V \otimes W \to W \otimes V$$

defined by $c_{V,W}(v \otimes w) = g \cdot w \otimes v$ for all $g \in G$, $v \in V_g$, and $w \in W$, is called the braiding of $V, W$.

Proposition 1.4.11. (1) For all $V, W \in G \mathcal{YD}$, $c_{V,W} : V \otimes W \to W \otimes V$ is an isomorphism in $G \mathcal{YD}$. 

(2) For all objects $U, V, W, V', W'$ in $\mathcal{G}_YD$ and all morphisms $f : V \to V'$, $g : W \to W'$ in $\mathcal{G}_YD$, the following diagrams commute.

\[
\begin{array}{c}
V \otimes W \xrightarrow{c_{V,W}} W \otimes V \\
\downarrow f \otimes g \downarrow g \otimes f \\
V' \otimes W' \xrightarrow{c_{V',W'}} W' \otimes V'
\end{array}
\]

\[\text{(1.4.3)}\]

\[
\begin{array}{c}
U \otimes V \otimes W \xrightarrow{c_{U,V \otimes W}} V \otimes W \otimes U \\
\downarrow c_{U,V} \otimes \text{id} \downarrow \text{id} \otimes c_{U,W} \\
V \otimes U \otimes W
\end{array}
\]

\[\text{(1.4.4)}\]

\[
\begin{array}{c}
U \otimes V \otimes W \xrightarrow{c_{U \otimes V, W}} W \otimes U \otimes V \\
\downarrow \text{id} \otimes c_{U,V} \otimes \text{id} \downarrow c_{U,W} \otimes \text{id} \\
U \otimes W \otimes V
\end{array}
\]

\[\text{(1.4.5)}\]

\[
\begin{array}{c}
k \otimes V \xrightarrow{c_{k,V}} V \otimes k \\
\downarrow \cong \downarrow \cong \\
V = V
\end{array}
\]

\[\text{(1.4.6)}\]

\[
\begin{array}{c}
V \otimes k \xrightarrow{c_{V,k}} k \otimes V \\
\downarrow \cong \downarrow \cong \\
V = V
\end{array}
\]

(Note that Proposition 1.4.9 is used in the formulation of (2).)

We will meet the diagrams of Proposition 1.4.11 later in Section 3.2 in the axioms of a braided monoidal category.

**Proof.** (1) To see that $c_{V,W}$ is $G$-linear and $G$-graded, let $g, h \in G$, and let $v \in V_g$, $w \in W_h$ be homogeneous elements. Then for all $a \in G$,

\[
c_{V,W}(a \cdot (v \otimes w)) = c_{V,W}(a \cdot v \otimes a \cdot w) = aag^{-1}a \cdot w \otimes a \cdot v = a \cdot c_{V,W}(v \otimes w),
\]

\[
\deg(c_{V,W}(v \otimes w)) = \deg(g \cdot w \otimes v) = ghg^{-1}g = \deg(v \otimes w).
\]

The map $c_{V,W}$ is an isomorphism with inverse

\[
c_{V,W}^{-1} : W \otimes V \to V \otimes W, \ \ w \otimes v \mapsto v \otimes g^{-1} \cdot w,
\]

for all $v \in V_g$, $g \in G$, and $w \in W$.

(2) The commutativity of the diagrams is easily checked on homogeneous elements. \[\square\]

**Definition 1.4.12.** Let $G$ be an abelian group, and $\chi : G \times G \to \mathbb{k}^\times$ a **bicharacter** of $G$, that is, a mapping $\chi$ such that for all $f, g, h \in G$

\[
\chi(f + g, h) = \chi(f, h)\chi(g, h), \ \ \chi(f, g + h) = \chi(f, g)\chi(f, h).
\]

Let $\mathcal{G}_YD$ be the full subcategory of $\mathcal{G}_YD$ whose objects are $G$-graded vector spaces $V = \bigoplus_{g \in G} V_g$ with $G$-action defined by $g \cdot v = \chi(g, h)v$ for all $v \in V_h$, $g, h \in G$. 
Note that a bicharacter $\chi$ satisfies $\chi(g,0) = 1 = \chi(0,g)$ for all $g \in G$.
Let $G$ be a free abelian group with basis $(\alpha_i)_{i \in I}$, and let $(q_{ij})_{i,j \in I}$ be a family of non-zero scalars in $\mathbb{k}$. Then
\[
\chi : G \times G \to \mathbb{k}^\times, \quad (\alpha_i, \alpha_j) \mapsto q_{ij} \quad \text{for all } i, j \in I,
\]
defines a bicharacter of $G$.

**Proposition 1.4.13.** Let $G$ be an abelian group and $\chi$ a bicharacter of $G$. Let $V, W \in G\mathcal{YD}$.

1. $V \otimes W \in G\mathcal{YD}$ with diagonal $G$-grading and $G$-action. The trivial object $\mathbb{k}$ of $G\mathcal{YD}$ is an object of $G\mathcal{YD}$.
2. The braiding $c = c_{V,W} : V \otimes W \to W \otimes V$ in $G\mathcal{YD}$ is given by
\[
c(v \otimes w) = \chi(g, h)w \otimes v
\]
for all $v \in V_g$, $w \in W_h$, $g, h \in G$.

**Proof.** Let $f, g, h \in G$, and $v \in V_g$, $w \in W_h$. Then
\[
f \cdot (v \otimes w) = f \cdot v \otimes f \cdot w = \chi(f, g)v \otimes \chi(f, h)w = \chi(f, g + h)v \otimes w.
\]
This proves that $V \otimes W \in G\mathcal{YD}$, and the remaining claims are obvious. \qed

If $\chi$ is a bicharacter of an abelian group, then Proposition 1.4.13 says that the subcategory $G\mathcal{YD} \subseteq G\mathcal{YD}$ is closed under tensor products.

**Example 1.4.14.** Let $G = \mathbb{Z}/(2)$ and $\chi : \mathbb{Z}/(2) \times \mathbb{Z}/(2) \to \mathbb{k}^\times$ the non-trivial bicharacter with $\chi(\bar{i}, \bar{j}) = (-1)^{ij}$, $i, j \in \{0, 1\}$. Assume that char$(k) \neq 2$. Then $S = G\mathcal{YD}$ is called the category of **super vector spaces**. Objects of $S$ are $\mathbb{Z}/(2)$-graded vector spaces $V = V_0 \oplus V_1$, where $V_i = V_i$, $i \in \{0, 1\}$. For a homogeneous element $v \in V_i$ we write $|v| = i$. If $V, W \in S$, then the grading of $V \otimes W$ is given by
\[
(V \otimes W)_0 = V_0 \otimes W_0 \oplus V_1 \otimes W_1, \quad (V \otimes W)_1 = V_0 \otimes W_1 \oplus V_1 \otimes W_0,
\]
and the braiding $c_{V,W} : V \otimes W \to W \otimes V$ by
\[
c(v \otimes w) = (-1)^{|v||w|}w \otimes v
\]
for homogeneous elements $v \in V_i$, $w \in W_i$.

In the remainder of this section, we want to construct the objects in $G\mathcal{YD}$ explicitly for arbitrary groups.

For an element $g \in G$ we denote the centralizer of $g$ by
\[
G^g = \{h \in G \mid hg = gh\},
\]
and the conjugacy class of $g$ by
\[
\mathcal{O}_g = \{h \triangleright g \mid h \in G\}.
\]

Let $\{\mathcal{O}_l \mid l \in L\}$ be the set of all conjugacy classes of $G$, and assume that $\mathcal{O}_k \neq \mathcal{O}_l$ for all $k \neq l$ in $L$.

Any Yetter-Drinfeld module $M \in G\mathcal{YD}$ has a decomposition
\[
(1.4.7) \quad M = \bigoplus_{l \in L} \bigoplus_{s \in \mathcal{O}_l} M_s
\]
into a direct sum of Yetter-Drinfeld modules $\bigoplus_{s \in \mathcal{O}_l} M_s$, $l \in L$. 
We first consider one conjugacy class \( O \subseteq G \). We denote by \( \mathcal{G}_G \mathcal{YD}(O) \) the full subcategory \( \mathcal{G}_G \mathcal{YD}(O) \) of \( \mathcal{G}_G \mathcal{YD} \) consisting of all \( M \in \mathcal{G}_G \mathcal{YD} \) with \( M = \bigoplus_{s \in O} M_s \). Choose an element \( g \in G \). Thus \( O = O_g \), and the map
\[
G/G^g \to O_g, \quad h = hG^g \mapsto h \cdot g,
\]
is bijective. Recall that \( M_{h \cdot g} = h \cdot M_g \) for all \( M \in \mathcal{H}_G \mathcal{YD}(O_g) \) and \( h \in G \). We will see that \( M \) is completely determined by the \( G^g \)-module \( M_g \).

**Definition 1.4.15.** Let \( g \in G \), and let \( V \) be a left \( kG^g \)-module. Define
\[
M(g, V) = kG \otimes_{kG^g} V
\]
as an object in \( \mathcal{G}_G \mathcal{YD}(O_g) \), where \( M(g, V) \) is the induced \( kG \)-module, and the \( G \)-grading is given by
\[
\deg(h \otimes v) = h \cdot g \text{ for all } h \in G, v \in V.
\]

Note that the grading is well-defined and \( M(g, V) \) is a Yetter-Drinfeld module over \( G \), since for all \( v \in V \), \( h \in G \) and \( a \in G^g \),
\[
\deg(ha \otimes v) = (ha) \cdot g = h \cdot g = \deg(h \otimes a \cdot v),
\]
and since for all \( v \in V \) and \( h, h' \in G \),
\[
\deg(h' \cdot (h \otimes v)) = \deg(h' h \otimes v) = (h'h) \cdot g = h' \cdot g = \deg(h \otimes v).
\]

Let \( V, W \) be left \( kG^g \)-modules, and \( f : V \to W \) a left \( kG^g \)-linear map. Then \( \text{id} \otimes f : M(g, V) \to M(g, W) \) is a morphism in \( \mathcal{G}_G \mathcal{YD} \).

Thus we have defined a functor
\[
F_g : kG^g \mathcal{M} \to \mathcal{G}_G \mathcal{YD}(O_g)
\]
with \( F_g(V) = M(g, V) \) and \( F_g(f) = \text{id} \otimes f \) for all left \( kG^g \)-modules \( V, W \) and all left \( kG^g \)-linear maps \( f : V \to W \).

**Lemma 1.4.16.** Let \( g \in G \), \( V \in kG^g \mathcal{M} \), and \( M \in \mathcal{G}_G \mathcal{YD}(O_g) \).

1. The decomposition of \( M(g, V) \) into \( G \)-homogeneous components is given by
\[
M(g, V) = \bigoplus_{s \in O_g} M(g, V)_s, \quad M(g, V)_{h \cdot g} = h \otimes V \text{ for all } h \in G.
\]

2. \( V \xrightarrow{\cong} M(g, V)_g, v \mapsto 1 \otimes v \), is a left \( kG^g \)-linear isomorphism.

3. \( M(g, M_g) \xrightarrow{\cong} M, h \otimes m \mapsto h \cdot m \), is an isomorphism of Yetter-Drinfeld modules in \( \mathcal{G}_G \mathcal{YD} \).

**Proof.** Let \( (h_x)_{x \in X} \) be a complete set of representatives of the cosets in \( G/G^g \), where \( X \) is a set of the same cardinality as \( O_g \). We can assume that \( h_{x_0} = 1 \) for some \( x_0 \in X \). Since \( kG \) is a free right \( kG^g \)-module with basis \( (h_x)_{x \in X} \),
\[
M(g, V) = kG \otimes_{kG^g} V = \bigoplus_{x \in X} h_x \otimes V.
\]

By (1.4.8), \( M(g, V)_{h_x \cdot g} = h_x \otimes V \), since \( h_x \otimes V \subseteq M(g, V)_{h_x \cdot g} \) for all \( x \in X \). In particular, \( M(g, V)_g = 1 \otimes V \), and \( V \xrightarrow{\cong} 1 \otimes V, v \mapsto 1 \otimes v \), is a \( kG^g \)-linear isomorphism. This proves (1) and (2).
The map \( f : M(g, M_g) = \mathbb{k}G \otimes_{\mathbb{k}G^n} M_g \to M, h \otimes m \mapsto h \cdot m \), is a morphism in \( _h\mathcal{YD}(O_g) \). By (2), \( f \) induces an isomorphism 
\[
f_g : M(g, M_g)_g \to M_g
\]
of left \( G^g \)-modules. Hence for all \( h \in G \), \( f \) induces a bijection 
\[
f_{h \cdot g} : M(g, M_g)_{h \cdot g} = hM(g, M_g)_g \to M_{h \cdot g} = h \cdot M_g,
\]
since \( f(h \cdot m) = h \cdot f(m) \) for all \( m \in M(g, M_g)_g \). Thus \( f \) is bijective. \( \square \)

**Proposition 1.4.17.** Let \( g \in G \). Then \( F_g : \mathbb{k}G^n\mathcal{M} \to \mathcal{O}_G\mathcal{YD}(O_g) \) is an equivalence of categories with quasi-inverse functor given by \( M \mapsto M_g \).

**Proof.** Let \( F'_g : \mathcal{O}_G\mathcal{YD}(O_g) \to \mathbb{k}G^n\mathcal{M} \) be the functor given by \( F'_g(M) = M_g \) for all \( M \in \mathcal{O}_G\mathcal{YD}(O_g) \). Since the isomorphisms in Lemma 1.4.16(2) and (3) are natural transformations in \( V \in \mathbb{k}G^n\mathcal{M} \) and in \( M \in \mathcal{O}_G\mathcal{YD}(O_g) \), \( F'_g F_g \cong \text{id} \) and \( F_g F'_g \cong \text{id} \). \( \square \)

We choose for any conjugacy class \( O_l \), \( l \in L \), an element \( g_l \in O_l \). It follows from Proposition 1.4.17 and (1.4.7) that there is a category equivalence

\[
(1.4.9) \quad \prod_{l \in L} \mathbb{k}G^n\mathcal{M} \cong \mathcal{O}_G\mathcal{YD}.
\]

**Corollary 1.4.18.** There is a bijection between the disjoint union of the isomorphism classes of the simple left \( \mathbb{k}G^n \)-modules, \( l \in L \), and the set of isomorphism classes of the simple Yetter-Drinfeld modules in \( \mathcal{O}_G\mathcal{YD} \).

**Proof.** This follows from Proposition 1.4.17 and (1.4.7), where for all \( l \in L \) and all simple left \( \mathbb{k}G^n \)-module \( V_1 \), the isomorphism class of \( V_1 \) is mapped onto the isomorphism class of \( M(g_l, V_1) \). \( \square \)

**Example 1.4.19.** Let \( G = \mathbb{Z} \) and let \( g \) be a generator of \( G \). For any \( \lambda \in \mathbb{k}^* \) and any \( k \geq 2 \), there is a \( \mathbb{k}G \)-module \( V = V(\lambda, k) \) with \( \dim V = k \) such that \( (g - \lambda)^k V = 0, (g - \lambda)^{k-1} V \neq 0 \), and any two such modules are isomorphic. Note that \( V \) is cyclic, indecomposable, and not irreducible as a \( \mathbb{k}G \)-module, since any non-zero submodule of \( V \) contains the one-dimensional eigenspace to the eigenvalue \( \lambda \) of the action of \( g \). Since \( G \) is abelian, \( F_g(V) = V \) as a \( G \)-module and the \( G \)-grading of \( F_g(V) \) is given by \( F_g(V) = F_g(V)_g \). By Proposition 1.4.17, \( F_g(V(\lambda, k)) \in \mathbb{Z}_2\mathcal{YD} \) is an indecomposable but not irreducible Yetter-Drinfeld module.

**Proposition 1.4.20.** Let \( G \) be a finite group, and assume that the characteristic of \( \mathbb{k} \) does not divide the order of \( G \). Then \( \mathcal{O}_G\mathcal{YD} \) is a semisimple category. For any \( M \in \mathcal{O}_G\mathcal{YD} \),
\[
M \cong \bigoplus_{\lambda \in \Lambda} M(g_{\lambda}, V_{\lambda}) \quad \text{in} \quad \mathcal{O}_G\mathcal{YD},
\]
where \( \Lambda \) is an index set, \( g_{\lambda} \in G \), and \( V_{\lambda} \) is a simple left \( \mathbb{k}G^n \)-module for all \( \lambda \in \Lambda \).

**Proof.** Let \( M \in \mathcal{O}_G\mathcal{YD} \). It follows from Proposition 1.4.17 and (1.4.7) that \( M \) is a direct sum of Yetter-Drinfeld modules of the form \( M(g, V) \), where \( g \in G \) and \( V \in \mathbb{k}G^n\mathcal{M} \). By our assumption and the Theorem of Maschke, the group algebra \( \mathbb{k}G^n \) is semisimple. Hence \( V \) is a direct sum of simple left \( \mathbb{k}G^n \)-modules. The functor \( F_g \) commutes with direct sums by the additivity of the tensor product. Hence \( M \) is a direct sum of Yetter-Drinfeld modules of the form \( M(g, V) \), where \( g \in G \) and \( V \) is a simple left \( \mathbb{k}G^n \)-module. This proves the claim by Corollary 1.4.18. \( \square \)
We end the section with an invariant of irreducible Yetter-Drinfeld modules.

**Proposition 1.4.21.** Assume that $k$ is an algebraically closed field. Let $V$ be a finite-dimensional irreducible object in $\mathcal{O}_G^\mathcal{YD}$. Then there exists $q_V \in k^\times$ such that $g \cdot v = q_V v$ for all $g \in G$ and $v \in V_g$.

**Proof.** We may assume that $V \neq 0$. Let $h \in G$ with $V_h \neq 0$. Since $V$ is irreducible, $V \in \mathcal{O}_G^\mathcal{YD}(Q_h)$. Since $V_h$ is finite-dimensional and $k$ is algebraically closed, there exists $q_V \in k^\times$ and $v \in V_h$ with $v \neq 0$, $h \cdot v = q_V v$. Let

$$W = \{w \in V_h \mid h \cdot w = q_V w\}.$$ 

Then $W \in kG^h\mathcal{M}$. Proposition 1.4.17 implies that $kG \cdot W$ is a Yetter-Drinfeld submodule of $V$. Thus $W = V_h$ since $V$ is irreducible and $(kG \cdot W)_h = W$. Finally, for all $g \in G$ and $v \in V_h$,

$$ghg^{-1} \cdot (g \cdot v) = gh \cdot v = q_V g \cdot v$$

which implies the claim. \qed

### 1.5. Braided vector spaces of group type

Let $V$ be a vector space and $c : V \otimes V \to V \otimes V$ a linear endomorphism. For any natural number $n \geq 2$ and $1 \leq i \leq n - 1$ we define $c_i \in \text{End}(V^{\otimes n})$ by applying $c$ at the $i$-th position, that is

$$c_i = \begin{cases} c \otimes \text{id}_{V^{\otimes (n-2)}}, & \text{if } i = 1, \\
\text{id}_{V^{\otimes (i-1)}} \otimes c \otimes \text{id}_{V^{\otimes (n-i-1)}}, & \text{if } 2 \leq i \leq n - 2, \\
\text{id}_{V^{\otimes (n-2)}} \otimes c, & \text{if } i = n - 1. \end{cases}$$

(1.5.1)

Note that $c_i$ depends on $n$. It will be clear from the context which $n$ is meant.

**Definition 1.5.1.** A braided vector space $(V, c)$ is a pair consisting of a vector space $V$ and a linear automorphism $c : V \otimes V \to V \otimes V$ satisfying

$$c_1c_2c_1 = c_2c_1c_2 \quad \text{in } \text{End}(V^{\otimes 3}).$$

If $(V, c)$ is a braided vector space, the automorphism $c$ is called a braiding (or a Yang-Baxter operator). If $(V, c)$ and $(W, d)$ are braided vector spaces, a braided linear map (or a morphism of braided vector spaces) $f : (V, c) \to (W, d)$ is a linear map $f : V \to W$ with $(f \otimes f)c = d(f \otimes f)$.

Clearly, the inverse of a bijective braided linear map is braided linear.

**Corollary 1.5.2.** Let $V \in \mathcal{O}_G^\mathcal{YD}$. Then $(V, c_V, V)$ is a braided vector space.

**Proof.** By (1.4.5), $c_1c_2 = c_{V \otimes V, V}$. Hence we have to show that

$$c_{V \otimes V, V}c_1 = c_2c_{V \otimes V, V}.$$ 

Since $c_1 = c \otimes \text{id}_V$ and $c_2 = \text{id}_V \otimes c$, this follows since by (1.4.3), $c_{V \otimes V, V}$ is a natural transformation with respect to endomorphisms of $V \otimes V$. \qed

**Example 1.5.3.** Assume that $G$ is abelian. If $V \in \mathcal{O}_G^\mathcal{YD}$, and $g \in G$, $\chi \in \hat{G}$, we define

$$V_g^\chi = \{v \in V_g \mid h \cdot v = \chi(h)v\}. $$

(1.5.2)

Then $V_g^\chi \subseteq V$ is a subobject in $\mathcal{O}_G^\mathcal{YD}$. 

An important class of Yetter-Drinfeld modules over $G$ is constructed as follows. Let $I$ be an index set, and $V$ a vector space with basis $x_i$, $i \in I$. For all $i \in I$, let $g_i \in G$, $\chi_i \in \hat{G}$. Then

$$V = \bigoplus_{i \in I} \mathbb{k} x_i \in \hat{G} \mathcal{YD}, \quad \text{where } \mathbb{k} x_i \in V_{g_i}^{\chi_i} \text{ for all } i \in I.$$  

By Definition 1.4.10, the braiding $c_{V,V}$ is given by

$$c_{V,V}(x_i \otimes x_j) = q_{ij} x_j \otimes x_i, \quad q_{ij} = \chi_j(g_i) \quad \text{for all } i, j \in I.$$  

**Remark 1.5.4.** Let $I$ be an index set, and let $(q_{ij})_{i,j \in I}$ be a family of non-zero scalars in $\mathbb{k}$. Let $V$ be a vector space with basis $x_i$, $i \in I$. We define a linear map $c : V \otimes V \to V \otimes V$ by

$$c(x_i \otimes x_j) = q_{ij} x_j \otimes x_i \quad \text{for all } i, j \in I.$$  

Then $c$ is a linear automorphism of $V \otimes V$, and for all $i, j, k \in I$,

$$c_1 c_2 c_1(x_i \otimes x_j \otimes x_k) = q_{ij} q_{ik} q_{jk} x_j \otimes x_k \otimes x_i,$$

$$c_2 c_1 c_2(x_i \otimes x_j \otimes x_k) = q_{jk} q_{ik} q_{ij} x_k \otimes x_j \otimes x_i.$$  

Thus $(V, c)$ always is a braided vector space. One says that $(V, c)$ is a braided vector space of **diagonal type**, and that $c$ is a diagonal braiding. The matrix $(q_{ij})_{i,j \in I}$ is called the braiding matrix of $(V, c)$ with respect to the basis $x_i$, $i \in I$.

The braiding of a braided vector space $(V, c)$ of diagonal type can be realized as the braiding of a Yetter-Drinfeld module over an abelian group. For example, let $G$ be a free abelian group with basis $g_i$, $i \in I$. Define characters $\chi_i \in \hat{G}$ by $\chi_j(g_i) = q_{ij}$ for all $i, j \in I$. Then $V \in \hat{G} \mathcal{YD}$ by (1.5.3) and $c_{V,V} = c$ by (1.5.4).

The following class of braided vector spaces was introduced by Takeuchi to characterize braiding of Yetter-Drinfeld modules over groups.

**Definition 1.5.5.** Let $(V, c)$ be a braided vector space. We call $(V, c)$ of **group type** if there are a basis $(x_i)_{i \in I}$ of $V$ and elements $g_i(x_j) \in V$ for all $i, j \in I$ such that

$$c(x_i \otimes x_j) = g_i(x_j) \otimes x_i \quad \text{for all } i, j \in I.$$  

Note that it follows from the bijectivity of $c$, that the family of elements $g_i(x_j)$, $i, j \in I$, defines linear automorphisms $g_i \in \text{Aut}(V)$ for all $i \in I$.

**Proposition 1.5.6.** Let $(V, c)$ be a braided vector space. Then the following are equivalent:

1. $(V, c)$ is of group type.
2. There are a group $G$ and a $kG$-module and a $kG$-comodule structure on $V$ such that $V \in \hat{G} \mathcal{YD}$ and $c = c_{V,V}$.

**Proof.** We prove first that (1) implies (2). Let $(x_i)_{i \in I}$ be a basis of $V$ and let $(g_i)_{i \in I}$ be a family of linear automorphisms of $V$ satisfying (1.5.6). For all $i, j, k \in I$ we compute

$$c_1 c_2 c_1(x_i \otimes x_j \otimes x_k) = c(g_i(x_j) \otimes g_i(x_k)) \otimes x_i,$$

$$c_2 c_1 c_2(x_i \otimes x_j \otimes x_k) = g_i g_j(x_k) \otimes g_i(x_j) \otimes x_i.$$  

Since $(V, c)$ is a braided vector space, we obtain that

$$c(g_i(x_j) \otimes g_i(x_k)) = g_i g_j(x_k) \otimes g_i(x_j) \quad \text{for all } i, j, k \in I.$$
Let \( G \subseteq \text{Aut}(V) \) be the subgroup generated by the automorphisms \( g_i, i \in I \). Hence \( V \) is a \( G \)-module. We define a \( G \)-grading on \( V \) by

\[
\deg(x_i) = g_i \quad \text{for all} \quad i \in I.
\]

Then \( V \) is a Yetter-Drinfeld module over \( G \) if

\[
g_i(x_j) = V_{g_i g_j g_i^{-1}} \quad \text{for all} \quad i, j \in I.
\]

(1.5.8)

Let \( i, j \in I \), and write \( g_i(x_j) = \sum_{l \in I'} \alpha_{ij}^l x_l \), where \( I' \subseteq I \) is a non-empty finite subset, and \( 0 \neq \alpha_{ij}^l \in \mathbb{k} \) for all \( l \in I' \). Then for all \( k \in I \),

\[
c(g_i(x_j) \otimes g_i(x_k)) = c\left( \sum_{l \in I'} \alpha_{ij}^l x_l \otimes g_i(x_k) \right) = \sum_{l \in I'} \alpha_{ij}^l g_i(x_k) \otimes x_l.
\]

Hence by (1.5.7), \( g_l g_i(x_k) = g_i g_j(x_k) \) for all \( k \in I \), \( l \in I' \). Thus for all \( l \in I' \), \( g_l = g_i g_j g_i^{-1} \), and \( g_i(x_j) \in V_{g_i g_j g_i^{-1}} \).

The equality \( c = c_{V,V} \) is clear from the definition of \( V \in \mathcal{O}_G YD \).

Now we prove that (2) implies (1). Let \( G \) be a group and let \( V \in \mathcal{O}_G YD \) be such that \( c = c_{V,V} \). Choose a basis \( (x_i)_{i \in I} \) of \( V \) of \( G \)-homogeneous elements, that is, with \( x_i \in V_{g_i} \) for all \( i \in I \), where \( g_i \in G \) for all \( i \in I \). Then

\[
c(x_i \otimes x_j) = g_i \cdot x_j \otimes x_i
\]

for all \( i, j \in I \) by Definition 1.4.10. This proves (1). \( \square \)

In order to describe braided vector spaces of group type without referring to the group, the notions of racks and two-cocycles are very useful.

**Definition 1.5.7.** Let \( X \) be a non-empty set and \( \triangleright : X \times X \to X \) a map denoted by \( (x, y) \mapsto x \triangleright y \) for all \( x, y \in X \). The pair \( (X, \triangleright) \) is called a **rack** if

1. For all \( x \in X \), the map \( \varphi_x : X \to X \), \( y \mapsto x \triangleright y \), is bijective.
2. The map \( \triangleright \) is left self-distributive, that is, for all \( x, y, z \in X \),

\[
x \triangleright (y \triangleright z) = (x \triangleright y) \triangleright (x \triangleright z).
\]

A rack \( (X, \triangleright) \) is called a **quandle** if \( x \triangleright x = x \) for all \( x \in X \). Two racks (or quandles) \( (X, \triangleright) \) and \( (Y, \triangleright') \) are called **isomorphic** if there is a bijection \( f : X \to Y \) such that \( f(x \triangleright z) = f(x) \triangleright' f(z) \) for all \( x, z \in X \).

**Example 1.5.8.** Let \( G \) be a group. The union \( X \) of any non-empty set of conjugacy classes of \( G \) is a quandle, where \( x \triangleright y = x y x^{-1} \) for all \( x, y \in X \) is the adjoint action of the group. The pair \( (G, \triangleright) \) with \( g \triangleright h = g h^{-1} g \) for all \( g, h \in G \) is a quandle.

**Example 1.5.9.** Let \( A \) be an abelian group. Let \( \sigma \) be an automorphism of \( A \) and let \( \triangleright : A \times A \to A \), \( x \triangleright y = x + \sigma(y - x) \). Then \( (A, \triangleright) \) is a quandle and is called an **affine rack** or **affine quandle**. Indeed, for any \( x \in A \) the inverse of \( \varphi_x \) is given by

\[
\varphi_x^{-1}(y) = x + \sigma^{-1}(y - x).
\]

Moreover,

\[
\varphi_x \varphi_y(z) = \varphi_x(y + \sigma(z - y)) = x + \sigma(y - x) + \sigma^2(z - y) = \varphi_{x \triangleright y} \varphi_x(z)
\]

for all \( x, y, z \in A \).
Example 1.5.10. Let $G$ be a group, $g \in G$ and $V$ a left $kG^g$-module. As in the proof of Lemma 1.4.16, let $(h_x)_{x \in X}$ be a complete set of representatives of $G/G^g$. For all $x, y \in X$, define $x \triangleright y \in X$ and $u(x, y) \in G^g$ by the equation
\[
(h_x \triangleright g)h_y = h_{x \triangleright y}u(x, y).
\]
Then $(X, \triangleright)$ is a rack.

Condition (1) of Definition 1.5.7 clearly holds, since $G/G^g$ is a left $G$-space, and left multiplication with $h_x \triangleright g$ is bijective. To check (2), let $x, y, z \in X$. By definition,
\[
(h_x \triangleright g)h_z = h_{x \triangleright z}u(x, z), \quad (h_x \triangleright g)h_{y \triangleright z} = h_{x \triangleright (y \triangleright z)}u(x, y \triangleright z),
\]
\[
(h_y \triangleright g)h_z = h_{y \triangleright z}u(y, z), \quad (h_{x \triangleright y} \triangleright g)h_z = h_{(x \triangleright y) \triangleright z}u(x \triangleright y, x \triangleright z).
\]
Hence
\[
h_{x \triangleright (y \triangleright z)}u(x, y \triangleright z) = (h_x \triangleright g)(h_y \triangleright g)h_z,
\]
\[
h_{(x \triangleright y) \triangleright z}u(x \triangleright y, x \triangleright z) = (h_{x \triangleright y} \triangleright g)(h_x \triangleright g)h_z
\]
\[
= (((h_x \triangleright g)h_yu(x, y)^{-1}) \triangleright g)(h_x \triangleright g)h_z
\]
\[
= (h_x \triangleright g)(h_y \triangleright g)h_z,
\]
where the last equality holds since $u(x, y) \in G^g$. This proves (2). Moreover,
\[
(1.5.9) \quad u(x \triangleright y, x \triangleright z)u(x, z) = u(x, y \triangleright z)u(y, z)
\]
for all $x, y, z \in X$.

The braiding of $M(g, V) = kG \otimes_{kG^g} V$ can hence be written as
\[
c(h_x \otimes v, h_y \otimes w) = (h_x \triangleright g)h_y \otimes w \otimes h_x \otimes v
\]
\[
= h_{x \triangleright y} \otimes u(x, y) \cdot w \otimes h_x \otimes v
\]
\[
= h_{x \triangleright y} \otimes q_{x,y}(w) \otimes h_x \otimes v
\]
for all $x, y \in X$, $v, w \in V$, where $q_{x,y} \in \text{Aut}(V)$, $q_{x,y}(w) = u(x, y) \cdot w$ for all $w \in V$.

The braiding in Example 1.5.10 can easily be formulated for any rack.

Definition 1.5.11. Let $(X, \triangleright)$ be a rack, and let $q : X \times X \to H$ for some group $H$ be a map which we write as $q(x, y) = q_{x,y}$ for all $x, y \in X$. Then $q$ is called a two-cocycle if
\[
(1.5.10) \quad q_{x \triangleright y, x \triangleright z}q_{x,z} = q_{x,y \triangleright z}q_{y,z}
\]
for all $x, y, z \in X$. We say that $q$ is constant if $H = \text{Aut}(V)$ for some vector space $V$ and there exists $\lambda \in k$ such that $q_{x,y} = \lambda \text{id}_V$ for all $x, y \in X$.

A constant map $q : X \times X \to \text{Aut}(V)$ is always a two-cocycle. The map $u$ in Example 1.5.10 is a two-cocycle with values in $G^g$ by (1.5.9).

Proposition 1.5.12. Let $X$ be a non-empty set, $V$ be a vector space, and $\triangleright : X \times X \to X$, $q : X \times X \to \text{Aut}(V)$ be maps. Let $M = kX \otimes V$ and let $c^q : M \otimes M \to M \otimes M$ be the linear map with
\[
(1.5.11) \quad c^q((x \otimes v) \otimes (y \otimes w)) = ((x \triangleright y) \otimes q_{x,y}(w)) \otimes (x \otimes v)
\]
for all $x, y \in X$, $v, w \in V$. Then $(M, c^q)$ is a braided vector space if and only if $(X, \triangleright)$ is a rack and $q$ is a two-cocycle. In this case, $(M, c^q)$ is of group type.
PROOF. In the proof we write \( xv \) instead of \( x \otimes v \) for all \( x \in X, \, v \in V \). Let \( x, y, z \in X \) and \( v, w, u \in V \). Then
\[
c_1 c_2 (xv \otimes yw \otimes zu) = (x \triangleright y) \triangleright (x \triangleright z) q_{x \triangleright y, x \triangleright z} (q_{x, z}(u)) \otimes (x \triangleright y) q_{x, y}(w) \otimes xv,
\]
\[
c_2 c_1 (xv \otimes yw \otimes zu) = (x \triangleright y \triangleright z) q_{x \triangleright y \triangleright z} (q_{y, z}(u)) \otimes (x \triangleright y) q_{x, y}(w) \otimes xv.
\]
This implies the first part of the claim. The rest is clear. \( \square \)

Example 1.5.13. Let \( X = \{1, 2, 3, 4\} \) and let \( \varphi_i, \, i \in X, \) be the permutations
\[
\varphi_1 = (2 \, 3 \, 4), \quad \varphi_2 = (1 \, 4 \, 3), \quad \varphi_3 = (1 \, 2 \, 4), \quad \varphi_4 = (1 \, 3 \, 2).
\]
Then \( (X, \triangleright) \) is a quandle, where \( x \triangleright y = \varphi_x(y) \) for all \( x, y \in X \). More precisely, consider the affine quandle structure on the field \( \mathbb{F}_4 \) with 4 elements and the auto-
morphism determined by left multiplication with an element of multiplicative order 3 in \( \mathbb{F}_4 \). This quandle and \( (X, \triangleright) \) are isomorphic.

Let \( V \) be a one-dimensional vector space, \( (X, \triangleright) \) a rack, \( M = kX \otimes V \cong kX \), and let \( c^q \) be as in Proposition 1.5.12, where \( \lambda \in k^\times \) and \( q \) is the constant two-cocycle with \( q_{x, y} = \lambda \) for all \( x, y \in X \). Then
\[
c^q(x \otimes y) = \lambda(x \triangleright y) \otimes x
\]
for all \( x, y \in X \).

Example 1.5.14. Let \( m \geq 2 \) be a positive integer and let \( 1 \leq i < m \) with \( \gcd(m, i) = 1 \). Multiplication with \( i \) in \( \mathbb{Z}/(m) \) is an automorphism. Hence
\[
\text{Aff}(m, i) = (\mathbb{Z}/(m), \triangleright), \quad x \triangleright y = x + i(y - x),
\]
is an affine quandle. For \( i = 1, \) \( x \triangleright y = y \) for all \( x, y \in \mathbb{Z}/(m) \).

1.6. Braided Hopf algebras and Nichols algebras over groups

Let again \( G \) be a group. To simplify the notation, we write \( C = YD_Y \).

The tensor product of two objects in \( C \) is an object in \( C \), the tensor product of two morphisms in \( C \) is a morphism in \( C \), and the canonical isomorphisms in Proposition 1.2.5 for \( U, V, W \in C \) are morphisms in \( C \) by Proposition 1.4.9.

Let \( A \in C \), and let \( \mu : A \otimes A \to A, \, \eta : k \to A \) be morphisms in \( C \). Then \( (A, \mu, \eta) \) is an algebra in \( C \) if the diagrams (1.1.3) and (1.1.4) commute. If \( A, B \) are algebras in \( C \), and \( \rho : A \to B \) is a morphism in \( C \), then \( \rho \) is a morphism of algebras in \( C \), if the diagrams (1.1.5) and (1.1.6) commute.

Let \( C \in C \), and let \( \Delta : C \to C \otimes C, \, \varepsilon : C \to k \) be morphisms in \( C \). The triple \( (C, \Delta, \varepsilon) \) is a coalgebra in \( C \) if the diagrams (1.1.7) and (1.1.8) commute. If \( C, D \) are coalgebras in \( C \), and \( \varphi : C \to D \) is a morphism in \( C \), then \( \varphi \) is a morphism of coalgebras in \( C \), if the diagrams (1.1.10) and (1.1.11) commute.

Thus algebras and coalgebras in \( C \) are algebras and coalgebras in the sense of Section 1.1 whose structure maps are morphisms in \( C \). In the same way modules in \( C \) and comodules in \( C \) are modules and comodules, respectively, whose structure maps are morphisms in \( C \).

Corollary 1.6.1. Let \( C \) be a coalgebra in \( C \), \( A \) an algebra in \( C \), and \( f \) an invertible map in Hom\( (C, A) \). If \( f \) is a morphism in \( C \), then so is \( f^{-1} \).

Proof. This is another application of Proposition 1.2.11. \( \square \)

Proposition 1.6.2. Let \( V \in C \), and \( T(V) = \bigoplus_{n \geq 0} T^n(V) \) the tensor algebra of the vector space \( V \).
(1) \(T(V)\) is an algebra in \(\mathcal{C}\), where \(T^n(V) = V^\otimes n, \ n \geq 0\), is the \(n\)-fold tensor product in \(\mathcal{C}\).

(2) For any algebra \(A\) in \(\mathcal{C}\) and any morphism \(f : V \to A\) in \(\mathcal{C}\), there is exactly one algebra morphism \(\varphi : T(V) \to A\) in \(\mathcal{C}\) extending \(f\).

**Proof.** This is clear from the universal property of the tensor algebra (or the free algebra), since for all \(n \geq 2\), \(V^\otimes n \xrightarrow{f^\otimes n} A^\otimes n \xrightarrow{\mu^{n-1}} A\) is a morphism in \(\mathcal{C}\), where \(\mu^{n-1}\) is the \((n-1)\)-fold iteration of the multiplication map \(\mu\).

**Definition 1.6.3.** (1) Let \((A, \mu_A, \eta_A)\) and \((B, \mu_B, \eta_B)\) be algebras in \(\mathcal{C}\). Define \(\mu_{A \otimes B}\) and \(\eta_{A \otimes B}\) by

\[
(A \otimes B) \otimes (A \otimes B) \xrightarrow{\text{id} \otimes \text{id}} (A \otimes A) \otimes (B \otimes B) \xrightarrow{\mu_A \otimes \mu_B} A \otimes B,
\]

\[k \cong k \otimes k \xrightarrow{\eta_A \otimes \eta_B} A \otimes B.
\]

Then \((A \otimes B, \mu_{A \otimes B}, \eta_{A \otimes B})\) is called the **tensor product of algebras** in \(\mathcal{C}\).

(2) Let \((C, \Delta_C, \varepsilon_C)\) and \((D, \Delta_D, \varepsilon_D)\) be coalgebras in \(\mathcal{C}\). Define \(\Delta_{C \otimes D}\) and \(\varepsilon_{C \otimes D}\) by

\[
C \otimes D \xrightarrow{\Delta_C \otimes \Delta_D} (C \otimes C) \otimes (D \otimes D) \xrightarrow{\text{id} \otimes \text{id}} (C \otimes D) \otimes (C \otimes D),
\]

\[C \otimes D \xrightarrow{\varepsilon_C \otimes \varepsilon_D} k \otimes k \cong k.
\]

Then \((C \otimes D, \Delta_{C \otimes D}, \varepsilon_{C \otimes D})\) is called the **tensor product of coalgebras** in \(\mathcal{C}\).

By Definition 1.4.10, the product \(\mu_{A \otimes B}\) is defined for elements \(a, x \in A\) and \(b, y \in B\), \(g \in G\), by

\[a \otimes b)(x \otimes y) = a(g \cdot x) \otimes by.
\]

The unit element of \(A \otimes B\) is \(1_A \otimes 1_B\).

**Proposition 1.6.4.** Let \(A, B, C, D\) be algebras in \(\mathcal{C}\).

(1) \((A \otimes B, \mu_{A \otimes B}, \eta_{A \otimes B})\) is an algebra in \(\mathcal{C}\).

(2) The canonical isomorphism \((A \otimes B) \otimes C \cong A \otimes (B \otimes C)\) is an isomorphism of algebras in \(\mathcal{C}\).

(3) Let \(\varphi : A \to C\) and \(\psi : B \to D\) be morphisms of algebras in \(\mathcal{C}\). Then \(\varphi \otimes \psi : A \otimes B \to C \otimes D\) is a morphism of algebras in \(\mathcal{C}\).

**Proof.** (1) It is clear from the definition that \(\mu_{A \otimes B}\) and \(\eta_{A \otimes B}\) are morphisms in \(\mathcal{C}\). To check associativity, consider elements \(a, u, x \in A\) and \(b, v \in B\), \(g, h \in G\). Then \(\deg(bv) = gh\), since the multiplication map \(B \otimes B \to B\) is \(G\)-graded. Hence

\[
((a \otimes b)(u \otimes v))(x \otimes y) = (a(g \cdot u) \otimes bv)(x \otimes y) = a(g \cdot u)((gh) \cdot x) \otimes by,
\]

\[(a \otimes b)((u \otimes v)(x \otimes y)) = (a \otimes b)(u(h \cdot x) \otimes vy) = a(g \cdot (u(h \cdot x))) \otimes by.
\]

This proves associativity, since the multiplication map \(A \otimes A \to A\) is left \(G\)-linear, hence \((g \cdot u)((gh) \cdot x) = g \cdot (u(h \cdot x))\).
(2) Let \(a, x \in A, b \in B_g, y \in B, c \in C_h, z \in C\), where \(g, h \in G\). We compute in \(A \otimes (B \otimes C)\) and then in \((A \otimes B) \otimes C\),
\[
(a \otimes (b \otimes c))(x \otimes (y \otimes z)) = a((gh) \cdot x) \otimes (b \otimes c)(y \otimes z) \\
= a((gh) \cdot x) \otimes b(h \cdot y) \otimes cz, \\
((a \otimes b) \otimes c)((x \otimes y) \otimes z) = (a \otimes b)(h \cdot x \otimes h \cdot y) \otimes cz \\
= a((gh) \cdot x) \otimes b(h \cdot y) \otimes cz.
\]
(3) Let \(a, u \in A, b, v \in B\), and assume that \(b \in B_g, g \in G\). Then
\[
(\varphi \otimes \psi)((a \otimes b)(u \otimes v)) = \varphi(a(g \cdot u)) \otimes \psi(bv) \\
= \varphi(a(g \cdot \varphi(u)) \otimes \psi(b)\psi(v) \\
= (\varphi(a) \otimes \psi(b))(\varphi(u) \otimes \psi(v)).
\]
This implies the claim. \(\square\)

**Proposition 1.6.5.** Let \(C, D, E, F\) be coalgebras in \(\mathcal{C}\).

1. \((C \otimes D, \Delta_{C \otimes D}, \varepsilon_{C \otimes D})\) is a coalgebra in \(\mathcal{C}\).
2. The canonical isomorphism \((C \otimes D) \otimes \mathcal{E} \cong C \otimes (D \otimes \mathcal{E})\) is an isomorphism of coalgebras in \(\mathcal{C}\).
3. Let \(\varphi : C \to E\) and \(\psi : D \to F\) be morphisms of coalgebras in \(\mathcal{C}\). Then \(\varphi \otimes \psi : C \otimes D \to E \otimes F\) is a morphism of coalgebras in \(\mathcal{C}\).

**Proof.** This can be shown as in the proof of Proposition 1.6.4 by direct computation using the comodule description of Yetter-Drinfeld modules in Remark 1.4.8. \(\square\)

We will see in Section 3.2 that Propositions 1.6.4 and 1.6.5 formally follow from the properties of the braiding in Proposition 1.4.11. Proposition 1.6.4 holds in braided monoidal categories, and Proposition 1.6.5 is Proposition 1.6.4 in the dual category.

**Definition 1.6.6.** (1) Let \(R\) be an object in \(\mathcal{C}\), and let \(\mu : R \otimes R \to R, \eta : \mathbb{k} \to R, \Delta : R \to R \otimes R, \varepsilon : R \to \mathbb{k}\) be morphisms in \(\mathcal{C}\). Then \((R, \mu, \eta, \Delta, \varepsilon)\) is a bialgebra in \(\mathcal{C}\) if \((R, \mu, \eta)\) is an algebra in \(\mathcal{C}\), \((R, \Delta, \varepsilon)\) is a coalgebra in \(\mathcal{C}\), and \(\Delta\) and \(\varepsilon\) are algebra maps in \(\mathcal{C}\).

(2) Let \(R\) be a bialgebra in \(\mathcal{C}\), and \(S : R \to R\) a morphism in \(\mathcal{C}\). Then \((R, S)\) is a Hopf algebra in \(\mathcal{C}\) with antipode \(S\), if the diagrams (1.2.2) commute.

(3) Let \(R, R'\) be bialgebras in \(\mathcal{C}\), and \(\varphi : R \to R'\) a morphism in \(\mathcal{C}\). Then \(\varphi\) is a bialgebra morphism in \(\mathcal{C}\), if \(\varphi\) is a morphism of algebras and coalgebras in \(\mathcal{C}\). A Hopf algebra morphism in \(\mathcal{C}\) between Hopf algebras in \(\mathcal{C}\) is a bialgebra morphism in \(\mathcal{C}\).

**Proposition 1.6.7.** Let \(R\) be an object in \(\mathcal{C}\), and let \(\mu : R \otimes R \to R, \eta : \mathbb{k} \to R, \Delta : R \to R \otimes R, \varepsilon : R \to \mathbb{k}\) be morphisms in \(\mathcal{C}\). Assume that \((R, \mu, \eta)\) is an algebra and \((R, \Delta, \varepsilon)\) is a coalgebra in \(\mathcal{C}\). Then the following are equivalent.

1. \(\Delta\) and \(\varepsilon\) are morphisms of algebras in \(\mathcal{C}\).
2. \(\mu\) and \(\eta\) are morphisms of coalgebras in \(\mathcal{C}\).
Proof. Replace in the proof of Proposition 1.2.2 the flip map $\tau_{R,R}$ by the braiding $c_{R,R}$. \hfill \Box

Remark 1.6.8. (1) Let $(R, S)$ be a Hopf algebra in $C$. Then $S$ is uniquely determined as the inverse of id in $\text{Hom}(R, R)$.

(2) If $R$ is a bialgebra in $C$, and the inverse $S$ of id in $\text{Hom}(R, R)$ exists, then $S$ is a morphism in $C$ by Corollary 1.6.1, hence $(R, S)$ is a Hopf algebra in $C$.

(3) Let $R, R'$ be Hopf algebras in $C$ and $\varphi : R \to R'$ a bialgebra morphism in $C$. Then $\varphi S_R = S_{R'} \varphi$ by the proof of Proposition 1.2.17(2).

Lemma 1.6.9. Let $R$ be a bialgebra in $C$. Then $P(R) \subseteq R$ is a subobject in $C$.

Proof. By definition, $P(R)$ is the kernel of the morphism

$$R \to R \otimes R, \quad x \mapsto \Delta(x) - (x \otimes 1 + 1 \otimes x)$$

in $C$. This implies the claim. \hfill \Box

An $\mathbb{N}_0$-graded object in $C$ is an object $V \in C$ with a family of subobjects $V(n) \subseteq V$, $n \geq 0$, in $C$ such that $V = \bigoplus_{n \geq 0} V(n)$ in $C$. The category of $\mathbb{N}_0$-graded objects in $C$ with graded morphisms in $C$ as morphisms is denoted by $\mathbb{N}_0$-$\text{Gr}(C)$.

An $\mathbb{N}_0$-graded algebra, coalgebra, bialgebra and Hopf algebra in $C$ is an algebra, coalgebra, bialgebra and Hopf algebra, respectively, in $C$ with an $\mathbb{N}_0$-grading of subobjects in $C$ such that the structure maps are graded.

For $V \in C$, the tensor algebra $T(V)$ is an algebra in $C$ by Proposition 1.6.2. The usual $\mathbb{N}_0$-grading with $T(V)(n) = T^n(V) = V^\otimes n$ for all $n \geq 0$ turns $T(V)$ into an $\mathbb{N}_0$-graded algebra in $C$ by construction.

Corollary 1.6.10. Let $R$ be an $\mathbb{N}_0$-graded connected bialgebra in $C$. Then $R$ is an $\mathbb{N}_0$-graded Hopf algebra in $C$.

Proof. Since $R$ is an algebra and a coalgebra, $\text{Hom}(R, R)$ is an algebra with convolution product. The identity map in $\text{Hom}(R, R)$ is invertible by Proposition 1.3.5. Hence the claim follows from Remark 1.6.8. \hfill \Box

Definition 1.6.11. Let $V \in C$, and $T(V)$ the tensor algebra of $V$ in $C$. By Proposition 1.6.2, there are uniquely determined algebra morphisms in $C$

$$\Delta : T(V) \to T(V) \otimes T(V), \quad \varepsilon : T(V) \to \mathbb{k}$$

such that

$$\Delta(v) = v \otimes 1 + 1 \otimes v, \quad \varepsilon(v) = 0$$

for all $v \in V$, where $T(V) \otimes T(V)$ is the tensor product of algebras in $C$.

Example 1.6.12. Let $V = \bigoplus_{i \in J} \mathbb{k} x_i \in \mathbb{C}_G \mathcal{Y}$, where $x_i \in V_{g_i^x}$, $x_j(g_i) = q_{ij}$ for all $i, j \in I$. Then in $T(V)$ for all $i, j \in I$,

$$\Delta(x_i x_j) = (x_i \otimes 1 + 1 \otimes x_i)(x_j \otimes 1 + 1 \otimes x_j)$$

$$= x_i x_j \otimes 1 + x_i \otimes x_j + q_{ij} x_j \otimes x_i + 1 \otimes x_i x_j.$$

Proposition 1.6.13. Let $V \in C$.

(1) The tensor algebra $T(V)$ is an $\mathbb{N}_0$-graded Hopf algebra in $C$ with comultiplication $\Delta$ and counit $\varepsilon$ of Definition 1.6.11.

(2) Let $R$ be a bialgebra in $C$, and $f : V \to P(R)$ a morphism in $C$. Then there is exactly one bialgebra map $\varphi : T(V) \to R$ in $C$ extending $f$. 

(3) Let $R$ be an $\mathbb{N}_0$-graded connected bialgebra in $C$, and $f : V \to R(1)$ a morphism in $C$. Then there is exactly one bialgebra map $\varphi : T(V) \to R$ in $C$ extending $f$, and $\varphi$ is $\mathbb{N}_0$-graded.

**Proof.** (1) Since $\Delta$ and $\varepsilon$ are homogeneous on $V$, they are $\mathbb{N}_0$-graded algebra morphisms in $C$. Then $(T(V), \Delta, \varepsilon)$ is an $\mathbb{N}_0$-graded coalgebra in $C$, since by Proposition 1.6.4(2), the diagrams (1.1.7) and (1.1.8) are diagrams of algebra morphisms which commute on the generators $v \in V$. Thus $T(V)$ is an $\mathbb{N}_0$-graded bialgebra in $C$. Then $T(V)$ is a Hopf algebra in $C$ by Corollary 1.6.10.

(2) By Proposition 1.6.2, there is a unique algebra map $\varphi : T(V) \to R$ in $C$ extending $f : V \to R$. It remains to show that $\varphi$ is a coalgebra map, that is, the diagrams

\[
\begin{array}{ccc}
T(V) & \xrightarrow{\varphi} & R \\
\downarrow \Delta & & \downarrow \Delta \\
T(V) \otimes T(V) & \xrightarrow{\varphi \otimes \varphi} & R \otimes R
\end{array}
\]

commute. All maps in the diagrams are algebra maps, and it is enough to prove commutativity on the generators in $V$. It is clear from the assumption on $f$ that both diagrams commute on elements of $V$.

(3) This follows from (2), since $R(1) \subseteq P(R)$ by Lemma 1.3.6(2). □

**Ideals, coideals, bi-ideals and Hopf ideals in $C$** are subobjects in $C$ which are ideals, coideals, bi-ideals and Hopf ideals, respectively. They describe quotients of algebras, coalgebras, bialgebras and Hopf algebras in $C$ as in Propositions 1.1.13 and 1.2.22.

**Lemma 1.6.14.** Let $A$ be a bialgebra in $C$, and $I \subseteq A$ a coideal in $C$. Then $AI$ and $IA$ are coideals of $A$ in $C$.

**Proof.** Since the multiplication map $A \otimes A \to A$ is a morphism in $C$, $AI$ is a subobject of $A$ in $C$. Since $\varepsilon$ is an algebra map, $\varepsilon(AI) \subseteq \varepsilon(A)\varepsilon(I) = 0$. Since $\Delta$ is an algebra map,

\[
\Delta(AI) \subseteq \Delta(A)\Delta(I) \subseteq (A \otimes A)(I \otimes A + A \otimes I)
\]

\[
= Ac(A \otimes I)A + Ac(A \otimes A)I = AI \otimes A + A \otimes AI.
\]

Hence $AI$ is a coideal of $A$ in $C$. Similarly, $IA \subseteq A$ is a coideal of $A$ in $C$. □

**Corollary 1.6.15.** Let $R = \bigoplus_{n \geq 0} R(n)$ be an $\mathbb{N}_0$-graded connected Hopf algebra in $C$, and let $I_R \subseteq R$ be the largest coideal contained in $\bigoplus_{n \geq 2} R(n)$. Then $R/I_R$ is an $\mathbb{N}_0$-graded connected quotient Hopf algebra in $C$ with

\[
P(R/I_R) = (R/I_R)(1) \cong R(1).
\]

**Proof.** By Theorem 1.3.16, $I_R = \bigoplus_{n \geq 2} \ker(\Delta_1^n)$, and $R/I_R$ is strictly graded, that is, $P(R/I_R) = (R/I_R)(1) \cong R(1)$. For all $n \geq 2$, the maps $\Delta_1^n$ are $\mathbb{N}_0$-graded morphisms in $C$. Hence $I_R \subseteq R$ is an $\mathbb{N}_0$-graded subobject in $C$, and $R/I_R$ is an $\mathbb{N}_0$-graded coalgebra quotient of $R$ in $C$. By the maximality of $I_R$ and by Lemma 1.6.14, $I_R$ is a bi-ideal of $R$. Then $R/I_R$ is an $\mathbb{N}_0$-graded Hopf algebra in $C$ by Corollary 1.6.10. □
**Definition 1.6.16.** Let $V \in C$. An $\mathbb{N}_0$-graded connected Hopf algebra $R$ in $C$ is a **pre-Nichols algebra of** $V$, if

(N1) $R(1) \cong V$ in $C$,
(N2) $R$ is generated as an algebra by $R(1)$.

A pre-Nichols algebra of $V$ is a **Nichols algebra of** $V$, if

(N3) $R$ is strictly graded, that is, $P(R) = R(1)$.

It is a remarkable fact that by Theorem 1.6.18 below the structure of a Nichols algebra of $V \in C$ is completely determined by $V$. This is somewhat similar to the situation of irreducible cocommutative Hopf algebras $U$ over a field of characteristic 0. The structure of $U$ is completely determined by the Lie algebra of its primitive elements. In this analogy, the Nichols algebra corresponds to the universal enveloping algebra of a Lie algebra.

The Nichols algebra can be constructed as the smallest $\mathbb{N}_0$-graded Hopf algebra quotient of $T(V)$ which is isomorphic to $V$ in degree one. Recall from Proposition 1.6.13 that $T(V)$ is an $\mathbb{N}_0$-graded connected coalgebra.

**Definition 1.6.17.** Let $V \in C$. Let $I(V)$ be the largest coideal of $T(V)$ contained in $\bigoplus_{n \geq 2} T^n(V)$. The **Nichols algebra of** $V$ is defined by

$$B(V) = T(V)/I(V).$$

Note that $I(V) = \bigoplus_{n \geq 2} \ker(\Delta^T_{1n}(V)) = I_{T(V)}$ by Theorem 1.3.16.

**Theorem 1.6.18.** Let $V \in C$.

(1) $B(V)$ is a Nichols algebra of $V$.

(2) Let $R$ be a pre-Nichols algebra of $V$, $f : R(1) \xrightarrow{\cong} V$ an isomorphism in $C$.

(a) There is exactly one morphism $\pi : R \to B(V)$ of $\mathbb{N}_0$-graded Hopf algebras in $C$ such that $f$ is the restriction of $\pi$ to $R(1)$, and $\pi$ is surjective.

(b) $\pi$ is bijective if and only if $R$ is a Nichols algebra of $V$.

**Proof.** (1) follows from Corollary 1.6.15.

(2) (a) Let $\varphi : T(V) \to R$ be the surjective $\mathbb{N}_0$-graded braided bialgebra map extending $f^{-1}$ by Proposition 1.6.13(3). Then $\ker(\varphi) \subseteq I(V)$, since $\varphi$ is bijective in degree 0 and 1. The induced map

$$\pi : R \cong T(V)/\ker(\varphi) \to T(V)/I(V) = B(V)$$

is a surjective map of $\mathbb{N}_0$-graded braided Hopf algebras with $\pi(1) = f$.

(b) If $P(R) = R(1)$, then $\pi$ in (1) is bijective by Proposition 1.3.10(2). Conversely, if $R \cong B(V)$, then $P(R) = R(1)$ by (1). \hfill $\square$

**Remark 1.6.19.** Let $U, V \in C$, and $f : U \to V$ a morphism in $C$. Then $f$ induces a morphism $T(f) : T(U) \to T(V)$ of $\mathbb{N}_0$-graded Hopf algebras in $C$. Since $T(f)$ is a coalgebra morphism, $T(f)(I(U)) \subseteq I(V)$. Hence the construction of the Nichols algebra is a functor from $C$ to the category of $\mathbb{N}_0$-graded Hopf algebras in $C$. Clearly, $f$ is surjective if and only if $B(f)$ is surjective.

Suppose that $f$ is injective. Then $T(f)^{-1}(I(V)) \subseteq \bigoplus_{n \geq 2} T^n(U)$. Hence $T(f)^{-1}(I(V)) = I(U)$, and $B(f)$ is injective.
Indeed, let $G$ be a group and $1$ contain the identity element of $G$. Hence $W$ is a group of order $2$. In particular, $S$ is generated by the set $W$. The pair $(W, S)$ is called a Coxeter system, and $W$ is called a Coxeter group. Let $n \geq 2$. We denote the elementary transpositions of the symmetric group $S_n$ by $s_i = (i i + 1)$ for all $1 \leq i \leq n - 1$. Note that

$$\text{ord}(s_i s_j) = \begin{cases} 1, & \text{if } i = j, \\ 3, & \text{if } |i - j| = 1, \\ 2, & \text{if } |i - j| > 1. \end{cases}$$

**Theorem 1.7.1.** For all $n \geq 2$, $(S_n, \{s_1, \ldots, s_{n-1}\})$ is a Coxeter system, that is, $S_n$ is generated by $s_1, \ldots, s_{n-1}$ with defining relations

$$s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \quad \text{for all } 1 \leq i \leq n - 2,$$

$$s_i s_j = s_j s_i \quad \text{for all } 1 \leq i, j \leq n - 1, |i - j| > 1,$$

$$s_i^2 = 1 \quad \text{for all } i.$$

**Proof.** For $n = 2$ the claim is trivial. Assume that $n \geq 3$. Let $W_n$ denote the Coxeter group given by generators $s_1, \ldots, s_{n-1}$ and relations (1.7.1)–(1.7.3). The elementary transpositions of $S_n$ satisfy Equations (1.7.1)–(1.7.3), hence there is a surjective map $W_n \to S_n$. On the other hand,

$$W_n = \{w, ws_{n-1}, ws_{n-1}s_{n-2}, \ldots, ws_{n-1}s_{n-2} \cdots s_1 \mid w \in \langle s_1, \ldots, s_{n-2} \rangle\}.$$

Indeed, let $i, j \in \{1, \ldots, n - 1\}$. Then

$$(s_{n-1}s_{n-2} \cdots s_i)s_j = \begin{cases} s_{j-1}(s_{n-1}s_{n-2} \cdots s_i) & \text{if } j > i, \\ s_{n-1}s_{n-2} \cdots s_{i+1} & \text{if } j = i, \\ s_{n-1}s_{n-2} \cdots s_{i-1} & \text{if } j = i - 1, \\ s_j(s_{n-1}s_{n-2} \cdots s_i) & \text{if } j < i - 1. \end{cases}$$

Hence $\{w, ws_{n-1}, ws_{n-1}s_{n-2}, \ldots, ws_{n-1}s_{n-2} \cdots s_1 \mid w \in \langle s_1, \ldots, s_{n-2} \rangle\}$ is a subgroup of $W_n$ containing all generators of $W_n$ and hence coincides with $W_n$. We conclude that $|W_n| \leq n|W_{n-1}|$ and hence $|W_n| \leq n!$ by induction on $n$. Therefore $W_n \cong S_n$ since $|S_n| = n!$. □
Let
\[
\Delta = \{(a, b) \in \mathbb{N}^2 \mid 1 \leq a, b \leq n, \ a \neq b\},
\]
\[
\Delta_+ = \{(a, b) \in \Delta \mid a < b\},
\]
\[
\Delta_- = \{(a, b) \in \Delta \mid a > b\},
\]
and define
\[
\alpha_1 = (1, 2), \ \alpha_2 = (2, 3), \ldots, \ \alpha_{n-1} = (n-1, n) \in \Delta_+.
\]
The symmetric group \(S_n\) acts on \(\Delta\) by
\[
S_n \times \Delta \to \Delta, \ (w, (a, b)) \mapsto (w(a), w(b)).
\]
For \(w \in S_n\) let
\[
\Delta_w = \{\alpha \in \Delta_+ \mid w(\alpha) \in \Delta_-\}.
\]
The elements of \(\Delta_w\) are called \textit{inversions} of \(w\).

The \textbf{length} \(\ell(w)\) of a permutation \(w \in S_n\) is defined as the smallest natural number \(l \in \mathbb{N}_0\) such that there exist \(1 \leq i_1, \ldots, i_l \leq n - 1\) with \(w = s_{i_1} \cdots s_{i_l}\). A sequence \((i_1, \ldots, i_l)\) with \(1 \leq i_1, \ldots, i_l \leq n - 1\) is called a \textbf{reduced decomposition} of \(w\) if \(w = s_{i_1} \cdots s_{i_l}\), and if \(l = \ell(w)\).

In practice, the length of a permutation is computed by counting the number of its inversions.

\begin{theorem}
Let \(w \in S_n\) and let \(i \in \mathbb{N}\) with \(i \leq n - 1\).
\begin{enumerate}
\item \(\ell(ws_i) = \ell(w) + 1\) if and only if \(w(i) < w(i+1)\).
\item \(\ell(ws_i) = \ell(w) - 1\) if and only if \(w(i) > w(i+1)\).
\item For any reduced decomposition \((i_1, \ldots, i_l)\) of \(w\),
\[
\Delta_w = \{s_{i_1} \cdots s_{i_2}(\alpha_{i_1}), s_{i_1} \cdots s_{i_3}(\alpha_{i_2}), \ldots, s_i(\alpha_{i_{l-1}}), \alpha_{i_l}\}
\]
and \(l = \ell(w) = |\Delta_w|\).
\end{enumerate}
\end{theorem}

\begin{proof}
(a) Let \(v \in W\), \(1 \leq m < n\), and \(1 \leq j < k \leq n - 1\). If \(j = m\) and \(k = m + 1\), then \((j, k)\) is an inversion of \(v\) if and only if it is not an inversion of \(vs_m\). Otherwise, \((j, k)\) is an inversion of \(v\) if and only if \((s_m(j), s_m(k))\) is an inversion of \(vs_m\). Therefore
\begin{align*}
(1.7.4) & \quad \alpha_m \in \Delta_v \Rightarrow \Delta_{vs_m} = s_m(\Delta_v \setminus \{\alpha_m\}), \ |\Delta_{vs_m}| = |\Delta_v| - 1, \\
(1.7.5) & \quad \alpha_m \notin \Delta_v \Rightarrow \Delta_{vs_m} = s_m(\Delta_v) \cup \{\alpha_m\}, \ |\Delta_{vs_m}| = |\Delta_v| + 1.
\end{align*}

(b) Clearly, \(w = \text{id}_{S_n}\) if and only if \(\Delta_w = \emptyset\). By induction on \(\ell(w)\), it follows from (1.7.4) and (1.7.5) that \(|\Delta_w| \leq \ell(w)\). On the other hand, if \(\Delta_w \neq \emptyset\) then there exists \(1 \leq m < n\) such that \(w(m) > w(m + 1)\). Then \(|\Delta_{ws_m}| = |\Delta_w| - 1\) by (1.7.4). By induction on \(|\Delta_w|\) it follows that there exist \(j_1, \ldots, j_l\) with \(l = |\Delta_w|\) such that \(\Delta_{ws_{j_1} \cdots s_{j_l}} = \emptyset\), and hence \(w = s_{j_l} \cdots s_{j_1}\). Thus \(\ell(w) \leq |\Delta_w|\). Therefore \(\ell(w) = |\Delta_w|\).

(c) Since \(\ell(w) = |\Delta_w|\) by (b), (1) and (2) follow from (1.7.4) and (1.7.5) with \(v = w\), \(m = i\). Finally, (3) follows by induction on \(\ell(w)\) from (1) and (1.7.5).
\end{proof}

\begin{definition}
Let \(n \geq 1\) be a natural number. The Artin \textbf{braid group} \(B_n\) is the group generated by elements \(\sigma_1, \ldots, \sigma_{n-1}\) with relations
\begin{align*}
(1.7.6) & \quad \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ for all } 1 \leq i \leq n - 2, \\
(1.7.7) & \quad \sigma_i\sigma_j = \sigma_j\sigma_i \text{ for all } 1 \leq i, j \leq n - 1, \ |i - j| > 1.
\end{align*}
\end{definition}
Thus $B_1$ is the trivial group with one element, and $B_2 \cong \mathbb{Z}$.

It follows from the description of $S_n$ in Theorem 1.7.1 that

$$B_n \rightarrow S_n, \quad \sigma_i \mapsto s_i, \quad 1 \leq i \leq n - 1,$$

defines a surjective group homomorphism.

The following Theorem, attributed to Matsumoto, is a special case of an important tool in the theory of Coxeter groups. Here it will be used to describe the components of the comultiplication of the tensor algebra of a braided vector space, see e.g. Theorem 1.9.1.

**Theorem 1.7.4.** Let $n \geq 2$. Then

$$\sigma : S_n \rightarrow B_n, \quad w = s_{i_1} \cdots s_{i_l} \mapsto \sigma_{i_1} \cdots \sigma_{i_l},$$

where $(i_1, \ldots, i_l)$ is a reduced decomposition of $w$, is a well-defined map.

**Proof.** Let $w \in S_n$, $l = \ell(w)$, and let $(i_1, \ldots, i_l)$, $(j_1, \ldots, j_l)$ be two reduced decompositions of $w$. We have to show that

$$\sigma_{i_1} \cdots \sigma_{i_l} = \sigma_{j_1} \cdots \sigma_{j_l}.$$  

(1.7.8)

We proceed by induction on $l$. If $l \leq 1$ then (1.7.8) clearly holds. Assume that $l \geq 2$. If $i_l = j_l$ then $(i_1, \ldots, i_{l-1})$ and $(j_1, \ldots, j_{l-1})$ are reduced decompositions of $ws_{i_l}$ and hence (1.7.8) holds by induction hypothesis.

Assume that $i_l < j_l - 1$. Then $(i_l, i_{l+1})$ and $(j_l, j_{l+1})$ are inversions of $w$. Theorem 1.7.2(2) implies that $w = us_{j_l}s_{i_l} = us_{i_l}s_{j_l}$ for some $u \in S_n \ell(u) = l - 2$. Therefore

$$\sigma_{i_1} \cdots \sigma_{i_l} = \sigma(u)\sigma_{j_1} \sigma_{i_l} = \sigma(u)\sigma_{i_1} \sigma_{j_l} = \sigma_{j_1} \cdots \sigma_{j_l},$$

by induction hypothesis and by (1.7.7).

Assume that $j_l = i_l + 1$. Then $(i_l, i_{l+1})$ and $(i_{l+1}, i_{l+2})$ are inversions of $w$. Hence $(i_l, i_{l+2}) \in \Delta_w$. Theorem 1.7.2(2) implies that $w = us_{j_l}s_{i_l}$ for some $u \in S_n$ such that $\ell(u) = l - 3$. Then $w = us_{j_l}s_{i_l}s_{j_l}$ and

$$\sigma_{i_1} \cdots \sigma_{i_l} = \sigma(u)\sigma_{i_1} \sigma_{j_l} \sigma_{i_l} = \sigma(u)\sigma_{j_1} \sigma_{i_1} \sigma_{j_l} = \sigma_{j_1} \cdots \sigma_{j_l},$$

by induction hypothesis and by (1.7.6). \qed

The map $\sigma$ in Theorem 1.7.4 is a section of the canonical map $\pi : B_n \rightarrow S_n$, that is, $\pi \sigma = \text{id}_{S_n}$. It is called the **Matsumoto section**.

Recall the notation $c_i : V^\otimes n \rightarrow V^\otimes n$, $n \geq 2$, $1 \leq i \leq n - 1$, in (1.5.1) for a vector space $V$ with endomorphism $c : V \otimes V \rightarrow V \otimes V$. By abuse of notation we thus identify $c_i$ with $c_i \otimes \text{id}_{V^\otimes m}$ for all $m \geq 0$.

**Lemma 1.7.5.** Let $(V, c)$ be a braided vector space, and $n \geq 2$. Then

$$B_n \rightarrow \text{Aut}(V^\otimes n), \quad \sigma_i \mapsto c_i, \quad 1 \leq i \leq n - 1,$$

defines a group homomorphism.

**Proof.** This follows from the definition of the braid group, since the automorphisms $c_i$ satisfy the relations of the generators $\sigma_i$ of $B_n$. \qed

The action of $B_n$ on $V^\otimes n$ defined in Lemma 1.7.5 will be denoted by

$$kB_n \otimes V^\otimes n \rightarrow V^\otimes n, \quad \sigma \otimes x \mapsto \sigma x,$$

for all $\sigma \in B_n$, $x \in V^\otimes n$. 

46 1. A QUICK INTRODUCTION TO NICHOLS ALGEBRAS
**Definition 1.7.6.** Let \((V, c)\) be a braided vector space, and \(n \geq 2\). For all \(w \in S_n\) we denote the image of \(w\) under the composition
\[
S_n \xrightarrow{\sigma} B_n \rightarrow \text{Aut}(V^{\otimes n})
\]
by \(c_w = c_{i_1} \cdots c_{i_l}\), if \((i_1, \ldots, i_l)\) is a reduced decomposition of \(w\).

**Corollary 1.7.7.** Let \((V, c)\) be a braided vector space, and \(n \geq 2\). Then \(c_{id} = \text{id}_{V^{\otimes n}}, c_{i} = c_{i}\) for all \(1 \leq i \leq n - 1\), and \(c_{w_1w_2} = c_{w_1}c_{w_2}\) for any \(w_1, w_2 \in S_n\) with \(\ell(w_1w_2) = \ell(w_1) + \ell(w_2)\).

**Proof.** This follows from Lemma 1.7.5 and Theorem 1.7.4. \(\square\)

If \(c\) is the flip map, Definition 1.7.6 describes the natural left action of the symmetric group \(S_n\) on \(V^{\otimes n}\) with
\[
c_w(x_1 \otimes \cdots \otimes x_n) = x_{w^{-1}(1)} \otimes \cdots \otimes x_{w^{-1}(n)}
\]
for all \(n \geq 2\) and \(x_i \in V\) for all \(1 \leq i \leq n\). More generally, there is an explicit formula for \(c_w\) in the case of diagonal braidings.

**Proposition 1.7.8.** Let \(V\) be a vector space with basis \((x_i)_{i \in I}\) and braiding \(c\) given by
\[
c(x_i \otimes x_j) = q_{ij}x_j \otimes x_i, i, j \in I,
\]
where the \(q_{ij}\), \(i, j \in I\), are non-zero scalars in \(k\). Then for all \(n \geq 1\), \(w \in S_n\) and all functions \(k : \{a \in \mathbb{N} \mid 1 \leq a \leq n\} \rightarrow I\),
\[
c_w(x_{k(1)} \otimes \cdots \otimes x_{k(n)}) = \prod_{a < b, w(a) > w(b)} q_{k(a), k(b)}x_{k(w^{-1}(1))} \otimes \cdots \otimes x_{k(w^{-1}(n))}.
\]

**Proof.** For \(w = s_i, 1 \leq i \leq n - 1\), the claim holds by definition of \(c_{s_i} = c_i\), and since \(\Delta_{s_i} = \{(i, i + 1)\}\). If the length of \(w\) is \(l \geq 2\), let \((i_1, \ldots, i_l)\) be a reduced decomposition of \(w\). Write \(w = s_{i_1}u, u = s_{i_2} \cdots s_{i_l}\). By induction on the length of \(w\) we may assume that the formula holds for \(u\). Let
\[
x_k = x_{k(1)} \otimes \cdots \otimes x_{k(n)}, k : \{a \in \mathbb{N} \mid 1 \leq a \leq n\} \rightarrow I.
\]
We know from Theorem 1.7.2(3) that \(\Delta_w = \Delta_u \cup \{(u^{-1}(i_1), u^{-1}(i_1 + 1))\}\) and \(|\Delta_w| = |\Delta_u| + 1\). Therefore
\[
c_w(x_k) = c_{i_1}c_u(x_k) = c_{i_1} \left( \prod_{a < b, u(a) > u(b)} q_{k(a), k(b)}x_{ku^{-1}} \right)
\]
\[
= \prod_{a < b, u(a) > u(b)} q_{k(a), k(b)}x_{ku^{-1}(i_1)}x_{ku^{-1}(i_1 + 1)}x_{ku^{-1}s_{i_1}}
\]
\[
= \prod_{a < b, w(a) > w(b)} q_{k(a), k(b)}x_{kw^{-1}}.
\]
This proves the claim. \(\square\)

We introduce the following useful notation. For all natural numbers \(2 \leq m \leq n\) and \(0 \leq i \leq n - m\) there are embeddings of groups
\[
(1.7.10) \quad \text{sh}^i_{m,n} : S_m \rightarrow S_n, \; s_j \mapsto s_{j+i}, \; 1 \leq j \leq m - 1.
\]
We will write
\[
(1.7.11) \quad \text{sh}^i_{m,n}(w) = w^{↑i}, \; w \in S_m.
\]

Thus we identify $S_m$ with \{ $w \in S_n \mid w(j) = j$ for all $m + 1 \leq j \leq n$ \}. The shift operators $↑i$ can also be defined for the braid group. There are group homomorphisms $\text{sh}^i_{m,n} : B_m \to B_n, \; \sigma_j \mapsto \sigma_{j+i}, \; 1 \leq j \leq m - 1$. These maps are embeddings, but we will not use this fact. However, we will write
\[
(1.7.12) \quad \text{sh}^i_{m,n}(\sigma) = \sigma^{↑i}, \; \sigma \in B_m.
\]

Another type of shift operators are defined for automorphisms:
\[
(1.7.13) \quad \text{Aut}(V^{⊗m}) \to \text{Aut}(V^{⊗n}), \; f \mapsto f^{↑i} = \text{id}_{V^{⊗i}} \otimes f \otimes \text{id}_{V^{⊗n-m-i}}.
\]

Then $c_j^{↑i} = c_{j+i}$ and $c_w^{↑i} = c_w^{↑i}$, for all $1 \leq j \leq m - 1$ and $w \in S_m$.

**Definition 1.7.9.** Let $(V, c)$ be a braided vector space. For $m, n \geq 1$ let
\[
s_{m,n} = \left( \frac{1}{n+1} \frac{2}{n+2} \ldots \frac{m}{n+m} \frac{m+1}{n+m+1} \frac{m+2}{n+m+2} \ldots \frac{m+n}{n+m+n} \right) \in S_{m,n},
\]
\[
c_{m,n} = c_{s_{m,n}} \in \text{Aut}(V^{⊗m+n}).
\]

We write $k = V^{⊗0}$, and denote for all $n \geq 0$ by $c_{n,0} : V^{⊗0} \otimes k \to k \otimes V^{⊗n}$ and $c_{0,n} : k \otimes V^{⊗n} \to V^{⊗n} \otimes k$ the canonical isomorphisms. By abuse of notation we again identify $c_{m,n}$ with $c_{m,n} \otimes \text{id}_{V^{⊗p}}$ for all $p \geq 0$.

**Corollary 1.7.10.** Let $(V, c)$ be a braided vector space, and $l, m, n \geq 1$. Then
\[
(1) \quad c_{m,n} = (c_n c_{n-1} \cdots c_1) (c_n c_{n-1} \cdots c_1)^{↑1} \cdots (c_n c_{n-1} \cdots c_1)^{↑m-1},
\]
\[
(2) \quad c_{m,n} = (c_1 c_2 \cdots c_m)^{↑n-1} (c_1 c_2 \cdots c_m)^{↑n-2} \cdots (c_1 c_2 \cdots c_m),
\]
\[
(3) \quad (c_{m,n})^{-1} = (c^{-1})_{n,m},
\]
\[
(4) \quad c_{l,m+n} = c_{l,n} c_{m,n}^{↑l},
\]
\[
(5) \quad c_{l,m+n} = c_{l,n} c_{m,n}^{↑m} c_{l,m}.
\]

In particular, for all $n \geq 1$ we obtain that
\[
(1.7.14) \quad c_{1,n} = c_n c_{n-1} \cdots c_1, \quad c_{n,1} = c_1 c_2 \cdots c_n.
\]

**Proof.** By counting the inversions of $s_{m,n}$ we see that $\ell(s_{m,n}) = mn$. Hence
\[
(n, n - 1, \ldots, 1, n + 1, n, \ldots, 2, \ldots, n + m - 1, n + m - 2, \ldots, m),
\]
\[
(n, n + 1, \ldots, n + m - 1, \ldots, 2, 3, \ldots, m + 1, 1, 2, \ldots, m)
\]
are reduced decompositions of $s_{m,n}$. Thus (1) and (2) follow from Theorem 1.7.4. The equality in (3) follows by computing the left-hand side with (1) and the right-hand side with (2). The equations in (4) and (5) follow from the formulas in (1) and (2). \[\square\]

For any group $G$ and any $V \in \mathcal{C}_G \mathcal{YD}$ (or $V$ in a braided strict monoidal category, see Section 3.2), the braid group acts on tensor powers of $V$ as in Lemma 1.7.5. The maps $c_{m,n}$ arise naturally in this context.

**Lemma 1.7.11.** Let $G$ be a group, and $V \in \mathcal{C}_G \mathcal{YD}$ with braiding $c = c_{V,V}$. Then for all $m, n \geq 1$,
\[
c_{V^{⊗m},V^{⊗n}} = c_{m,n}.
\]
PROOF. By Corollary 1.7.10(2) it suffices to show that for all \( m, n \geq 1 \),
\[
c_{V^{\otimes m}, V^{\otimes n}} = (c_{n}c_{n+1} \cdots c_{n+m-1}) \cdots (c_{2}c_{3} \cdots c_{m+1})(c_{1}c_{2} \cdots c_{m}).
\]
(1) By induction on \( m \) we first prove that \( c_{V^{\otimes m}, V} = c_{1}c_{2} \cdots c_{m} \) for all \( m \geq 1 \). This
is clear for \( m = 1 \). Let \( m \geq 1 \). Then
\[
c_{V^{\otimes m+1}, V} = c_{V^{\otimes m}} \otimes V = (c_{V^{\otimes m}, V} \otimes \text{id}_V)c_{m+1}
\]
by (1.4.5), and the claim follows by induction.
(2) Now we show for fixed \( m \) by induction on \( n \) that \( c_{V^{\otimes m}, V^{\otimes n}} = c_{m,n} \) for all \( n \geq 1 \). For \( n = 1 \) this holds by (1). Let \( n \geq 1 \). Then by (1) and (1.4.4),
\[
c_{V^{\otimes m}, V^{\otimes (n+1)}} = (\text{id}_{V^{\otimes n}} \otimes c_{V^{\otimes m}, V})(c_{V^{\otimes m}, V^{\otimes n}} \otimes \text{id}_{V})
\]
and the claim follows by induction. \( \square \)

1.8. SHUFFLE PERMUTATIONS AND BRAIDED SHUFFLE ELEMENTS

Recall the notion of a shuffle permutation from Section 1.2.

**Definition 1.8.1.** Let \( n \) be a natural number, and \( 0 \leq i \leq n \). A permutation
\( w \in S_n \) is called an \((i, n - i)\)-**shuffle** or simply an \(i\)-shuffle if
\[
w(1) < \cdots < w(i), \text{ and } w(i + 1) < \cdots < w(n).
\]
Let \( S_{i,n-i} \) denote the set of all \(i\)-shuffles in \( S_n \).

Note that \( S_{0,n} = \{\text{id}\} = S_{n,0} \). The cardinality of \( S_{i,n-i} \) is \( \binom{n}{i} \). To obtain all
\((n - 1, 1)\)- and \((1, n - 1)\)-shuffles, one looks at the image of \( n \) and 1, respectively.
Let \( 1 \leq i \leq n \). Then
\[
s_is_{i+1} \cdots s_{n-1} = (i \ i \ 1 \ \cdots \ n) = (1 \ 2 \ i \ 3 \ \cdots \ n - 1 \ \ i \ n)
\]
is an \((n - 1, 1)\)-shuffle of length \( n - i \), and
\[
s_{i-1}s_{i-2} \cdots s_1 = (i \ i \ 1 \ \cdots \ 1) = (1 \ 2 \ 3 \ \cdots \ i - 1 \ i \ i + 1 \ \cdots \ n)
\]
is a \((1, n - 1)\)-shuffle of length \( i - 1 \). Thus
\[(1.8.1) \quad S_{n-1,1} = \{\text{id}\} \cup \{s_is_{i+1} \cdots s_{n-1} \mid 1 \leq i \leq n - 1\},
\]
\[(1.8.2) \quad S_{1,n-1} = \{\text{id}\} \cup \{s_is_{i-1} \cdots s_1 \mid 1 \leq i \leq n - 1\}.
\]
Shuffle permutations can be described inductively.

**Proposition 1.8.2.** Let \( n \geq 2 \) and \( 1 \leq i \leq n - 1 \).

1. \( S_{i,n-i} = S_{i-1,n-i-1} \cup S_{i-1,n-i}s_{n-1} \cdots s_{i} \) (disjoint union).
2. Let \( w \in S_{n-1} \). Then \( \ell(ws_{n-1} \cdots s_i) = \ell(w) + n - i \).

**Proof.** Let \( u \in S_{i,n-i} \). If \( u(n) = n \), then \( u \in S_{i,n-1-i} \). If \( u(n) \neq n \), then \( u(i) = n \), since \( u \) is an \(i\)-shuffle. Note that \( s_{n-1} \cdots s_i = (n \ n - 1 \cdots i) \). Define
\[
\ell(u_1) = n,
\]
and
\[
u_1(1) < u_1(2) < \cdots < u_1(i - 1)
\]
and
\[
u_1(i) = u(i + 1) < u_1(i + 1) = u(i + 2) < \cdots < u_1(n - 1) = u(n).
\]
Hence \( u = u_1s_{n-1} \cdots s_i \), and \( u_1 \in S_{i-1,n-i} \). This proves the inclusion \( \subseteq \) in (1),
and the other inclusion follows similarly.
We prove (2) by induction on $n-i$. Let $u_1 = ws_{n-1} \cdots s_{i+1}$ and $u = u_1s_i$. Then
\[
\ell(u_1) = \ell(w) + n - i - 1 \quad \text{by induction hypothesis.}
\]
As $u_1(i) = w(i) < n = u_1(i+1)$, we conclude that $\ell(u) = \ell(u_1) + 1$ by Theorem 1.7.2(1). This implies the claim. □

In the next Proposition we show that the $i$-shuffles are a complete set of representatives of $\mathbb{S}_n$ modulo the subgroup
\[
\langle s_{i+1}, \ldots, s_{n-1} \rangle \langle s_1, \ldots, s_{i-1} \rangle \cong \mathbb{S}_{n-i} \times \mathbb{S}_i.
\]

**Proposition 1.8.3.** Let $n \geq 2$ and $1 \leq i \leq n-1$.

1. The map
\[
\mathbb{S}_{i,n-i} \times \mathbb{S}_{n-i} \times \mathbb{S}_i \to \mathbb{S}_n, \quad (u, s, t) \mapsto us^\uparrow t,
\]
is bijective.

2. Let $u \in \mathbb{S}_{i,n-i}$, $s \in \mathbb{S}_{n-i}$, $t \in \mathbb{S}_i$. Then $\ell(us^\uparrow t) = \ell(u) + \ell(s) + \ell(t)$.

**Proof.** (1) Let $w \in \mathbb{S}_n$. Total orderings of the sets $\{w(l) \mid 1 \leq l \leq i\}$ and $\{w(l) \mid i + 1 \leq l \leq n\}$ define permutations $v_1$ of $\{1, \ldots, i\}$ and $v_2$ of $\{i + 1, \ldots, n\}$ with
\[
wv_1(1) < \cdots < wv_1(i) \quad \text{and} \quad wv_2(i+1) < \cdots < wv_2(n).
\]
Thus $v_1 \in \langle s_1, \ldots, s_{i-1} \rangle$, $v_2 \in \langle s_{i+1}, \ldots, s_{n-1} \rangle$, and $wv_1v_2 \in \mathbb{S}_{i,n-i}$. Set $u = wv_1v_2$, $t = v_1^{-1}$ and $s \in \mathbb{S}_{n-i}$ such that $s^\uparrow i = v_2^{-1}$. Then $w = us^\uparrow t$. Hence the map $\mathbb{S}_{i,n-i} \times \mathbb{S}_{n-i} \times \mathbb{S}_i \to \mathbb{S}_n$ in (1) is surjective. It is bijective since
\[
|\mathbb{S}_{i,n-i} \times \mathbb{S}_{n-i} \times \mathbb{S}_i| = n! = |\mathbb{S}_n|.
\]

To prove (2), we count the inversions of $w = us^\uparrow t$. Let $1 \leq k < l \leq n$. We distinguish three cases. If $l \leq i$, then $(k, l)$ is an inversion of $w$ if and only if $(k, l)$ is an inversion of $t$. If $i + 1 \leq k$, then $(k, l)$ is an inversion of $w$ if and only if $(k, l)$ is an inversion of $s^\uparrow i$. If $k \leq i < l$, then $(k, l)$ is an inversion of $w$ if and only if $(t(k), s^\uparrow i(l))$ is an inversion of $u$. This implies (2) by Theorem 1.7.2(3). □

**Corollary 1.8.4.** Let $n \geq 2$.

1. The multiplication map $\mathbb{S}_{n-1,1} \times \mathbb{S}_{n-2,1} \times \cdots \times \mathbb{S}_{1,1} \to \mathbb{S}_n$ is bijective.

2. Let $w_i \in \mathbb{S}_{i,1}$ for all $1 \leq i \leq n-1$. Then
\[
\ell(w_{n-1}w_{n-2} \cdots w_1) = \ell(w_{n-1}) + \ell(w_{n-2}) + \cdots + \ell(w_1).
\]

**Proof.** By Proposition 1.8.3, the multiplication map $\mathbb{S}_{n-1,1} \times \mathbb{S}_{n-1} \to \mathbb{S}_n$ is bijective, and $\ell(ut) = \ell(u) + \ell(t)$ for all $u \in \mathbb{S}_{n-1,1}$ and $t \in \mathbb{S}_{n-1}$. Hence the claim follows by induction on $n$. □

**Corollary 1.8.5.** Let $n \geq 2$. Then $\mathbb{S}_{i,n-i} \mathbb{S}_{n-i}^\uparrow = \mathbb{S}_{n-1,1} \mathbb{S}_{n-2,1} \cdots \mathbb{S}_{i,1}$ for any $1 \leq i < n$.

**Proof.** Both subsets $\mathbb{S}_{i,n-i} \mathbb{S}_{n-i}^\uparrow$ and $\mathbb{S}_{n-1,1} \mathbb{S}_{n-2,1} \cdots \mathbb{S}_{i,1}$ of $\mathbb{S}_n$ have cardinality $n(n-1) \cdots (i+1)$ by Proposition 1.8.3(1) and Corollary 1.8.4(1). Moreover, both sets consist of representatives of minimal length of the left $\mathbb{S}_i$ cosets of $\mathbb{S}_n$ by Proposition 1.8.3(2) and Corollary 1.8.4. □

**Remark 1.8.6.** Using Corollary 1.8.4 together with (1.8.1) one obtains reduced decompositions for any element of $\mathbb{S}_n$. In particular,
\[
(1, 2, \ldots, n-1, 1, 2, \ldots, n-2, \ldots, 1, 2, 1)
\]
is a reduced decomposition of the unique longest element

\[ w_0 = \left( \frac{1}{n} \frac{2}{n-1} \cdots \frac{n}{1} \right) \]

in \( S_n \), and \( w_0 \) has length \( \frac{n(n-1)}{2} \) and order two. Conjugation with \( w_0 \) in \( S_n \) is the inner automorphism

\[ (1.8.3) \quad \alpha_n : S_n \to S_n, \; s_i \mapsto s_{n-i}, \; 1 \leq i \leq n-1. \]

Since the map \( \alpha_n \) permutes the elementary reflections, it preserves the length of elements in \( S_n \).

Theorem 1.7.2(1) implies that any reduced decomposition of an element \( w \in S_n \) can be extended to a reduced decomposition of \( w_0 \). Hence

\[ (1.8.4) \quad \ell(w_0) = \ell(w) + \ell(w^{-1}w_0) \]

for all \( w \in S_n \).

We introduce the following important elements in the group algebra \( \mathbb{ZB}_n \) of the braid group with integer coefficients. Recall the Matsumoto section \( \sigma : S_n \to B_n \) of Theorem 1.7.4.

**Definition 1.8.7.** Let \( n \geq 2 \) and \( 0 \leq i \leq n \). We define the **braided symmetrizer** and the **braided shuffle** elements in \( \mathbb{ZB}_n \) by

\[ S_n = \sum_{w \in S_n} \sigma(w), \quad S_{i,n-i} = \sum_{w \in S_{i,n-i}} \sigma(w^{-1}). \]

Note that \( S_{0,n} = 1 = S_{n,0} \), and by (1.8.1) and (1.8.2),

\[ (1.8.5) \quad S_{i,n-1} = 1 + \sigma_1 + \sigma_1\sigma_2 + \cdots + \sigma_1\sigma_2\cdots\sigma_{n-1}, \]

\[ (1.8.6) \quad S_{n-1,1} = 1 + \sigma_{n-1} + \sigma_{n-1}\sigma_{n-2} + \cdots + \sigma_{n-1}\cdots\sigma_2\sigma_1. \]

We define an algebra automorphism of \( \mathbb{ZB}_n \) by

\[ \alpha_n : \mathbb{ZB}_n \to \mathbb{ZB}_n, \; \sigma_i \mapsto \sigma_{n-i}, \; 1 \leq i \leq n-1, \]

and an algebra antiautomorphism by

\[ (1.8.8) \quad \beta_n : \mathbb{ZB}_n \to \mathbb{ZB}_n, \; \sigma_i \mapsto \sigma_i, \; 1 \leq i \leq n-1. \]

Applying \( \alpha_n, \beta_n \) or \( \beta_n\alpha_n \) gives new representations of elements in \( \mathbb{ZB}_n \). In particular, by (1.8.5) and (1.8.6), \( \alpha_n(S_{1,n-1}) = S_{n-1,1} \).

For all natural numbers \( 2 \leq m \leq n \), and \( 0 \leq i \leq n - m \) the shift operation of the braid groups extends to an algebra map

\[ \mathbb{ZB}_m \to \mathbb{ZB}_n, \; \sigma_j \mapsto \sigma_{i+j}, \; 1 \leq j \leq m - 1. \]

Let \( x^{i} \) denote the image of \( x \in \mathbb{ZB}_m \) under this map. For \( i = 0 \) we write \( x \) instead of \( x^{i} \). With this convention, expressions like \( S_i S_{n-i}^{i} S_{i,n-i} \) for \( 1 \leq i \leq n-1 \) make sense in \( \mathbb{ZB}_k \) for all \( k \geq n \), see Corollary 1.8.8 below.

By Theorem 1.7.4, the reduced decompositions of permutations we have obtained above translate directly into equalities in the group algebra \( \mathbb{ZB}_n \).

**Corollary 1.8.8.** Let \( n \geq 2 \) and \( 1 \leq i < n \). Then

1. \( S_{i,n-i} = S_{i,n-1-i} + \sigma_i\sigma_{i+1}\cdots\sigma_{n-1}S_{1,n-i} \)
2. \( S_n = S_1 S_{n-1}^{i} S_{i,n-i} \)
3. \( S_n = S_{1,1} S_{2,1} \cdots S_{n-1,1} \)
4. \( S_{n-i}^{i} s_{i,n-i} = S_{i,1} S_{i+1,1} \cdots S_{n-1,1} \).
Proof. (1), (2), and (3) follow from Proposition 1.8.2, Proposition 1.8.3, and Corollary 1.8.4, respectively. (4) follows from Corollary 1.8.5, Proposition 1.8.3(2), and Corollary 1.8.4(2).

Remark 1.8.9. By applying $\alpha_n, \beta_n$ and $\beta_n \alpha_n$ to the product decomposition of $S_n$ in Corollary 1.8.8(3) we obtain three more formulas. In particular,

\[ S_1 = 1, \]
\[ S_2 = 1 + \sigma_1, \]
\[ S_3 = (1 + \sigma_1)(1 + \sigma_2 + \sigma_2\sigma_1), \]
\[ = (1 + \sigma_2)(1 + \sigma_1 + \sigma_1\sigma_2), \]
\[ = (1 + \sigma_2 + \sigma_1\sigma_2)(1 + \sigma_1), \]
\[ = (1 + \sigma_1 + \sigma_2\sigma_1)(1 + \sigma_2), \]
\[ S_4 = (1 + \sigma_1)(1 + \sigma_2 + \sigma_2\sigma_1)(1 + \sigma_3 + \sigma_3\sigma_2 + \sigma_3\sigma_2\sigma_1), \]
\[ = (1 + \sigma_3)(1 + \sigma_2 + \sigma_2\sigma_3)(1 + \sigma_1 + \sigma_1\sigma_2 + \sigma_1\sigma_2\sigma_3), \]
\[ = (1 + \sigma_3 + \sigma_2\sigma_3 + \sigma_1\sigma_2\sigma_3)(1 + \sigma_2 + \sigma_1\sigma_2)(1 + \sigma_1), \]
\[ = (1 + \sigma_1 + \sigma_2\sigma_1 + \sigma_3\sigma_2\sigma_1)(1 + \sigma_2 + \sigma_3\sigma_2)(1 + \sigma_3). \]

The braided symmetrizer and the braided shuffle elements in $\mathbb{ZB}_n$ define endomorphism on $n$-fold tensor products of braided vector spaces $(V,c)$. Recall the $\mathbb{ZB}_n$-module structure

\[ \mathbb{ZB}_n \otimes V^\otimes n \to V^\otimes n, \quad \sigma_i \mapsto c_i, \ 1 \leq i \leq n, \]

of $V^\otimes n$ in Lemma 1.7.5.

Definition 1.8.10. Let $(V,c)$ be a braided vector space. Let $n \geq 2$, and $1 \leq i \leq n-1$. The braided shuffle map $S_{i,n-i}^{(V,c)} = S_{i,n-i}^{(V,c)} : V^\otimes n \to V^\otimes n$ and the braided symmetrizer map $S_n^{(V,c)} = S_n^{(V,c)} : V^\otimes n \to V^\otimes n$ are defined by

\[ S_{i,n-i} = \sum_{w \in S_{i,n-i}} c_{w^{-1}}, \quad S_n = \sum_{w \in S_n} c_w. \]

The inductive description of the braided shuffle map and the braided symmetrizer map in the next corollary is an immediate consequence of Corollary 1.8.8(1) and (2).

Corollary 1.8.11. Let $(V,c)$ be a braided vector space. Let $1 \leq i < n$. Then the following equations hold in $\text{End}(V^\otimes n)$:

\[ S_{i,n-i} = S_{i,n-i-1} \otimes \text{id}_V + c_{i+1}c_{i+1} \cdots c_{n-1}(S_{i-1,n-i} \otimes \text{id}_V), \]
\[ S_n = (S_i \otimes S_{n-i})S_{i,n-i}. \]

The braided shuffle elements $S_{n-1,1}$ in $\mathbb{ZB}_n$ have an interesting description as rational functions. For the proof we need an easy commutation rule in the braid group.

Lemma 1.8.12. Let $n \geq 2$, and $p_{n-1} = \sigma_{n-1}\sigma_{n-2} \cdots \sigma_1 \in \mathbb{B}_n$. Then

\[ \sigma_{i-1}p_{n-1} = p_{n-1}\sigma_i \]

for all $2 \leq i \leq n-1$. 

Proof. Using the relations of the braid group we compute

\[ p_{n-1}\sigma_i = \sigma_{n-1} \cdots \sigma_{i+1}\sigma_i\sigma_{i-1}\sigma_{i-2} \cdots \sigma_1\sigma_i \]
\[ = \sigma_{n-1} \cdots \sigma_{i+1}\sigma_i\sigma_{i-1}\sigma_{i-2} \cdots \sigma_1 \quad \text{(by (1.7.7))} \]
\[ = \sigma_{n-1} \cdots \sigma_{i+1}\sigma_i\sigma_{i-1}\sigma_{i-2} \cdots \sigma_1 \quad \text{(by (1.7.6))} \]
\[ = \sigma_{i-1}p_{n-1}. \quad \text{(by (1.7.7))} \]

This proves the Lemma. \[ \square \]

**Proposition 1.8.13.** Let \( n \geq 2 \). Then

1. \( S_{n-1,1}(1 - \sigma_{n-1}\sigma_{n-2} \cdots \sigma_1) = (1 - \sigma_{n-1}^2\sigma_{n-2} \cdots \sigma_1)S_{n-2,1}^\dagger \).
2. \( S_{n-1,1}(1 - \sigma_{n-1}\sigma_{n-2} \cdots \sigma_1)(1 - \sigma_{n-1}\sigma_{n-2} \cdots \sigma_2) \cdots (1 - \sigma_{n-1}) = (1 - \sigma_{n-1}^2\sigma_{n-2} \cdots \sigma_2) \cdots (1 - \sigma_{n-1}^2). \)

**Proof.** (1) Let \( p_{n-1} = \sigma_{n-1}\sigma_{n-2} \cdots \sigma_1 \). It follows from (1.8.6) that

\[ \sigma_{n-1}S_{n-2,1} = S_{n-1,1} - 1, \]
\[ S_{n-2,1}^\dagger + p_{n-1} = S_{n-1,1}. \]

It follows from Lemma 1.8.12 that

\[ p_{n-1}S_{n-2,1}^\dagger = S_{n-2,1}p_{n-1}. \]

Then

\[ (1 - \sigma_{n-1}p_{n-1})S_{n-2,1}^\dagger = S_{n-2,1}^\dagger - \sigma_{n-1}S_{n-2,1}p_{n-1} \quad \text{(by (1.8.13))} \]
\[ = S_{n-2,1}^\dagger - (S_{n-1,1} - 1)p_{n-1} \quad \text{(by (1.8.11))} \]
\[ = S_{n-2,1}^\dagger - S_{n-1,1}p_{n-1} + p_{n-1} \]
\[ = S_{n-1,1}(1 - p_{n-1}) \quad \text{(by (1.8.12)).} \]

(2) follows from (1). \( \square \)

**Corollary 1.8.14.** For all \( n \geq 1 \) let \( p_n = \sigma_n\sigma_{n-1} \cdots \sigma_1 \) and

\[ T_n = (1 - \sigma_n^2\sigma_{n-1} \cdots \sigma_1) \cdots (1 - \sigma_n^2\sigma_{n-1}) (1 - \sigma_n^2) \in \mathbb{ZB}_{n+1}, \]
\[ \varphi_n = \beta_{n+1}(S_{1,n-1}) - \beta_{n+1}(S_{n-1,1}) \sigma_np_n \in \mathbb{ZB}_{n+1}. \]

Let \( \varphi_0 = 0 \). Then the following hold for all \( n \geq 1 \).

1. \( T_n = S_{n,1}(1 - \sigma_n\sigma_{n-1} \cdots \sigma_1) \cdots (1 - \sigma_n\sigma_{n-1}) (1 - \sigma_n). \)
2. \( S_nT_n = S_{n+1}(1 - \sigma_n\sigma_{n-1} \cdots \sigma_1) \cdots (1 - \sigma_n\sigma_{n-1}) (1 - \sigma_n). \)
3. \( \varphi_n = 1 - \beta_{n+1}(p_n)p_n + \varphi_{n-1}^\dagger \sigma_1. \)
4. \( S_{n+1}T_{n+1} = \varphi_{n+1}^\dagger T_n^\dagger = \varphi_{n+1}^\dagger \varphi_n^\dagger \cdots \varphi_1^\dagger. \)

**Remark 1.8.15.** For \( 1 \leq n \leq 3 \) the definition of \( \varphi_n \) says that

\[ \varphi_1 = 1 - \sigma_1^2, \]
\[ \varphi_2 = 1 + \sigma_1 - \sigma_2^2\sigma_1 - \sigma_1\sigma_2^2\sigma_1, \]
\[ \varphi_3 = 1 + \sigma_1 + \sigma_2\sigma_1 - \sigma_3^2\sigma_2\sigma_1 - \sigma_2\sigma_3^2\sigma_2\sigma_1 - \sigma_1\sigma_2\sigma_3^2\sigma_2\sigma_1. \]

**Proof of Corollary 1.8.14.** (1) holds by Proposition 1.8.13(2), and (2) follows from (1), since \( S_{n+1} = S_nS_{n,1} \) by Corollary 1.8.8(2).
(3) holds for \( n = 1 \) by definition, since \( \varphi_1 = 1 - \sigma_1^2 \). For \( n \geq 2 \) the claim is obtained from (1.8.11) and (1.8.12) using the maps \( \alpha_n \) and \( \beta_n \). Indeed,

\[
\varphi_n = \beta_{n+1} \alpha_n (S_{n-1,1}) - \beta_{n+1} (S_{n-1,1}) \sigma_n p_n \\
= \beta_{n+1} \alpha_n (1 + \sigma_{n-1} S_{n-2,1}) - \beta_{n+1} (S_{n-2,1} \uparrow^1 + p_{n-1}) \sigma_n p_n \\
= 1 + \beta_{n+1} (S_{1,n-2} \uparrow^1) \sigma_1 \\
- \beta_{n+1} (S_{n-2,1} \uparrow^1) (\sigma_{n-1} p_{n-1}) \uparrow^1 \sigma_1 - \beta_{n+1} (\sigma_n p_{n-1}) p_n \\
= 1 - \beta_{n+1} (p_n) p_n + \varphi_{n-1} \uparrow^1 \sigma_1.
\]

(4) To prove the first equation, by definition of \( T_{n+1} \) it suffices to show that \( S_{n+1} (1 - \sigma_{n+1} p_{n+1}) = \varphi_{n+1} S_{n} \uparrow^1 \). We obtain that

\[
S_{n+1} (1 - \sigma_{n+1} p_{n+1}) = \beta_{n+1} (S_{1,n} S_{n} \uparrow^1 - \beta_{n+1} (S_{n,1} \sigma_{n+1} p_{n+1} \\
= \beta_{n+1} (S_{1,n}) S_{n} \uparrow^1 - \beta_{n+1} (S_{n,1}) \sigma_{n+1} p_{n+1} S_{n} \uparrow^1 = \varphi_{n+1} S_{n} \uparrow^1,
\]

where the first equation follows from Corollary 1.8.8(2), the second equation from Lemma 1.8.12, and the third from (1.8.15).

The second equation in (4) follows by induction from the first one and from \( S_1 T_1 = 1 - \sigma_1^2 = \varphi_1 \). \( \square \)

### 1.9. Braided symmetrizer and Nichols algebras

In this section we fix a braided vector space \((V, c)\), where \( V \in \mathcal{O}_G \mathcal{YD} \), \( G \) a group, and \( c = c_{V,V} \). In Section 6.4 we will see that the results in this section hold for any braided vector space \((V, c)\) with exactly the same proofs.

Recall that by Proposition 1.6.13 the tensor algebra \( T(V) \) is an \( \mathbb{N}_0 \)-graded Hopf algebra in \( \mathcal{O}_G \mathcal{YD} \) with braiding given for all \( m, n \geq 0 \) by

\[
c_{m,n} : V^\otimes m \otimes V^\otimes n \to V^\otimes n \otimes V^\otimes m.
\]

In the next theorem we prove an explicit formula for the components of the comultiplication in terms of the braiding of \( V \). This formula is similar to the one for the usual comultiplication of \( T(V) \) in Example 1.2.24. However, the case of a non-trivial braiding is more involved.

**Theorem 1.9.1.** For all \( n \geq 2 \) and \( 1 \leq i \leq n - 1 \),

\[
\Delta_{i,n-i} = S_{i,n-i} : T^n(V) = V^\otimes n \to T^i(V) \otimes T^{n-i}(V) = V^\otimes n,
\]

where \( \Delta \) is the comultiplication of \( T(V) \).

**Proof.** Let \( n \geq 1 \) and \( v_1, \ldots, v_n \in V \). For clarity we will write \( v_1 v_2 \cdots v_n \) for the element \( v_1 \otimes v_2 \otimes \cdots \otimes v_n \in V^\otimes n \). We show by induction on \( n \) that

\[
\Delta(v_1 \cdots v_n) = 1 \otimes v_1 \cdots v_n + \sum_{i=1}^{n-1} S_{i,n-i}(v_1 \cdots v_n) + v_1 \cdots v_n \otimes 1.
\]

For \( n = 1 \) the formula clearly holds.
Let \( n \geq 2 \) and \( v_1, \ldots, v_n \in V \). By induction hypothesis,
\[
\Delta(v_1 \cdots v_n) = \Delta(v_1 \cdots v_{n-1})\Delta(v_n)
\]
\[
= \left(1 \otimes v_1 \cdots v_{n-1} + \sum_{i=1}^{n-2} S_{i,n-1-i}(v_1 \cdots v_{n-1}) + v_1 \cdots v_{n-1} \otimes 1\right)
\times (1 \otimes v_n + v_n \otimes 1).
\]
Multiplication of the first factor with \( 1 \otimes v_n \) gives the sum
\[
1 \otimes v_1 \cdots v_n + \sum_{i=1}^{n-2} S_{i,n-1-i}(v_1 \cdots v_{n-1})v_n + v_1 \cdots v_{n-1} \otimes v_n.
\]
For the multiplication with \( v_n \otimes 1 \) we need the braiding. First,
\[
(v_1 \cdots v_{n-1} \otimes 1)(v_n \otimes 1) = v_1 \cdots v_n \otimes 1,
\]
and by Lemma 1.7.11 and (1.7.14),
\[
(1 \otimes v_1 \cdots v_{n-1})(v_n \otimes 1) = c_1 \cdots c_{n-1}(v_1 \otimes \cdots \otimes v_n).
\]
To compute the middle terms
\[
S_{i,n-1-i}(v_1 \cdots v_{n-1})(v_n \otimes 1) \in (T^i(V) \otimes T^{n-1-i}(V))(T^1(V) \otimes 1)
\]
for \( 1 \leq i \leq n-2 \), we note that by Lemma 1.7.11 and (1.7.14) in \( T(V) \otimes T(V) \) for all \( x \in T^i(V) \), \( y \in T^{n-1-i}(V) \),
\[
(x \otimes y)(v_n \otimes 1) = c_{n-1-i,1}^i(x \otimes y \otimes v_n) = c_{i+1}c_{i+2} \cdots c_{n-1}(x \otimes y \otimes v_n).
\]
Hence
\[
\sum_{i=1}^{n-2} S_{i,n-1-i}(v_1 \cdots v_{n-1})(v_n \otimes 1)
\]
\[
= \sum_{i=1}^{n-2} c_{i+1}c_{i+2} \cdots c_{n-1}(S_{i,n-1-i} \otimes \text{id}_V)(v_1 \otimes \cdots \otimes v_n)
\]
\[
= \sum_{i=2}^{n-1} c_i\sum_{i=2}^{n-1} c_{i+1} \cdots c_{n-1}(S_{i-1,n-i} \otimes \text{id}_V)(v_1 \otimes \cdots \otimes v_n).
\]
By adding up and reordering the summands we obtain
\[
\Delta(v_1 \cdots v_n) = 1 \otimes v_1 \cdots v_n + v_1 \cdots v_n \otimes 1 + A + B + C,
\]
where
\[
A = \sum_{i=2}^{n-2} \left(S_{i,n-1-i} \otimes \text{id}_V + c_i \cdots c_{n-1}(S_{i-1,n-i} \otimes \text{id}_V)\right)(v_1 \cdots v_n),
\]
\[
B = (S_{1,n-2} \otimes \text{id}_V)(v_1 \cdots v_n) + c_1 \cdots c_{n-1}(v_1 \cdots v_n),
\]
\[
C = v_1 \cdots v_{n-1} \otimes v_n + c_{n-1}(S_{n-2,1} \otimes \text{id}_V)(v_1 \cdots v_n).
\]
By (1.8.9),
\[
A = \sum_{i=2}^{n-2} S_{i,n-i}(v_1 \cdots v_n), \quad B = S_{1,n-1}(v_1 \cdots v_n), \quad C = S_{n-1,1}(v_1 \cdots v_n)
\]
which implies (1.9.1). \qed
We note that Theorem 1.9.1 is related to the $q$-binomial formula.

**Definition 1.9.2.** Let $Q(v)$ be the field of rational functions in the indeterminate $v$ over the rational numbers. For all natural numbers $n \geq 0$ and $0 \leq i \leq n$ define elements in $Q(v)$ by

\[
(n)_v = 1 + v + v^2 + \cdots + v^{n-1} = \frac{v^n - 1}{v - 1},
\]
\[
(n)_v^i = (1)_v(2)_v \cdots (n)_v, \quad (0)_v^i = 1,
\]
\[
\left(\frac{n}{i}\right)_v = \frac{(n)_v^i}{(i)_v(n - i)_v^i}.
\]

For all $i < 0$ and all $i > n$ let $\left(\frac{n}{i}\right)_v = 0$.

**Lemma 1.9.3.** Let $n \geq 0$.

1. For all $0 \leq i \leq n$, $\left(\frac{n}{i}\right)_v = \left(\frac{n-1}{i-1}\right)_v + v^i \left(\frac{n-1}{i}\right)_v$.
2. For all $0 \leq i \leq n$, $\left(\frac{n}{i}\right)_v^i = v^{n-i} \left(\frac{n-1}{i}\right)_v + \left(\frac{n-1}{i}\right)_v$.
3. For all $0 \leq i \leq n$, $\left(\frac{n}{i}\right)_v \in \mathbb{Z}[v]$.

**Proof.** The first equation in (1) holds by definition, and the second is clear for $i = 0$ and for $i = n$. For $0 < i < n$, (1) follows by direct computation:

\[
\left(\frac{n-1}{i-1}\right)_v + v^i \left(\frac{n-1}{i}\right)_v = \frac{(n-1)_v^i}{(i)_v(n - i)_v^i} + v^i \frac{(n-1)_v^i}{(i)_v(n - i)_v^i} = \frac{(n-1)_v^i}{(i)_v(n - i)_v^i} \left( (i)_v + v^i (n - i)_v \right)
\]

which clearly equals $\left(\frac{n}{i}\right)_v$. (2) follows from (1) with $i$ replaced by $n - i$, and (3) follows from (1) by induction on $n$. \qed

Let $q$ be any element in $k$, and let $n, i \in N_0$ with $i \leq n$. Lemma 1.9.3 allows us to define the $q$-numbers and $q$-binomial numbers $(n)_q$ and $\left(\frac{n}{i}\right)_q$ in $k$ as the images of $(n)_v$ and $\left(\frac{n}{i}\right)_v$ under the ring homomorphism $\mathbb{Z}[v] \rightarrow k$ mapping $v$ onto $q$.

**Lemma 1.9.4.** Let $n \geq 2$ and let $q \in k$ be a primitive $n$-th root of unity. Then $\left(\frac{n}{i}\right)_q = 0$ for all $0 < i < n$.

**Proof.** By assumption, $q \neq 1$. Hence $(m)_q = (q^m - 1)/(q - 1)$ for any $m \in N_0$. Let $0 < i < n$. Then $(i)_q^i (n - i)_q^i \neq 0$ in $k$ by assumption. Hence

\[
\left(\frac{n}{i}\right)_q = \frac{(n)_q^i}{(i)_q^i (n - i)_q^i} = 0
\]

in $k$, since $(n)_q = 0$. \qed

For any ring $A$, let $Z(A) = \{a \in A \mid ax = xa \text{ for all } x \in A \}$ denote its **center**.

**Proposition 1.9.5.** Let $A$ be an algebra, $q \in Z(A)$, and $x, y \in A$. Assume that $yx = qxy$. For all $0 \leq i \leq n$, let $\left(\frac{n}{i}\right)_q \in A$ be the image of $\left(\frac{n}{i}\right)_v$ under the ring homomorphism $\mathbb{Z}[v] \rightarrow A$ mapping $v$ onto $q$. Then for all $n \geq 0$,

\[
(x + y)^n = \sum_{i=0}^n \left(\frac{n}{i}\right)_q x^i y^{n-i} = \sum_{i=0}^n \left(\frac{n}{i}\right)_q x^{n-i} y^i.
\]

**Proof.** This follows by induction on $n$ as in the proof of the usual binomial formula using $yx^i = q^i x^iy$ for all $i \geq 0$, and Lemma 1.9.3(1). \qed
Example 1.9.6. Let us consider the special case of Theorem 1.9.1 when $V = kx$ is one-dimensional. Then there is a non-zero scalar $q \in k$ such that the braiding is given by $c(x \otimes x) = qx \otimes x$. Let $n \geq 2$ and $w \in S_n$. The linear map $c_w : V^\otimes n \to V^\otimes n$ is multiplication with the scalar $q^{\ell(w)}$, and by (1.8.9) we see that

$$S_{i,n-i} = S_{i,n-i} + q^{n-i}S_{i-1,n-i}$$

in $\text{End}(V^\otimes n)$ for all $1 \leq i \leq n-1$. These formulas are the recursion formulas for the $q$-binomial coefficients, see Lemma 1.9.3(2). Hence

$$S_{i,n-i} = \binom{n}{i}_q \text{id} \quad \text{for all } 0 \leq i \leq n,$$

where the second formula follows from (1.8.10).

By Theorem 1.9.1,

$$\Delta_{i,n-i}(x^n) = S_{i,n-i}(x^n) = \binom{n}{i}_q x^i \otimes x^{n-i}.\quad (1.9.2)$$

The same result follows from the $q$-binomial formula in Proposition 1.9.5. Indeed,

$$\Delta(x^n) = (x \otimes 1 + 1 \otimes x)^n = \sum_{i=0}^{n} \binom{n}{i}_q x^i \otimes x^{n-i}.\quad (1.9.4)$$

We will now see that explicit relations of the Nichols algebra are given by the braided symmetrizer maps.

Corollary 1.9.7. Let $n \geq 2$, and let $S_n = S_n^{(V,c)} : V^\otimes n \to V^\otimes n$ be the braided symmetrizer map.

1. $\Delta_{1,n} = S_n$ in $\text{End}(V^\otimes n)$, where $\Delta$ is the comultiplication of the tensor algebra $T(V)$.
2. $B(V) = k \oplus V \oplus \bigoplus_{n \geq 2} V^\otimes n / \ker(S_n)$.

Proof. (1) We proceed by induction on $n$. The case when $n = 1$ is trivial. Let $n \geq 2$, and assume that $\Delta_{1,n-1} = S_{n-1}$. Then

$$\Delta_{1,n} = (\Delta_1 \otimes \Delta_{1,n-1}) \Delta_{1,n-1} = (S_1 \otimes S_{n-1})S_{1,n-1} = S_n,$$

where the first equation holds by Lemma 1.3.13(1b), the second by induction and Theorem 1.9.1, and the third was shown in (1.8.10).

(2) follows from (1) and Definition 1.6.17. □

Corollary 1.9.8. Let $n \geq 2$, $1 \leq i \leq n-1$, and for all $1 \leq j \leq n$ let $\pi_j : V^\otimes j \to V^\otimes j / \ker(S_j)$ be the canonical map. Then

$$\ker(\Delta_{1,n}^{T(V)}) = \ker((\pi_i \otimes \pi_{n-i})S_{1,n-1}).$$

Proof. The claim follows directly from Corollary 1.9.7 and (1.8.10), since $\ker(S_i \otimes S_{n-i}) = \ker(\pi_i \otimes \pi_{n-i})$. □

It is important to note that the Nichols algebra $B(V) = T(V)/I(V)$ as an algebra and a coalgebra only depends on the braided vector space $(V,c)$. Let $G'$ be
another group, and \( V' \in G_G^G \mathcal{YD} \) such that there is a linear isomorphism \( f : V \to V' \) with
\[
(f \otimes f)c_{V,V} = (f \otimes f)c_{V',V'}.
\]
Then \( f \) induces an isomorphism \( B(V) \to B(V') \) of algebras and coalgebras.

### 1.10. Examples of Nichols algebras

We are going to describe several examples of Nichols algebras.

Throughout we will use the following notation for algebras given by **generators and relations**. Let \( X \) be a set, and let \( f_i, g_i \in k\langle X \rangle \), \( i \in I \), be elements in the free algebra, where \( I \) is some index set. Let \( \langle f_i - g_i \mid i \in I \rangle \) be the ideal of \( k\langle X \rangle \) generated by the elements \( f_i - g_i \), \( i \in I \). Then
\[
k\langle X \mid f_i = g_i \text{ for all } i \in I \rangle = k\langle X \rangle/(f_i - g_i \mid i \in I)
\]
is the algebra generated by \( X \) with relations \( f_i = g_i \), \( i \in I \). By abuse of notation we denote the residue class of \( x \in X \) in \( k\langle X \mid f_i = g_i \text{ for all } i \in I \rangle \) by the same symbol \( x \).

In the whole section let \( G \) be a group.

The Nichols algebra of a one-dimensional object \( V \in G_G^G \mathcal{YD} \) is easy to compute.

**Example 1.10.1.** Let \( V \in G_G^G \mathcal{YD} \) be one-dimensional with basis \( x \in V \), and \( c = c_{V,V} \). Then there is a non-zero scalar \( q \) such that \( c(x \otimes x) = qx \otimes x \). Let
\[
N(q) = \begin{cases} 
\text{ord}(q) & \text{if } q \neq 1 \text{ and } \text{ord}(q) \text{ is finite}, \\
p & \text{if } q = 1 \text{ and } \text{char}(k) = p > 0, \\
\infty & \text{otherwise}.
\end{cases}
\]

Thus if \( (m)_q = 0 \) for some natural number \( m \geq 2 \), then \( N(q) \) is the smallest such \( m \); otherwise \( N(q) = \infty \). We have seen in (1.9.3) that \( S_n = (n)_q\text{id} \). Hence \( I(V) = \bigoplus_{n \geq N} kx^n \) in \( T(V) = k[x] \), and
\[
B(V) \cong \begin{cases} k[x]/(x^{N(q)}) & \text{if } N(q) \neq \infty, \\
k[x] & \text{otherwise}.
\end{cases}
\]

**Example 1.10.2.** Let \( V \in G_G^G \mathcal{YD} \) be finite-dimensional with basis \( x_1, \ldots, x_\theta \) and \( x_i \in V^N_{q_i} \), \( g_i \in G \), \( \chi_i \in \hat{G} \) for all \( 1 \leq i \leq \theta \). Assume that \( \text{char}(k) = 0 \), and that \( B(V) \) is finite-dimensional. Then for all \( 1 \leq i \leq \theta \), \( \chi_i(g_i) \neq 1 \). This follows from Example 1.10.1 and Remark 1.6.19.

In the next two examples we discuss Nichols algebras of irreducible but not one-dimensional Yetter-Drinfeld modules over non-abelian groups.

**Example 1.10.3.** Let \( V_n, n \geq 3 \), be the irreducible Yetter-Drinfeld module in \( G_{n+2}^1 \mathcal{YD} \) in Example 1.4.7 with basis \( x_t, t \in \mathcal{O}_2 \). Then the quadratic relations of \( B(V_n) \) in \( \ker(\text{id}_{V(\otimes 2)} + c) \) are
\[
x_t^2 = 0 \text{ for all } t \in \mathcal{O}_2,
\]
\[
x_sx_t + x_tx_s = 0 \text{ for all } s,t \in \mathcal{O}_2 \text{ with } st = ts, s \neq t,
\]
\[
x_sx_t + x_{t\triangleright s} + x_{t\triangleright s}x_s = 0 \text{ for all } s,t \in \mathcal{O}_2 \text{ with } st \neq ts.
\]
Let $\tilde{B}(V_n) = T(V_n)/\langle x \in V_n^{\otimes 2} \mid c(x) = -x \rangle$ be the algebra generated by $x_t$, $t \in \mathcal{O}_2$, with the above quadratic relations of the Nichols algebra only. It is known that

$$\dim \tilde{B}(V_3) = 12, \quad \dim \tilde{B}(V_4) = 576, \quad \dim \tilde{B}(V_5) = 8,294,400,$$

and that $B(V_n) = \tilde{B}(V_n)$ for $n = 3, 4, 5$. For $n = 3, 4$ this was shown in [MS00], and for $n = 5$ by M. Graña (with help by J.-E. Roos). But for $n \geq 6$, the Nichols algebra of $V_n$ is a mystery. It is not even known whether $\tilde{B}(V_n)$ is finite-dimensional for one $n \geq 6$.

**Example 1.10.4.** Let $(X, \triangleright)$ and $q$ be the rack and constant two-cocycle in Example 1.5.13 with $X = \{1, 2, 3, 4\}$ and $\lambda = -1$. We write $x_i$ for the basis vector of $kX$ corresponding to $i \in X$. Then $(kX, c^\lambda)$ is a braided vector space of group type by Proposition 1.5.12. By Proposition 1.5.6, $kX \in \mathcal{G}YD$ for some group $G$. The Nichols algebra of $kX$ appeared first in [Gn00b]. We follow the presentation in [HV18]. The Nichols algebra $B(kX)$ can be presented as an algebra by generators $x_i$, $i \in X$, and relations

$$x_1^2 = x_2^2 = x_3^2 = x_4^2 = 0,$$
$$x_1x_2 + x_2x_3 + x_3x_1 = 0,$$
$$x_1x_3 + x_3x_4 + x_4x_1 = 0,$$
$$x_1x_4 + x_4x_2 + x_2x_1 = 0,$$
$$x_2x_4 + x_4x_3 + x_3x_2 = 0,$$
$$(x_1 + x_2 + x_3)^6 = 0.$$

Let $y = x_1x_3 + x_3x_2 + x_2x_1 \in B(kX)$. The elements

$$x_1^{n_1}(x_1 + x_2)^{n_2}x_3^{n_3}y^{n_4}x_4^{n_4}, \text{ where } n_1, n_3, n_4 \in \{0, 1\}, n_2, n_0 \in \{0, 1, 2\},$$

form a basis of $B(kX)$. In particular, $\dim B(kX) = 72$. Note that the quadratic relations of $B(kX)$ can easily be obtained using Corollary 1.9.8.

For the next example we need the logarithm of an automorphism.

**Lemma 1.10.5.** Assume that $\text{char}(k) = 0$. Let $V$ be a vector space and let $\mu : V \times V \to V$, $\mu(u, v) = uv$, be a bilinear map. Let $\sigma$ be an automorphism of $(V, \mu)$. Assume that $\sigma - \text{id}$ is locally nilpotent, that is, for all $v \in V$ there is $m \geq 0$ with $(\sigma - \text{id})^m(v) = 0$. Then

$$\log(\sigma) = \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m} (\sigma - \text{id})^m \in \text{End}(V)$$

is a derivation of $(V, \mu)$, that is, $\log(\sigma)(uv) = \log(\sigma)(u)v + u \log(\sigma)(v)$ for all $u, v \in V$.

**Proof.** Let $x = \sigma - \text{id}$. First note that for any $k \geq 1$,

$$(1.10.2) \quad \sigma^k \sum_{n=0}^{\infty} (-1)^n \binom{n + k - 1}{k - 1} x^n = \text{id}_V$$

in $\text{End}(V)$. Indeed the claim is true for $k = 1$, and for $k > 1$ it follows by induction on $k$ by substituting $\sigma^k = \sigma^{k-1}(x + \text{id}_V)$. 

For any \( v \in V \), \( \log(\sigma)(v) \) is well-defined since \( x \) is locally nilpotent. Moreover, \( x(uv) = x(u)\sigma(v) + ux(v) \) for all \( u, v \in V \). Since \( x \) and \( \sigma \) are commuting endomorphisms, it follows for any \( u, v \in V \) that
\[
\log(\sigma)(uv) = \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m} x^m(uv)
\]
\[
= \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m} \sum_{k=0}^{m} \binom{m}{k} x^k(u)\sigma^k x^{m-k}(v)
\]
\[
= u \log(\sigma)(v) + \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k(u) \sum_{m=k}^{\infty} \frac{(-1)^{m+1}}{m} \binom{m}{k} \sigma^k x^{m-k}(v)
\]
\[
= u \log(\sigma)(v) + \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k(u) \sum_{n=0}^{\infty} (-1)^n \binom{n+k-1}{k-1} \sigma^k x^n(v)
\]
\[
= u \log(\sigma)(v) + \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} x^k(u) v
\]
where (1.10.2) is used in the fifth equation. This proves the claim. \( \square \)

**Example 1.10.6.** Assume that \( \text{char}(k) = 0 \). Let \( J^+ = F_g(V(1, 2)) \in \mathcal{YD} \) be the Yetter-Drinfeld module in Example 1.4.19. Thus \( J^+ = J_g^+ \), where \( g \) is a generator of \( Z \), and there is a basis \( v_1, v_2 \) of \( J^+ \) such that \( g \cdot v_1 = v_1, g \cdot v_2 = v_2 + v_1 \). We prove that
\[
\mathcal{B}(J^+) = k\langle v_1, v_2 \rangle / (v_2v_1 - v_1v_2 + \frac{1}{2} v_1^2)
\]
and that the monomials
\[
(1.10.3) \quad v_1^k v_2^l, \quad k, l \geq 0,
\]
form a basis of \( \mathcal{B}(J^+) \).

Let \( x = v_2v_1 - v_1v_2 + \frac{1}{2} v_1^2 \in T(J^+) \). Then
\[
\Delta_{T(J^+)}(x) = x \otimes 1 + 1 \otimes x + v_2 \otimes v_1 + v_1 \otimes v_2
\]
\[
- v_1 \otimes v_2 - (v_1 + v_2) \otimes v_1 + v_1 \otimes v_1
\]
\[
= x \otimes 1 + 1 \otimes x.
\]
Hence \( x = 0 \) in \( \mathcal{B}(J^+) \). Hence \( \mathcal{B}(J^+) \) is spanned by the monomials \( v_1^k v_2^l, \) \( k, l \geq 0 \).

Let \( \sigma \) be the automorphism of the algebra \( \mathcal{B}(J^+) \) with \( \sigma(v) = g \cdot v \) for all \( v \in \mathcal{B}(J^+) \). Then \( \sigma - \text{id} \) is locally nilpotent, and hence \( \partial = \log(\sigma) \) is a derivation of \( \mathcal{B}(J^+) \) by Lemma 1.10.5. By definition, \( \partial(v_1) = 0, \partial(v_2) = v_1 \). Let \( i_1, \ldots, i_m \in \{1, 2\}, m \geq 1 \). Then by induction on \( n \) it follows that
\[
\partial^n(v_{i_1} \cdots v_{i_m}) = n! v_1^{i_1}
\]
where \( n = i_1 + \cdots + i_m - m \). Let \((a_i)_{0 \leq i \leq m} \in k^{m+1} \) with \( \sum_{i=0}^{m} a_i v_1^{m-i} v_2^i = 0 \), and let \( 0 \leq l_0 \leq m \) such that \( a_i = 0 \) for all \( i > l_0 \). Then
\[
\partial^{l_0} \left( \sum_{i=0}^{m} a_i v_1^{m-i} v_2^i \right) = a_{l_0} l_0! v_1^{i_1}.
\]
Since $v_l^m \neq 0$ by Example 1.10.1, it follows that $a_{l0} = 0$, and hence $a_l = 0$ for all $0 \leq l \leq m$ by induction on $m - l$. Hence the monomials in (1.10.3) are linearly independent in $B(J^+)$.

**Example 1.10.7.** Assume that $\text{char}(k) = 0$. Let $J^- = F_g(V(-1,2)) \in \mathcal{Z}_Y \mathcal{D}$ be the Yetter-Drinfeld module in Example 1.4.19. Thus $J^- = J_g^-$, where $g$ is a generator of $\mathbb{Z}$, and there is a basis $v_1, v_2$ of $J^-$ with $g \cdot v_1 = -v_1, g \cdot v_2 = -v_2 + v_1$. We prove that

$$B(J^-) = \mathbb{k}(v_1, v_2)/(v_1^2, v_2^2 - v_1 v_2 v_1)$$

and that the monomials

$$(1.10.4) \quad v_1^{a_1} (v_2 v_1)^{a_2} v_2^{a_3}, \quad a_1 \in \{0, 1\}, a_2, a_3 \geq 0,$$

form a basis of $B(J^-)$.

For all $k \geq 2$ let $\pi_k : (J^-)^{\otimes k} \to (J^-)^{\otimes k}/\ker(S_k)$ be the canonical map. Since $gv_1 = -v_1$, it follows that $c(v_1 \otimes v_1) = -v_1 \otimes v_1$ and hence $v_1^2 = 0$ in $B(J^-)$. Let $x = v_2^2 v_1 - v_1 v_2^2 - v_1 v_2 v_1 \in T(J^-)$. By Corollary 1.9.8, $x \in \ker(\Delta_{1^k})$ if and only if

$$(1.10.5) \quad (\text{id}_{J^-} \otimes \pi_2)S_{1,2}(x) = 0. \quad \text{Since } S_{1,2}(x) = 0 \text{, it follows that } x = 0 \text{ in } B(J^-), \text{ and therefore } \mathcal{B}(J^-) \text{ is spanned by the monomials in (1.10.4). Below we will further need that }$$

$$(1.10.6) \quad v_2(v_2v_1)^k = (v_1v_2)^kv_2 + k(v_1v_2)^kv_1$$

for all $k \geq 1$ which follows from $x = 0$ by induction on $k$.

Assume that there is a non-trivial linear combination of the monomials in (1.10.4) which is zero in $B(J^-)$. By multiplying this with $v_1$ from the left or $v_2$ from the right if necessary, it follows that there is $m \geq 2$, $m$ even, and a non-trivial linear combination of the monomials $v_1(v_2v_1)^{a}v_2^{m-1-2a}, 0 \leq a \leq (m-1)/2$, which is zero in $B(J^-)$.

Let $\sigma$ be the automorphism of the algebra $B(J^-)$, where $\sigma(v) = (-1)^n gv$ for all $v \in B(J^-)/(n)$, $n \geq 0$. Then $\sigma(v_1) = v_1, \sigma(v_2) = v_2 - v_1$, and the map $\sigma - \text{id}$ is locally nilpotent. Hence $\partial = -\log(\sigma)$ is a derivation of $B(J^-)$ by Lemma 1.10.5. By definition, $\partial(v_1) = 0, \partial(v_2) = v_1$. For any $n \geq 1$ let

$$M_n = \{(i_1, i_2, \ldots, i_{2n}) \in \{1, 2\}^{2n} \mid i_1 = 1, \forall 1 \leq k \leq n : i_{2k} = 2\}.$$ 

Since $v_l^2, x \in I(J^-)$, it follows by induction on $n$ that

$$(1.10.6) \quad \forall n \geq 1, (i_1, i_2, \ldots, i_{2n}) \in \{1, 2\}^{2n} \setminus M_n : v_1v_{i_2} \cdots v_{i_{2n}} = 0$$

in $B(J^-)$. Then by induction on $k$ it follows from (1.10.6) that

$$(1.10.7) \quad \partial^k(v_1i_2 \cdots v_{i_{2n}}) = k!(v_1v_2)^n, \quad \partial^{k+1}(v_1i_2 \cdots v_{i_{2n}}) = 0$$

in $B(J^-)$ for any $(i_1, \ldots, i_{2n}) \in M_n$, where $k = \sum_{j=1}^{n} i_{2j-1} - n$ is the number of 2’s at the odd positions. Let $(a_l)_{0 \leq l \leq m/2} \in \mathbb{k}^{m/2}$ be such that

$$\sum_{l=0}^{m/2-1} a_l(v_1v_2)^{m/2-1}v_2^{2l} = 0$$
in \( B(J^-) \), and let \( 0 \leq l_0 < m/2 \) with \( a_l = 0 \) for all \( l > l_0 \). Then

\[
\partial^{l_0} \left( \sum_{l=0}^{m/2-1} a_l (v_1 v_2)^{m/2-l} v_2^l \right) = a_{l_0} l_0! (v_1 v_2)^{m/2}
\]

by (1.10.7). We prove that for any \( n \geq 1 \), \((v_1 v_2)^n\) and \((v_2 v_1)^n\) are linearly independent in \( B(J^-) \). Then it follows that \( a_{l_0} = 0 \), and hence \( a_l = 0 \) for all \( 0 \leq l < m/2 \) by induction on \( m/2 - l \). Hence the monomials in (1.10.4) are linearly independent in \( B(J^-) \).

Since

\[
\begin{align*}
(1.10.8) & \quad S_{1,1}(v_1 v_2) = v_1 \otimes v_2 + (-v_2 + v_1) \otimes v_1, \\
(1.10.9) & \quad S_{1,1}(v_2 v_1) = v_2 \otimes v_1 - v_1 \otimes v_2,
\end{align*}
\]

the monomials \( v_1 v_2 \) and \( v_2 v_1 \) are linearly independent in \( B(J^-) \). Let now \( n \geq 1 \) and assume that \((v_1 v_2)^n\) and \((v_2 v_1)^n\) are linearly independent. Then

\[
(id \otimes \pi_{2n}) S_{1,2n}((v_1 v_2)^n v_1) = v_1 \otimes (v_2 v_1)^n + g^2 v_1 \otimes (v_1 v_2)^n
\]

by (1.10.6), and hence \((v_1 v_2)^n v_1 \neq 0\) by (1.8.9).

Let now \( \lambda_1, \lambda_2 \in \mathbb{k} \). Then

\[
(id \otimes \pi_{2n+1}) S_{1,2n+1}(\lambda_1 (v_1 v_2)^n v_1 + \lambda_2 (v_2 v_1)^n v_1) = \lambda_1 (v_1 \otimes (v_2 v_1)^n v_2 + g^2 v_1 \otimes (v_1 v_2)^n + g^2 v_1 \otimes (v_1 v_2)^n)
\]

\[
+ \lambda_2 (v_2 \otimes (v_1 v_2)^n + g v_1 \otimes (v_2 v_1)^n + g^2 v_1 \otimes (v_2 v_1)^n)
\]

\[
= (\lambda_2 - \lambda_1) v_2 \otimes (v_1 v_2)^n v_1 + (\lambda_1 - \lambda_2) v_1 \otimes (v_2 v_1)^n v_2
\]

\[
+ (\lambda_1 - \lambda_2) v_1 \otimes (v_2 v_1)^n v_2 + (\lambda_1 (2n+1) - \lambda_2 n) v_1 \otimes (v_2 v_1)^n v_1,
\]

where the first equation follows from (1.10.6), and the second from (1.10.5). Since \((v_1 v_2)^n v_1 \neq 0\), we conclude from (1.8.9) that \((v_1 v_2)^{n+1}\) and \((v_2 v_1)^{n+1}\) are linearly independent. This finishes the proof.

As Example 1.10.1 shows, it can happen that the tensor algebra of an object \( V \in \mathcal{G} \mathcal{Y} \mathcal{D} \) is strictly graded, or equivalently that \( I(V) = 0 \). In the next proposition we find general necessary conditions for \( I(V) \neq 0 \).

**Lemma 1.10.8.** Let \((V, c)\) be a braided vector space, \( n \geq 2 \), and assume that \( S_{n-1,1}^{(V, c)} \neq 0 \) is not an isomorphism. Then

\[
\ker(id_{V^\otimes n} - c^2_{m-1} c_{m-2} \cdots c_1) \neq 0
\]

for some \( 2 \leq m \leq n \).

**Proof.** The identity of Proposition 1.8.13(2) in the group algebra of the braid group implies the following equation in \( \text{Aut}(V^\otimes n) \), \( n \geq 2 \).

\[
S_{n-1,1}(id_{V^\otimes n} - c_{n-1} c_{n-2} \cdots c_1)(id_{V^\otimes n} - c_{n-1} c_{n-2} \cdots c_2) \cdots (id_{V^\otimes n} - c_{n-1})
\]

\[
= (id_{V^\otimes n} - c^2_{n-1} c_{n-2} \cdots c_1)(id_{V^\otimes n} - c^2_{n-1} c_{n-2} \cdots c_2) \cdots (id_{V^\otimes n} - c^2_{n-1}).
\]

Thus \( \ker(id_{V^\otimes n} - c^2_{n-1} c_{n-2} \cdots c_1) \neq 0 \) for some \( 1 \leq i \leq n-1 \), since \( S_{n-1,1} \) is not an isomorphism. The lemma follows with \( m = n - i + 1 \). \( \square \)

**Proposition 1.10.9.** Let \( V \in \mathcal{G} \mathcal{Y} \mathcal{D} \) be finite-dimensional with \( \dim V = d \), \( c = c_{V,V} \), and assume that \( I(V) \neq 0 \).
There exists \( n \geq 2 \), such that \( \ker(\text{id}_V \otimes r - c^2_{n-1}c_{n-2} \cdots c_1) \neq 0 \).

If the braiding is diagonal with matrix \((q_{a,b})_{1 \leq a, b \leq d}\), then there is an integer \( n \geq 2 \) and a sequence \((k_1, \ldots, k_n) \in \{1, \ldots, d\}^n\) such that

\[
\prod_{1 \leq i < j \leq n} q_{k_i, k_j} q_{k_j, k_i} = 1.
\]

**Proof.** (1) The tensor algebra \( T(V) \) is not strictly graded, since \( I(V) \neq 0 \). Hence by Proposition 1.3.14 and Theorem 1.9.1,

\[
\Delta_{n-1,1} = S_{n-1,1} : V^\otimes n \rightarrow V^\otimes n
\]

is not injective for some \( n \geq 2 \). Thus (1) follows from Lemma 1.10.8.

(2) By (1) there is an integer \( n \geq 2 \) and a non-zero element \( x \in V^\otimes n \) such that \( c^2_{n-1}c_{n-2} \cdots c_1(x) = x \). Let \( x_1, \ldots, x_d \) be a basis of \( V \) such that

\[
c(x_a \otimes x_b) = q_{a,b} x_b \otimes x_a \text{ for all } a, b \in \{1, \ldots, d\}.
\]

Then there is a unique presentation of \( x = \sum_{k = (k_1, \ldots, k_n) \in \{1, \ldots, d\}^n} \alpha_k x_k \) with \( \alpha_k \in \mathbb{k} \) for all \( k \in \{1, \ldots, d\}^n \), where \( x_k = x_{k_1} \otimes \cdots \otimes x_{k_n} \). Now

\[
c^2_{n-1}c_{n-2} \cdots c_1(x_{k_1} \otimes \cdots \otimes x_{k_n}) = \sum_{k=k_1,k_3} q_{k_1,k_2} q_{k_1,k_3} q_{k_3,k_{n-1}} q_{k_1,k_n} q_{k_n,k_1} x_{k_2} \otimes x_{k_3} \otimes \cdots \otimes x_{k_{n-1}} \otimes x_{k_1} \otimes x_{k_n},
\]

\[
(c^2_{n-1}c_{n-2} \cdots c_1)^{n-1}(x_{k_1} \otimes \cdots \otimes x_{k_n}) = \prod_{1 \leq i < j \leq n} q_{k_i, k_j} q_{k_j, k_i} x_{k_1} \otimes \cdots \otimes x_{k_n}.
\]

Since \( c^2_{n-1}c_{n-2} \cdots c_1(x) = x \), it follows that \( (c^2_{n-1}c_{n-2} \cdots c_1)^{n-1}(x) = x \), which implies (2) by the above equations. \( \square \)

**Example 1.10.10.** Let \( 0 \neq V \in \mathcal{G}YD \) be finite-dimensional, \( c = c_{V,V} \), such that \( c(x \otimes y) = qy \otimes x \) for all \( x, y \in V \), where \( 0 \neq q \in \mathbb{k} \). Then by Example 1.10.1 and Proposition 1.10.9(2), the following are equivalent.

(1) \( B(V) = T(V) \).

(2) (a) \( q \) is not a root of 1, or

(b) \( q = 1 \), \( \dim V = 1 \), and \( \text{char}(\mathbb{k}) = 0 \).

One of the main problems we want to discuss in this book is the structure of the Nichols algebra of a direct sum of objects in \( \mathcal{G}YD \).

We now study the easy case of a direct sum \( V_1 \oplus V_2 \) of subobjects \( V_1, V_2 \) of \( V \) in \( \mathcal{G}YD \) such that

\[
\text{id}_{V_i \otimes V_j} = (V_i \otimes V_j \xrightarrow{c_{V_i,V_j}} V_j \otimes V_i \xrightarrow{c_{V_j,V_i}} V_i \otimes V_j)
\]

for all \( i \neq j \).

For a Hopf algebra \( H \) in \( \mathcal{G}YD \) let

\[
\text{ad} = (H \otimes H \xrightarrow{\Delta \otimes \text{id}_H} H \otimes H \otimes H \xrightarrow{\text{id}_H \otimes c_{H,H}} H \otimes H \otimes H \xrightarrow{\text{id}_H \otimes \mu_H} H \otimes H \xrightarrow{\mu_r(\text{id}_H \otimes \mu_H)} H)
\]

be the braided adjoint action.

For elements \( x, y \in H \), we write

\[
\text{ad}(x \otimes y) = \text{ad}(x(y)) = \text{ad}_c(x(y)), \text{ where } c = c_{H,H}.
\]
If \( x \in P(H) \), \( y \in H \), then \( \text{ad} \, x(y) = xy - (x_{(-1)} \cdot y)x_{(0)} \) is the braided commutator of \( x \) and \( y \). If \( x \in P(H) \) is homogeneous of degree \( g \in G \), then
\[
\text{ad} \, x(y) = xy - (g \cdot y)x.
\]

**Lemma 1.10.11.** Let \( H \) be a Hopf algebra in \( G \mathrm{YD} \) with braiding \( c = c_{H,H} \), and \( x, y \in P(H) \). Then
\[
\Delta(\text{ad} \, x(y)) = \text{ad} \, x(y) \otimes 1 + 1 \otimes \text{ad} \, x(y) + (\text{id}_{H \otimes H} - c^2)(x \otimes y)
\]

**Proof.** Let \( x \) be homogeneous of degree \( g \in G \). Then
\[
\begin{align*}
\Delta(\text{ad} \, x(y)) &= \Delta(x)\Delta(y) - (g \cdot \Delta(y))\Delta(x) \\
&= (x \otimes 1 + 1 \otimes x)(y \otimes 1 + 1 \otimes y) \\
&\quad - (g \cdot y \otimes 1 + 1 \otimes g \cdot y)(x \otimes 1 + 1 \otimes x) \\
&\quad - (g \cdot y)\Delta(x) \\
&= xy \otimes 1 + x \otimes y + g \cdot y \otimes x + 1 \otimes xy \\
&\quad - (g \cdot y)x \otimes 1 - g \cdot y \otimes x - c(g \cdot y \otimes x) - 1 \otimes (g \cdot y)x \\
&= \text{ad} \, x(y) \otimes 1 + 1 \otimes \text{ad} \, x(y) + (\text{id}_{H \otimes H} - c^2)(x \otimes y).
\end{align*}
\]

\[
\square
\]

**Proposition 1.10.12.** Let \( V_1, V_2 \in G \mathrm{YD} \), \( V = V_1 \oplus V_2 \), and \( c = c_{V,V} \). For all \( 1 \leq i \leq 2 \), identify \( B(V_i) \) with the image of the injective map \( B(V_i) \to B(V) \) induced by the inclusion \( V_i \subseteq V \) (see Remark 1.6.19).

1. The multiplication map \( B(V_1) \otimes B(V_2) \xrightarrow{\mu_{12}} B(V) \) is an injective map of \( \mathbb{N}_0 \)-graded coalgebras in \( G \mathrm{YD} \), where \( B(V_1) \otimes B(V_2) \) is the tensor product of coalgebras in \( G \mathrm{YD} \).

2. The following are equivalent.
   (a) \( \mu_{12} \) is bijective.
   (b) \( c^2|_{V_2} \otimes V_1 = \text{id}_{V_2 \otimes V_1} \).
   (c) \( B(V_1) \otimes B(V_2) \) is a Hopf algebra in \( G \mathrm{YD} \), where the coalgebra and algebra structure is the tensor product of coalgebras and of algebras in \( G \mathrm{YD} \).

If (c) holds, then \( \mu_{12} \) is an isomorphism of Hopf algebras in \( G \mathrm{YD} \).

Proposition 1.10.12 and its proof below generalize directly to pairs of Yetter-Drinfeld modules over Hopf algebras with bijective antipode using the definitions in Section 7.1.

**Proof.** (1) By Remark 1.6.19, the inclusion maps \( V_i \subseteq V \), \( 1 \leq i \leq 2 \), define injective morphisms of \( \mathbb{N}_0 \)-graded Hopf algebras \( B(V_i) \to B(V) \) in \( G \mathrm{YD} \) which we view as inclusions. The map
\[
\mu_{12} = (B(V_1) \otimes B(V_2) \subseteq B(V) \otimes B(V) \xrightarrow{\mu} B(V))
\]
is a coalgebra homomorphism by Proposition 1.6.7. Hence the tensor product coalgebra \( B(V_1) \otimes B(V_2) \) in \( G \mathrm{YD} \) is an \( \mathbb{N}_0 \)-graded subcoalgebra of \( B(V) \otimes B(V) \). By Proposition 1.3.17, the coalgebra \( B(V_1) \otimes B(V_2) \) is strictly graded with
\[
P(B(V_1) \otimes B(V_2)) = V_1 \otimes 1 + 1 \otimes V_2.
\]
Since \( \mu_{12} \) defines an isomorphism \( V_1 \otimes 1 + 1 \otimes V_2 \to V_1 \oplus V_2 \), we conclude with Corollary 1.3.11 that \( \mu_{12} \) is injective.
(2) (a) ⇒ (b). By (a), \( \mathcal{B}(V_1)\mathcal{B}(V_2) = \mathcal{B}(V) \), and \( V_1V_2 + V_1^2 + V_2^2 = \mathcal{B}^2(V) \). By Definition 1.6.17 and Corollary 1.9.7, the symmetrizer maps \( \text{ad} \) bijective by Proposition 1.10.12. Hence span the vector space \( \mathcal{B}^2(V) \) surjective.

Recall that \( S_2 \) is the tensor product algebra. Then by Theorem 1.6.18, there is a surjective map called a quantum linear space. Note that

\[
(\text{id} - c^2)(a) = S_2(\text{id} - c)(a) = S_2(b + u_1 + u_2)
\]

for some \( b \in V_1 \otimes V_2 \), \( u_1 \in V_1 \otimes V_1 \), \( u_2 \in V_2 \otimes V_2 \). Since \( c^2(a) \in V_2 \otimes V_1 \) and \( c(b) \in V_2 \otimes V_1 \), it follows that \( b = 0 \) and \( S_2(a) = c(a) = 0 \).

(b) ⇒ (c). Assume that \( c^2| V_2 \otimes V_1 = \text{id}| V_2 \otimes V_1 \). Let \( x \in V_1 \), \( y \in V_2 \). By Lemma 1.10.11, \( \text{ad}(y(x)) \) is primitive, hence

\[
0 = \text{ad}(y(x)) = yx - \mu_{\mathcal{B}(V)}c(y \otimes x)
\]

in \( \mathcal{B}(V) \), and \( \mu_{12} : \mathcal{B}(V_1) \otimes \mathcal{B}(V_2) \to \mathcal{B}(V) \) is an algebra map, where \( \mathcal{B}(V_1) \otimes \mathcal{B}(V_2) \) is the tensor product algebra. Then \( \mu_{12} \) is an isomorphism, since the algebra \( \mathcal{B}(V) \) is generated by \( V_1 \) and \( V_2 \). This proves (c).

(c) ⇒ (a). By (c), \( R = \mathcal{B}(V_1) \otimes \mathcal{B}(V_2) \) is a pre-Nichols algebra of \( V_1 \otimes 1 \oplus 1 \otimes V_2 \). By Theorem 1.6.18, there is a surjective map \( \pi : R \to \mathcal{B}(V) \) of Hopf algebras in \( \mathcal{G}_D \), where \( \pi(1) \) is the isomorphism \( V_1 \otimes 1 \oplus 1 \otimes V_2 \cong V \). Then \( \pi = \mu_{12} \) is surjective.

We combine Example 1.10.1 with Proposition 1.10.12.

**Example 1.10.13.** Let \( (q_{ij})_{1 \leq i,j \leq n} \), \( n \geq 2 \), be a family of non-zero scalars in \( \mathbb{k} \) with \( q_{ij}q_{ji} = 1 \) for all \( i \neq j \). For all \( 1 \leq i \leq n \), we define \( N_i = N(q_{ii}) \). Let \( V \in \mathcal{G}_D \) be a vector space with basis \( x_1, \ldots, x_n \) and diagonal braiding given by \( c(x_i \otimes x_j) = q_{ij}x_j \otimes x_i \) for all \( 1 \leq i,j \leq n \). Assume that the elements \( x_1, \ldots, x_n \) span one-dimensional subobjects of \( V \) in \( \mathcal{G}_D \). The braided vector space \( (V,c) \) is called a quantum linear space. Note that \( c^2(x_i \otimes x_j) = x_i \otimes x_j \) for all \( i \neq j \), and \( \text{ad}(x_i(x_j)) = x_i x_j - q_{ij}x_j x_i \) for all \( i,j \). Hence for all \( i \neq j \), \( x_i x_j = q_{ij}x_j x_i \in \mathcal{B}(V) \) by Lemma 1.10.11. Let

\[
A = \mathbb{k}\langle x_1, \ldots, x_n | x_i x_j = q_{ij}x_j x_i, x_k^{N_k} = 0 \text{ for all } i,j,k \leq n, 1 \leq k \leq n \rangle.
\]

By Example 1.10.1, there is a well-defined algebra map

\[
\varphi : A \to \mathcal{B}(V), \quad x_i \mapsto x_i \text{ for all } 1 \leq i \leq n.
\]

It is clear from the relations that the elements \( x_1^{t_1} \cdots x_n^{t_n}, 0 \leq t_i < N_i, 1 \leq i \leq n \), span the vector space \( A \). (Here, \( t < \infty \) for all \( t \in \mathbb{N}_0 \).) Their images under \( \varphi \) are a basis of \( \mathcal{B}(V) \), since the multiplication map \( \mathcal{B}(kx_1) \otimes \cdots \otimes \mathcal{B}(kx_n) \to \mathcal{B}(V) \) is bijective by Proposition 1.10.12. Hence \( \varphi \) is an isomorphism.
Example 1.10.14. Assume in Example 1.10.13 that \( q_{ij} = 1 \) for all \( i, j \), that is, 
\( c(x \otimes y) = y \otimes x \) for all \( x, y \in V \). Then by Example 1.10.13,
\[
\mathcal{B}(V) \cong \begin{cases} 
S(V), \text{the symmetric algebra of } V, & \text{if } \text{char}(k) = 0; \\
S(V)/(v^p \mid v \in V), & \text{if } \text{char}(k) = p > 0.
\end{cases}
\]

Example 1.10.15. (a) Assume in Example 1.10.13 that \( q_{ij} = -1 \) for all \( i, j \), 
that is, \( c(x \otimes y) = -y \otimes x \) for all \( x, y \in V \). By Example 1.10.13, 
\[
\mathcal{B}(V) \cong k(x_1, \ldots, x_n \mid x_i^2 = 0, x_i x_j + x_j x_i = 0 \text{ for all } i \neq j) \cong \Lambda(V)
\]
is the exterior algebra of \( V \) of dimension \( 2^n \). By Example 1.4.14, the braiding can 
be realized by a Yetter-Drinfeld module \( V \) over the group \( G \) of order 2.

(b) Let \( \text{char}(k) = 0 \), \( G = \{1, g\} \) the group with two elements, and \( \bar{G} = \{\varepsilon, \chi\} \), 
where \( \chi(g) = -1 \). Let \( V \in \mathfrak{x} \mathfrak{y} \mathfrak{D} \). Then \( V = V^\varepsilon \oplus V^\chi \) as \( kG \)-module. Assume that 
\( \mathcal{B}(V) \) is finite-dimensional. Then, by Example 1.10.2, \( V = V^\chi \) as Yetter-Drinfeld 
module. Hence \( \mathcal{B}(V) \cong \Lambda(V) \) by (a).

Example 1.10.16. Let \( \text{char}(k) = 0 \), and let \( V = V_0 \oplus V_1 \) be a finite-dimensional 
super vector space. By Example 1.4.14, \( V \in \mathfrak{x} \mathfrak{y} \mathfrak{D} \), where \( G = \mathbb{Z}/(2) \), and the 
braiding is given by 
\[
c_{V_0, V} = \tau : V_0 \otimes V \rightarrow V \otimes V_0, \quad c_{V, V_0} = \tau : V \otimes V_0 \rightarrow V_0 \otimes V,
\]
\[
c_{V_1, V_1} = -\tau : V_1 \otimes V_1 \rightarrow V_1 \otimes V_1,
\]
where \( \tau \) is the flip map. Then by Examples 1.10.13, 1.10.14 and 1.10.15,
\[
\mathcal{B}(V) \cong S(V_0) \otimes \Lambda(V_1)
\]
is the graded-symmetric algebra of \( V_0 \oplus V_1 \).

If the assumption on the braiding in Proposition 1.10.12(2) is not satisfied, then 
the description of \( \mathcal{B}(V_1 \oplus V_2) \) is much more difficult.

Without proof we mention the fundamental example of a Nichols algebra \( \mathcal{B}(V) \) 
coming from the theory of quantum groups. Here, the braiding of \( V \) is given by a 
Yetter-Drinfeld structure over a free abelian group of finite rank, and \( V \) is a direct 
sum of finitely many one-dimensional Yetter-Drinfeld modules \( V_i \). The Nichols 
algebras of each summand \( V_i \) are simply polynomial algebras in one variable, but 
\( \mathcal{B}(V) \) is given by the complicated quantum Serre relations.

Definition 1.10.17. Let \( I \) be a non-empty finite set. Recall from [Kac90, §1.1] 
that a (generalized) Cartan matrix \( A = (a_{ij})_{i,j \in I} \) is a matrix in \( \mathbb{Z}^{I \times I} \) such that 
\begin{enumerate}
\item \( a_{ii} = 2 \) and \( a_{jk} \leq 0 \) for all \( i, j, k \in I \) with \( j \neq k \),
\item \( a_{ij} = 0 \) if \( i, j \in I \) and \( a_{ij} = 0 \), then \( a_{ji} = 0 \).
\end{enumerate}
A Cartan matrix \( A = (a_{ij})_{i,j \in I} \) is called symmetrizable, if there are integers 
\( d_i \geq 1 \) for all \( i \in I \) such that \( d_i a_{ij} = d_j a_{ji} \) for all \( i, j \in I \). A Cartan matrix \( (a_{ij})_{i,j \in I} \) is called of finite type if it is symmetrizable and if the symmetric bilinear form 
\( (\cdot, \cdot) : \mathbb{R}^I \times \mathbb{R}^I \rightarrow \mathbb{R}, (x, y) \mapsto \sum_{i,j \in I} x_i d_i a_{ij} y_j \), 
is positive definite.

The classification of Cartan matrices of finite type is well-known and is easily 
obtained from the definition by induction on the cardinality of \( I \). We follow the 
convention in [Kac90, §4.8].
Theorem 1.10.18. Let $l \geq 1$. Then up to a bijection of the index set, the indecomposable Cartan matrices of finite type in $\mathbb{Z}^{l \times l}$, see Definition 10.1.15, are the following.

1. **Type $A_l$, $l \geq 1$**: $a_{ij} = \begin{cases} -1, & \text{if } |i - j| = 1, \\ 0, & \text{if } |i - j| \geq 2. \end{cases}$

Then $d_i = 1$ for all $1 \leq i \leq l$.

2. **Type $B_l$, $l \geq 2$**: $a_{ij} = \begin{cases} -1, & \text{if } |i - j| = 1, i \neq l, \\ -2, & \text{if } i = l, j = l - 1, \\ 0, & \text{if } |i - j| \geq 2. \end{cases}$

Then $d_i = 2$ for all $1 \leq i \leq l - 1$ and $d_l = 1$.

3. **Type $C_l$, $l \geq 3$**: $a_{ij} = \begin{cases} -1, & \text{if } |i - j| = 1, j \neq l, \\ -2, & \text{if } i = l - 1, j = l, \\ 0, & \text{if } |i - j| \geq 2. \end{cases}$

Then $d_i = 1$ for all $1 \leq i \leq l - 1$ and $d_l = 2$.

4. **Type $D_l$, $l \geq 4$**: $a_{ij} = -1$ if $|i - j| = 1$, $i, j < l$; $a_{l-2l} = a_{l,l-2} = -1$; $a_{ij} = 0$ otherwise, whenever $i \neq j$. Then $d_i = 1$ for all $1 \leq i \leq l$.

5. **Type $E_l$, $6 \leq l \leq 8$**: $a_{ij} = -1$ if $|i - j| = 1$, $i, j < l$; $a_{l-3l} = a_{l,l-3} = -1$; $a_{ij} = 0$ otherwise, whenever $i \neq j$. Then $d_i = 1$ for all $1 \leq i \leq l$.

6. **Type $F_4$, $l = 4$**: $a_{ij} = \begin{cases} -1, & \text{if } |i - j| = 1, (i,j) \neq (3,2), \\ 0, & \text{if } |i - j| \geq 2. \end{cases}$

$a_{32} = -2$. Then $d_1 = d_2 = 2$, $d_3 = d_4 = 1$.

7. **Type $G_2$, $l = 2$**: $a_{12} = -1$, $a_{21} = -3$. Then $d_1 = 3$, $d_2 = 1$.

In particular, for any such Cartan matrix $A$ there exist unique integers $d_i$, $1 \leq i \leq r$, such that $d_1a_{ij} = d_ja_{ji}$ for all $1 \leq i, j \leq r$, and $\{d_i \mid 1 \leq i \leq r\}$ is one of the sets $\{1\}$, $\{1, 2\}$, $\{1, 3\}$.

The following example is an immediate consequence of Theorem 1.10.18.

**Example 1.10.19.** A Cartan matrix $A \in \mathbb{Z}^{2 \times 2}$ is of finite type if and only if $a_{12}a_{21} \in \{0, 1, 2, 3\}$. An indecomposable Cartan matrix $A \in \mathbb{Z}^{3 \times 3}$ is of finite type if there exist $i, j, k \in \{1, 2, 3\}$ such that $a_{ik} = a_{ki} = 0$, $a_{ij} = a_{ji} = -1$, and $a_{jk}a_{kj} \in \{1, 2\}$.

**Example 1.10.20.** Let $q \in \mathbb{k}$ be non-zero and not a root of one, $G = \mathbb{Z}^n$ a free abelian group of rank $n \geq 1$ with basis $K_1, \ldots, K_n$, and $(a_{ij})_{i \leq i, j \leq n}$ a Cartan matrix of finite type, where $(d_ia_{ij})$ is symmetric and $d_i \in \{1, 2, 3\}$ for all $i$. We define a Yetter-Drinfeld module $V \in \mathcal{G}\mathcal{YD}$ with basis $x_i \in V_{K_i}$, $1 \leq i \leq n$, where $\chi_1, \ldots, \chi_n$ are characters of $\mathbb{Z}^n$ with $\chi_i(K_j) = q^{d_ia_{ij}}$ for all $1 \leq i, j \leq n$, that is $\deg(x_i) = K_i$, $g \cdot x_i = \chi_i(g)x_i$ for all $g \in G, 1 \leq i \leq n$. Then $V = \mathbb{k}x_1 \oplus \cdots \oplus \mathbb{k}x_n$ is the direct sum of one-dimensional Yetter-Drinfeld modules $\mathbb{k}x_i$. We prove in Theorem 16.2.5 that $B(V) \cong \mathbb{k}\langle x_1, \ldots, x_n \mid (ad x_i)^{1-a_{ij}}(x_j) = 0 \text{ for all } i \neq j \rangle$ is given by the quantum Serre relations. Thus $B(V) = U_q^+(\mathfrak{g})$, where $\mathfrak{g}$ is the semisimple Lie algebra defined by the matrix $(a_{ij})_{1 \leq i, j \leq n}$. 
We note that the elements \((\text{ad } x_i)^{1-a_{ij}}(x_j) \in T(V), i \neq j\), are primitive by Proposition 4.3.12, hence \(k \langle x_1, \ldots, x_n \mid (\text{ad } x_i)^{1-a_{ij}}(x_j) = 0 \text{ for all } i \neq j \rangle\) is a Hopf algebra in \(G^G_{\mathcal{YD}}\).

**Remark 1.10.21.** Nichols algebras of Yetter-Drinfeld modules play an important role in the classification theory of Hopf algebras. They appear naturally as subalgebras of graded Hopf algebras associated to the coradical filtration, see Corollary 7.1.17.

### 1.11. Notes

1.1. The first comultiplication appeared in a paper by Heinz Hopf [Hop41] written in German and published in the Ann. of Math. in 1941.

1.4. Yetter-Drinfeld modules over a Hopf algebra, in particular over a group algebra, together with their braiding were introduced 1990 by Yetter in [Yet90].

The explicit description of Yetter-Drinfeld modules over groups was given in the equivalent category of Hopf bimodules in several early papers, beginning with [Nic78] over finite abelian groups in the semisimple case, [DPR90] over finite groups over the complex numbers as modules over the Drinfeld double of the group algebra, and in the general case in [CR97].

1.5. The fruitful idea to describe braided vector spaces of group type by racks was introduced in [AGn03].

1.6. Nichols defined in [Nic78] a bialgebra of type one as the image of a canonical map from the tensor algebra to the cotensor algebra of a Hopf bimodule. Bialgebras of type one contain Nichols algebras as subalgebras. Hopf bimodules are equivalent to Yetter-Drinfeld modules, see Notes to Section 3.7. It was shown independently in several papers ([Sch96], [Ros95], [Róź96], [BD97]) that the Nichols algebra can be seen as the image of a canonical map from the tensor algebra to the shuffle algebra of the braided vector space. See the notes to Section 6.4 for the definition of the shuffle algebra which is dual to the braided tensor algebra.

1.7. We have found the notation \(\uparrow i\) for the shift operator in [IO09].

1.8. The equations in Proposition 1.8.13 appeared in [DK+97, Lemma 6.12].

1.9. Theorem 1.9.1 about the comultiplication of the tensor algebra already was shown in [HH92, Proposition 4.8].

The braided (anti)symmetrizer map was introduced by Woronowicz in [Wor89], where he defined the braiding for Hopf bimodules (which he called bicovariant bimodules). Corollary 1.9.7 describing the relations of the Nichols algebra as a Hopf algebra by the braided symmetrizer map was shown in the papers mentioned in the notes to Section 1.6, since the canonical map from the tensor algebra to the shuffle algebra is given by the quantum symmetrizer.
1.10. Proposition 1.10.9(2) is shown in [Fd+01, Corollary (5.2.b)], by a different method. Example 1.10.10 is a very special case of the main result of [HZ18], where the finite-dimensional braided vector spaces $V$ of diagonal type satisfying $B(V) = T(V)$ are determined.

Proposition 1.10.12 also holds for the general braidings in Chapter 7. The equivalence of (a) and (b) was first shown in [Gn00a] for finite-dimensional Nichols algebras.