Introduction to Hopf algebras and representations

Kalle Kytölä
Department of Mathematics and Statistics
University of Helsinki

Spring semester 2011

Contents

Chapter 1

Preliminaries in linear algebra

During most parts of this course, vector spaces are over the field $\mathbb{C}$ of complex numbers. Often any other algebraically closed field of characteristic zero could be used instead. In some parts these assumptions are not used, and $\mathbb{K}$ denotes any field. We usually omit explicitly mentioning the ground field, which should be clear from the context.

Definition 1.1. Let V, W be $\mathbb{K}$-vector spaces. The space of linear maps (i.e. the space of homomorphisms of $\mathbb{K}$-vector spaces) from V to W is denoted by

$$\mathrm{Hom}(V, W) = \Big\{ T : V \to W \;\Big|\; T \text{ is a } \mathbb{K}\text{-linear map} \Big\}.$$

The vector space structure on $\mathrm{Hom}(V, W)$ is with pointwise addition and scalar multiplication. The (algebraic) dual of a vector space V is the space of linear maps from V to the ground field,

$$V^* = \mathrm{Hom}(V, \mathbb{K}).$$

We denote the duality pairing by brackets $\langle \cdot, \cdot \rangle$. The value of a dual vector $\varphi \in V^*$ on a vector $v \in V$ is thus usually denoted by $\langle \varphi, v \rangle$.

Definition 1.2. For $T : V \to W$ a linear map, the transpose is the linear map $T^* : W^* \to V^*$ defined by

$$\langle T^*(\varphi), v \rangle = \langle \varphi, T(v) \rangle \qquad \text{for all } \varphi \in W^*,\ v \in V.$$

1.1 On diagonalization of matrices

In this section, vector spaces are over the field $\mathbb{C}$ of complex numbers.

Recall first the following definitions.

Definition 1.3. The characteristic polynomial of a matrix $A \in \mathbb{C}^{n \times n}$ is

$$p_A(x) = \det\Big(x\mathbb{I} - A \Big).$$

The minimal polynomial of a matrix A is the polynomial q_A of smallest positive degree such that $q_A(A) = 0$, with the coefficient of highest degree term equal to 1.

The Cayley-Hamilton theorem states that the characteristic polynomial evaluated at the matrix itself is the zero matrix, that is $p_A(A) = 0$ for any square matrix A. An equivalent statement is that the polynomial $q_A(x)$ divides $p_A(x)$. These facts follow explicitly from the Jordan normal form discussed later in this section.

Motivation and definition of generalized eigenvectors

Given a square matrix A, it is often convenient to diagonalize A. This means finding an invertible matrix P ("a change of basis"), such that the conjugated matrix $P\,A\,P^{-1}$ is diagonal. If, instead of matrices, we think of a linear operator A from vector space V to itself, the equivalent question is finding a basis for V consisting of eigenvectors of A.

Recall from basic linear algebra that (for example) any real symmetric matrix can be diagonalized. Unfortunately, this is not the case with all matrices.

Example 1.4. Let $\lambda \in \mathbb{C}$ and

$$A = \begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix} \in \mathbb{C}^{3\times 3}.$$

The characteristic polynomial of A is

$$p_A(x) = \det(x\mathbb{I} - A) = (x-\lambda)^3,$$

so we know that A has no other eigenvalues but λ. It follows from $\det(A - \lambda\mathbb{I}) = 0$ that the eigenspace pertaining to the eigenvalue λ is nontrivial, $\dim(\mathrm{Ker}\,(A-\lambda\mathbb{I})) > 0$. Note that

$$A - \lambda\mathbb{I} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix},$$

so that the image of A is two dimensional, $\dim(\mathrm{Im}\,(A-\lambda\mathbb{I})) = 2$. By rank-nullity theorem,

$$\dim(\mathrm{Im}\,(A-\lambda\mathbb{I})) + \dim(\mathrm{Ker}\,(A-\lambda\mathbb{I})) = \dim\left(\mathbb{C}^3\right) = 3,$$

so the eigenspace pertaining to λ must be one-dimensional. Thus the maximal number of linearly independent eigenvectors of A we can have is one — in particular, there doesn't exist a basis of $\mathbb{C}^3$ consisting of eigenvectors of A.

We still take a look at the action of A in some basis. Let

$$w_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \qquad w_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \qquad w_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}.$$

Then the following "string" indicates how $A - \lambda\mathbb{I}$ maps these vectors

$$w_3 \overset{A-\lambda}{\mapsto} w_2 \overset{A-\lambda}{\mapsto} w_1 \overset{A-\lambda}{\mapsto} 0.$$

In particular we see that $(A-\lambda\mathbb{I})^3 = 0$.

The "string" in the above example illustrates and motivates the following definition.

Definition 1.5. Let V be a vector space and $A : V \to V$ be a linear map. A vector $v \in V$ is said to be a generalized eigenvector of eigenvalue λ if for some positive integer p we have $(A - \lambda\mathbb{I})^p\, v = 0$. The set of these generalized eigenvectors is called the generalized eigenspace of A pertaining to eigenvalue λ.

With $p = 1$ the above would correspond to the usual eigenvectors.

The Jordan canonical form

Although not every matrix has a basis of eigenvectors, we will see that every complex square matrix has a basis of generalized eigenvectors. More precisely, if V is a finite dimensional complex vector space and $A : V \to V$ is a linear map, then there exists eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_k$ of A (not necessarily distinct) and a basis $\{w_m^{(j)} \; : \; 1 \leq j \leq k, 1 \leq m \leq n_j\}$ of V which consists of "strings" as follows

$$\begin{array}{ccccccccccc}
w_{n_1}^{(1)} & \overset{A-\lambda_1}{\mapsto} & w_{n_1-1}^{(1)} & \overset{A-\lambda_1}{\mapsto} & \cdots & \overset{A-\lambda_1}{\mapsto} & w_2^{(1)} & \overset{A-\lambda_1}{\mapsto} & w_1^{(1)} & \overset{A-\lambda_1}{\mapsto} & 0 \\
w_{n_2}^{(2)} & \overset{A-\lambda_2}{\mapsto} & w_{n_2-1}^{(2)} & \overset{A-\lambda_2}{\mapsto} & \cdots & \overset{A-\lambda_2}{\mapsto} & w_2^{(2)} & \overset{A-\lambda_2}{\mapsto} & w_1^{(2)} & \overset{A-\lambda_2}{\mapsto} & 0 \\
 & & & & & & \vdots & & \vdots & & \vdots \\
w_{n_k}^{(k)} & \overset{A-\lambda_k}{\mapsto} & w_{n_k-1}^{(k)} & \overset{A-\lambda_k}{\mapsto} & \cdots & \overset{A-\lambda_k}{\mapsto} & w_2^{(k)} & \overset{A-\lambda_k}{\mapsto} & w_1^{(k)} & \overset{A-\lambda_k}{\mapsto} & 0.
\end{array} \tag{1.1}$$

Note that in this basis the matrix of A takes the "block diagonal form"

$$A = \begin{bmatrix} J_{\lambda_1;n_1} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & J_{\lambda_2;n_2} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & J_{\lambda_3;n_3} & & \mathbf{0} \\ \vdots & \vdots & & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & J_{\lambda_k;n_k} \end{bmatrix}, \tag{1.2}$$

where the blocks correspond to the subspaces spanned by $w_1^{(j)}, w_2^{(j)}, \ldots, w_{n_j}^{(j)}$ and the matrices of the blocks are the following "Jordan blocks"

$$J_{\lambda_j;n_j} = \begin{bmatrix} \lambda_j & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda_j & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda_j & & 0 & 0 \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_j & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda_j \end{bmatrix} \in \mathbb{C}^{n_j \times n_j}.$$

Definition 1.6. A matrix of the form (1.2) is said to be in Jordan normal form (or Jordan canonical form).

The characteristic polynomial of the a matrix A in Jordan canonical form is

$$p_A(x) = \det(x\mathbb{I} - A) = \prod_{j=1}^{k} (x - \lambda_j)^{n_j}.$$

Note also that if we write a block $J_{\lambda;n} = \lambda\mathbb{I} + N$ as a sum of diagonal part $\lambda\mathbb{I}$ and upper triangular part N, then the latter is nilpotent: $N^n = 0$. In particular the assertion $p_A(A) = 0$ of the Cayley-Hamilton theorem can be seen immediately for matrices which are in Jordan canonical form.

Definition 1.7. Two $n \times n$ square matrices A and B are said to be similar if $A = P\,B\,P^{-1}$ for some invertible matrix P.

It is in this sense that any complex square matrix can be put to Jordan canonical form, the matrix P implements a change of basis to a basis consisting of the strings of the above type. Below is a short and concrete proof.

Theorem 1.8
Given any complex $n \times n$ matrix A, there exists an invertible matrix P such that the conjugated matrix $P\,A\,P^{-1}$ is in Jordan normal form.

Proof. In view of the above discussion it is clear that the statement is equivalent to the following: if V is a finite dimensional complex vector space and $A : V \to V$ a linear map, then there exists a basis of V consisting of strings as in (1.1).

We prove the statement by induction on $n = \dim(V)$. The case $n = 1$ is clear. As an induction hypothesis, assume that the statement is true for all linear maps of vector spaces of dimension less than n.

Take any eigenvalue λ of A (any root of the characteristic polynomial). Note that

$$\dim(\mathrm{Ker}(A - \lambda \mathbb{I})) > 0,$$

and since $n = \dim(\mathrm{Ker}(A - \lambda\mathbb{I})) + \dim(\mathrm{Im}(A - \lambda\mathbb{I}))$, the dimension of the image of $A - \lambda\mathbb{I}$ is strictly less than n. Denote

$$R \;=\; \mathrm{Im}(A - \lambda\mathbb{I}) \qquad \text{and} \qquad r \;=\; \dim(R) \;<\; n.$$

Note that R is an invariant subspace for A, that is $A\,R \subset R$ (indeed, $A\,(A - \lambda\mathbb{I})\,v = (A - \lambda\mathbb{I})\,A\,v$). We can use the induction hypothesis to the restriction of A to R, to find a basis

$$\{w_m^{(j)} \;:\; 1 \leq j \leq k, 1 \leq m \leq n_j\}$$

of R in which the action of A is described by the strings as in (1.1).

Let $q = \dim(R \;\cap\; \mathrm{Ker}(A - \lambda\mathbb{I}))$. This means that in R there are q linearly independent eigenvectors of A with eigenvalue λ. The vectors at the right end of the strings span the eigenspaces of A in R, so we assume without loss of generality that the last q strings correspond to eigenvalue λ and others to different eigenvalues: $\lambda_1, \lambda_2, \ldots, \lambda_{k-q} \neq \lambda$ and $\lambda_{k-q+1} = \lambda_{k-q+2} = \cdots = \lambda_k = \lambda$. For all j such that $k - q < j \leq k$ the vector $w_{n_j}^{(j)}$ is in R, so we can choose

$$y^{(j)} \in V \quad \text{such that} \quad (A - \lambda\mathbb{I})\,y^{(j)} \;=\; w_{n_j}^{(j)}.$$

The vectors $y^{(j)}$ extend the last q strings from the left.

Find vectors

$$z^{(1)}, z^{(2)}, \ldots, z^{(n-r-q)}$$

which complete the linearly independent collection

$$w_1^{(k-q+1)}, \ldots, w_1^{(k-1)}, w_1^{(k)}$$

to a basis of $\mathrm{Ker}(A - \lambda\mathbb{I})$. We have now found n vectors in V, which form strings as follows

$$\begin{array}{ccccccccc}
 & & & & & & z^{(1)} & \overset{A-\lambda}{\mapsto} & 0 \\
 & & & & & & \vdots & & \vdots \\
 & & & & & & z^{(n-r-q)} & \overset{A-\lambda}{\mapsto} & 0 \\
 & & w_{n_1}^{(1)} & \overset{A-\lambda_1}{\mapsto} & \cdots & \overset{A-\lambda_1}{\mapsto} & w_1^{(1)} & \overset{A-\lambda_1}{\mapsto} & 0 \\
 & & \vdots & & & & \vdots & & \vdots \\
 & & w_{n_{k-q}}^{(k-q)} & \overset{A-\lambda_{k-q}}{\mapsto} & \cdots & \overset{A-\lambda_{k-q}}{\mapsto} & w_1^{(k-q)} & \overset{A-\lambda_{k-q}}{\mapsto} & 0 \\
y^{(k-q+1)} & \overset{A-\lambda}{\mapsto} & w_{n_{k-q+1}}^{(k-q+1)} & \overset{A-\lambda}{\mapsto} & \cdots & \overset{A-\lambda}{\mapsto} & w_1^{(k-q+1)} & \overset{A-\lambda}{\mapsto} & 0 \\
\vdots & & \vdots & & & & \vdots & & \vdots \\
y^{(k)} & \overset{A-\lambda}{\mapsto} & w_{n_k-1}^{(k)} & \overset{A-\lambda}{\mapsto} & \cdots & \overset{A-\lambda}{\mapsto} & w_1^{(k)} & \overset{A-\lambda}{\mapsto} & 0.
\end{array}$$

It suffices to show that these vectors are linearly independent. Suppose that a linear combination of them vanishes

$$\sum_{j=k-q+1}^{k} \alpha_j\, y^{(j)} + \sum_{j,m} \beta_{j,m}\, w_m^{(j)} + \sum_{l=1}^{n-r-q} \gamma_l\, z^{(l)} \;=\; 0.$$

From the string diagram we see that the image of this linear combination under $A - \lambda\mathbb{I}$ is a linear combination of the vectors $w_m^{(j)}$, which are linearly independent, and since the coefficient of $w_{n_j}^{(j)}$ is α_j, we get $\alpha_j = 0$ for all j. Now recalling that $\{w_m^{(j)}\}$ is a basis of R, and $\{w_1^{(j)} : k - q < j \leq k\} \cup \{z^{(l)}\}$ is a basis of $\mathrm{Ker}\,(A - \lambda\mathbb{I})$, and $\{w_1^{(j)} : k - q < j \leq k\}$ is a basis of $R \cap \mathrm{Ker}\,(A - \lambda\mathbb{I})$, we see that all the coefficients in the linear combination must vanish. This finishes the proof. □

Exercise 1 (Around the Jordan normal form)

(a) *Find two matrices $A, B \in \mathbb{C}^{n\times n}$, which have the same minimal polynomial and the same characteristic polynomial, but which are not similar.*

(b) *Show that the Jordan normal form of a matrix $A \in \mathbb{C}^{n\times n}$ is unique up to permutation of the Jordan blocks. In other words, if $C_1 = P_1\,A\,P_1^{-1}$ and $C_2 = P_2\,A\,P_2^{-1}$ are both in Jordan normal form, C_1 with blocks $J_{\lambda_1,n_1}, \ldots J_{\lambda_k;n_k}$ and C_2 with blocks $J_{\lambda'_1,n'_1}, \ldots J_{\lambda'_l;n'_l}$, then $k = l$ and there is a permutation $\sigma \in S_k$ such that $\lambda_j = \lambda'_{\sigma(j)}$ and $n_j = n'_{\sigma(j)}$ for all $j = 1, 2, \ldots, k$.*

(c) *Show that any two matrices with the same Jordan normal form up to permutation of blocks are similar.*

Let us make some preliminary remarks of the interpretation of Jordan decomposition from the point of view of representations. We will return to this when we discuss representations of algebras, but a matrix determines a representation of the quotient of the polynomial algebra by the ideal generated by the minimal polynomial of the matrix. Diagonalizable matrices can be thought of as a simple example of completely reducible representations: the vector space V is a direct sum of eigenspaces of the matrix. In particular, if all the roots of the minimal polynomial have multiplicity one, then all representations are completely reducible. Non-diagonalizable matrices are a simple example of a failure of complete reducibility. The Jordan blocks $J_{\lambda_j;n_j}$ correspond to subrepresentations (invariant subspaces) which are indecomposable, but not irreducible if $n_j > 1$.

1.2 On tensor products of vector spaces

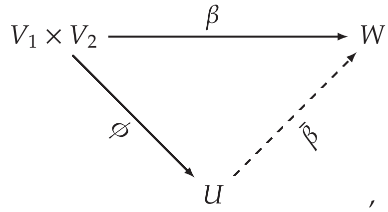
A crucial concept in the course is that of a tensor product of vector spaces. Here, vector spaces can be over any field $\mathbb{K}$, but it should be noted that the concept of tensor product depends of the field. In this course we only need tensor products of complex vector spaces.

Definition 1.9. Let V_1, V_2, W be vector spaces. A map $\beta : V_1 \times V_2 \to W$ is called bilinear if for all $v_1 \in V_1$ the map $v_2 \mapsto \beta(v_1, v_2)$ is linear $V_2 \to W$ and for all $v_2 \in V_2$ the map $v_1 \mapsto \beta(v_1, v_2)$ is linear $V_1 \to W$.

Multilinear maps $V_1 \times V_2 \times \cdots \times V_n \to W$ are defined similarly.

The tensor product is a space which allows us to replace some bilinear (more generally multilinear) maps by linear maps.

Definition 1.10. Let V_1 and V_2 be two vector spaces. A tensor product of V_1 and V_2 is a vector space U together with a bilinear map $\phi : V_1 \times V_2 \to U$ such that the following universal property holds: for any bilinear map $\beta : V_1 \times V_2 \to W$, there exists a unique linear map $\bar{\beta} : U \to W$ such that the diagram



,

commutes, that is $\beta = \bar{\beta} \circ \phi$.

Proving the uniqueness (up to canonical isomorphism) of an object defined by a universal isomorphism is a standard exercise in abstract nonsense. Indeed, if we suppose U' with a bilinear map $\phi' : V_1 \times V_2 \to U'$ is another tensor product, then the universal property of U gives a linear map $\bar{\phi}' : U \to U'$ such that $\phi' = \bar{\phi}' \circ \phi$. Likewise, the universal property of U' gives a linear map $\bar{\phi} : U' \to U$ such that $\phi = \bar{\phi} \circ \phi'$. Combining these we get

$$\mathrm{id}_U \circ \phi \;=\; \phi \;=\; \bar{\phi} \circ \phi' \;=\; \bar{\phi} \circ \bar{\phi}' \circ \phi.$$

But here are two ways of factorizing the map ϕ itself, so by the uniqueness requirement in the universal property we must have equality $\mathrm{id}_U = \bar{\phi} \circ \bar{\phi}'$. By a similar argument we get $\mathrm{id}_{U'} = \bar{\phi}' \circ \bar{\phi}$. We conclude that $\bar{\phi}$ and $\bar{\phi}'$ are isomorphisms (and inverses of each other).

Now that we know that tensor product is unique (up to canonical isomorphism), we use the following notations

$$U \;=\; V_1 \otimes V_2 \qquad \text{and}$$

$$V_1 \times V_2 \;\ni\; (v_1, v_2) \;\overset{\phi}{\mapsto}\; v_1 \otimes v_2 \;\in\; V_1 \otimes V_2.$$

An explicit construction which shows that tensor products exist is done in Exercise 2. The same exercise establishes two fundamental properties of the tensor product:

- If $(v_i^{(1)})_{i \in I}$ is a linearly independent collection in V_1 and $(v_j^{(2)})_{j \in J}$ is a linearly independent collection in V_2, then the collection $\left(v_i^{(1)} \otimes v_j^{(2)}\right)_{(i,j) \in I \times J}$ is linearly independent in $V_1 \otimes V_2$.
- If the collection $(v_i^{(1)})_{i \in I}$ spans V_1 and the collection $(v_j^{(2)})_{j \in J}$ spans V_2, then the collection $\left(v_i^{(1)} \otimes v_j^{(2)}\right)_{(i,j) \in I \times J}$ spans the tensor product $V_1 \otimes V_2$.

It follows that if $(v_i^{(1)})_{i \in I}$ and $(v_j^{(2)})_{j \in J}$ are bases of V_1 and V_2, respectively, then

$$\left(v_i^{(1)} \otimes v_j^{(2)}\right)_{(i,j) \in I \times J}$$

is a basis of the tensor product $V_1 \otimes V_2$. In particular if V_1 and V_2 are finite dimensional, then

$$\dim(V_1 \otimes V_2) \;=\; \dim(V_1)\, \dim(V_2)\,.$$

Exercise 2 (A construction of the tensor product)
We saw that the tensor product of vector spaces, defined by the universal property, is unique (up to isomorphism) if it exists. The purpose of this exercise is to show existence by an explicit construction, under the simplifying assumption that V and W are function spaces (it is easy to see that this can be assumed without loss of generality).

For any set X, denote by $\mathbb{K}^X$ the vector space of $\mathbb{K}$ valued functions on X, with addition and scalar multiplication defined pointwise. Assume that $V \subset \mathbb{K}^X$ and $W \subset \mathbb{K}^Y$ for some sets X and Y. For $f \in \mathbb{K}^X$ and $g \in \mathbb{K}^Y$, define $f \otimes g \in \mathbb{K}^{X \times Y}$ by

$$\big(f \otimes g\big)(x, y) \;=\; f(x)\, g(y).$$

Also set

$$V \otimes W \;=\; \mathrm{span}\left\{ f \otimes g \;\middle|\; f \in V,\; g \in W \right\},$$

so that the map $(f, g) \mapsto f \otimes g$ is a bilinear map $V \times W \to V \otimes W$.

(a) *Show that if $(f_i)_{i \in I}$ is a linearly independent collection in V and $(g_j)_{j \in J}$ is a linearly independent collection in W, then the collection $\left(f_i \otimes g_j\right)_{(i,j) \in I \times J}$ is linearly independent in $V \otimes W$.*

(b) *Show that if* $(f_i)_{i\in I}$ *is a collection that spans* V *and* $(g_j)_{j\in J}$ *is collection that spans* W*, then the collection* $\left(f_i \otimes g_j\right)_{(i,j)\in I\times J}$ *spans* $V \otimes W$*.*

(c) *Conclude that if* $(f_i)_{i\in I}$ *is a basis of* V *and* $(g_j)_{j\in J}$ *is a basis of* W*, then* $\left(f_i \otimes g_j\right)_{(i,j)\in I\times J}$ *is a basis of* $V \otimes W$*. Conclude furthermore that* $V \otimes W$*, equipped with the bilinear map* $\phi(f, g) = f \otimes g$ *from* $V \times W$ *to* $V \otimes W$*, satisfies the universal property defining the tensor product.*

A tensor of the form $v^{(1)} \otimes v^{(2)}$ is called a simple tensor. By part (b) of the above exercise, any $t \in V_1 \otimes V_2$ can be written as a linear combination of simple tensors

$$t = \sum_{\alpha=1}^{n} v_\alpha^{(1)} \otimes v_\alpha^{(2)},$$

for some $v_\alpha^{(1)} \in V_1$ and $v_\alpha^{(2)} \in V_2$, $\alpha = 1, 2, \ldots, n$. Note, however, that such an expression is by no means unique! The smallest n for which it is possible to write t as a sum of simple tensors is called the rank of the tensor, denoted by $n = \mathrm{rank}(t)$. An obvious upper bound is $\mathrm{rank}(t) \leq \dim(V_1)\dim(V_2)$. One can do much better in general, as follows from the following useful observation.

Lemma 1.11
Suppose that

$$t = \sum_{\alpha=1}^{n} v_\alpha^{(1)} \otimes v_\alpha^{(2)},$$

where $n = \mathrm{rank}(t)$*. Then both* $(v_\alpha^{(1)})_{\alpha=1}^n$ *and* $(v_\alpha^{(2)})_{\alpha=1}^n$ *are linearly independent collections.*

Proof. Suppose, by contraposition, that there is a linear relation

$$\sum_{\alpha=1}^{n} c_\alpha v_\alpha^{(1)} = 0,$$

where not all the coefficients are zero. We may assume that $c_n = 1$. Thus $v_n^{(1)} = -\sum_{\alpha=1}^{n-1} c_\alpha v_\alpha^{(1)}$ and using bilinearity we simplify t as

$$t = \sum_{\alpha=1}^{n-1} v_\alpha^{(1)} \otimes v_\alpha^{(2)} + v_n^{(1)} \otimes v_n^{(2)} = \sum_{\alpha=1}^{n-1} v_\alpha^{(1)} \otimes v_\alpha^{(2)} - \sum_{\alpha=1}^{n-1} c_\alpha\, v_\alpha^{(1)} \otimes v_n^{(2)} = \sum_{\alpha=1}^{n-1} v_\alpha^{(1)} \otimes \left(v_\alpha^{(1)} - c_\alpha v_n^{(2)}\right)$$

which contradicts minimality of $n = \mathrm{rank}(t)$. The linear independence of $(v_\alpha^{(2)})$ is proven similarly. □

As a consequence we get a better upper bound

$$\mathrm{rank}(t) \leq \min\{\dim(V_1), \dim(V_2)\}.$$

Taking tensor products with the one-dimensional vector space $\mathbb{K}$ does basically nothing: for any vector space V we can canonically identify

$$\begin{aligned} V \otimes \mathbb{K} &\cong V \\ v \otimes \lambda &\mapsto \lambda v \end{aligned} \qquad \text{and} \qquad \begin{aligned} \mathbb{K} \otimes V &\cong V \\ \lambda \otimes v &\mapsto \lambda v. \end{aligned}$$

By the obvious correspondence of bilinear maps $V_1 \times V_2 \to W$ and $V_2 \times V_1 \to W$, one also always gets a canonical identification

$$V_1 \otimes V_2 \cong V_2 \otimes V_1.$$

Almost equally obvious correspondences give the canonical identifications

$$(V_1 \otimes V_2) \otimes V_3 \;\cong\; V_1 \otimes (V_2 \otimes V_3)$$

etc., which allow us to omit parentheses in multiple tensor products.

A slightly more interesting property than the above obvious identifications, is the existence of an embedding

$$V_2 \otimes V_1^* \;\hookrightarrow\; \mathrm{Hom}(V_1, V_2)$$

which is obtained by associating to $v_2 \otimes \varphi$ the linear map

$$v_1 \;\mapsto\; \langle \varphi, v_1 \rangle \, v_2$$

(and extending linearly from the simple tensors to all tensors). The following exercise verifies among other things that this is indeed an embedding and that in the finite dimensional case the embedding becomes an isomorphism.

Exercise 3 (The relation between $\mathrm{Hom}(V, W)$ and $W \otimes V^*$)

(a) For $w \in W$ and $\varphi \in V^*$, we associate to $w \otimes \varphi$ the following map $V \to W$

$$v \;\mapsto\; \langle \varphi, v \rangle \, w.$$

Show that the linear extension of this defines an injective linear map

$$W \otimes V^* \;\longrightarrow\; \mathrm{Hom}(V, W).$$

(b) Show that if both V and W are finite dimensional, then the injective map in (a) is an isomorphism

$$W \otimes V^* \;\cong\; \mathrm{Hom}(V, W).$$

Show that under this identification, the rank of a tensor $t \in W \otimes V^*$ is the same as the rank of a matrix of the corresponding linear map $T \in \mathrm{Hom}(V, W)$.

Definition 1.12. When

$$f : V_1 \to W_1 \qquad \text{and} \qquad g : V_2 \to W_2$$

are linear maps, then there is a linear map

$$f \otimes g : V_1 \otimes V_2 \to W_1 \otimes W_2$$

defined by the condition

$$(f \otimes g)(v_1 \otimes v_2) \;=\; f(v_1) \otimes g(v_2) \qquad \text{for all } v_1 \in V_1,\; v_2 \in V_2.$$

The above map clearly depends bilinearly on (f, g), so we get a canonical map

$$\mathrm{Hom}(V_1, W_1) \otimes \mathrm{Hom}(V_2, W_2) \;\hookrightarrow\; \mathrm{Hom}(V_1 \otimes V_2, W_1 \otimes W_2),$$

which is easily seen to be injective. When all the vector spaces V_1, W_1, V_2, W_2 are finite dimensional, then the dimensions of both sides are given by

$$\dim(V_1)\;\dim(V_2)\;\dim(W_1)\;\dim(W_2)\,,$$

so in this case the canonical map is an isomorphism

$$\mathrm{Hom}(V_1, W_1) \otimes \mathrm{Hom}(V_2, W_2) \;\cong\; \mathrm{Hom}(V_1 \otimes V_2, W_1 \otimes W_2).$$

As a particular case of the above, interpreting the dual of a vector space V as $V^* = \mathrm{Hom}(V, \mathbb{K})$ and using $\mathbb{K} \otimes \mathbb{K} \cong \mathbb{K}$, we see that the tensor product of duals sits inside the dual of the tensor product. Explicitly, if V_1 and V_2 are vector spaces and $\varphi_1 \in V_1^*$, $\varphi_2 \in V_2^*$, then

$$v_1 \otimes v_2 \;\mapsto\; \langle \varphi_1, v_1 \rangle \langle \varphi_2, v_2 \rangle$$

defines an element of the dual of $V_1 \otimes V_2$. To summarize, we have an embedding

$$V_1^* \otimes V_2^* \hookrightarrow (V_1 \otimes V_2)^*.$$

If V_1 and V_2 are finite dimensional this becomes an isomorphism

$$V_1^* \otimes V_2^* \cong (V_1 \otimes V_2)^*.$$

As a remark, later in the course we will notice an asymmetry in the dualities between algebras and coalgebras, Theorems 3.34 and 3.45. This asymmetry is essentially due to the fact that in infinite dimensional case one only has an inclusion $V^* \otimes V^* \subset (V \otimes V)^*$ but not an equality.

The transpose behaves well under the tensor product of linear maps.

Lemma 1.13
When $f : V_1 \to W_1$ and $g : V_2 \to W_2$ are linear maps, then the map

$$f \otimes g : V_1 \otimes V_2 \to W_1 \otimes W_2$$

has a transpose $(f \otimes g)^*$ which makes the following diagram commute

$$\begin{array}{ccc} (W_1 \otimes W_2)^* & \xrightarrow{(f \otimes g)^*} & (V_1 \otimes V_2)^* \\ \uparrow & & \uparrow \\ W_1^* \otimes W_2^* & \xrightarrow[f^* \otimes g^*]{} & V_1^* \otimes V_2^*. \end{array}$$

Proof. Indeed, for $\varphi \in W_1^*$, $\psi \in W_2^*$ and any simple tensor $v_1 \otimes v_2 \in V_1 \otimes V_2$ we compute

$$\begin{aligned} \langle (f^* \otimes g^*)(\varphi \otimes \psi), v_1 \otimes v_2 \rangle &= \langle f^*(\varphi) \otimes g^*(\psi), v_1 \otimes v_2 \rangle \\ &= \langle f^*(\varphi), v_1 \rangle \, \langle g^*(\psi), v_2 \rangle \\ &= \langle \varphi, f(v_1) \rangle \, \langle \psi, g(v_2) \rangle \\ &= \langle \varphi \otimes \psi, f(v_1) \otimes g(v_2) \rangle \\ &= \langle \varphi \otimes \psi, (f \otimes g)(v_1 \otimes v_2) \rangle \\ &= \langle (f \otimes g)^*(\varphi \otimes \psi), v_1 \otimes v_2 \rangle. \end{aligned}$$

□

Chapter 2

Representations of finite groups

We begin by taking a brief look at the classical topic of representations of finite groups. Here many things are easier than later in the course when we discuss representations of "quantum groups". The most important result is that all finite dimensional representations are direct sums of irreducible representations, of which there are only finitely many.

2.1 Reminders about groups and related concepts

Definition 2.1. A group is a pair $(G, *)$, where G is a set and $*$ is a binary operation on G

$$*: G \times G \to G \qquad (g, h) \mapsto g * h$$

such that the following hold

"Associativity": $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ for all $g_1, g_2, g_3 \in G$

"Neutral element": there exists an element $e \in G$ s.t. for all $g \in G$ we have $g * e = g = e * g$

"Inverse": for any $g \in G$, there exists an element $g^{-1} \in G$ such that $g * g^{-1} = e = g^{-1} * g$

A group $(G, *)$ is said to be finite if its order $|G|$ (that is the cardinality of G) is finite.

We usually omit the notation for the binary operation $*$ and write simply $gh := g * h$. For the binary operation in abelian (i.e. commutative) groups we often, though not always, use the additive symbol $+$.

Example 2.2. The following are abelian groups

- a vector space V with the binary operation $+$ of vector addition
- the set $\mathbb{K} \setminus \{0\}$ of nonzero numbers in a field with the binary operation of multiplication
- the infinite cyclic group $\mathbb{Z}$ of integers with the binary operation of addition
- the cyclic group of order N consisting of all N^{th} complex roots of unity $\left\{e^{2\pi i k/N} \;\middle|\; k = 0, 1, 2, \ldots, N-1\right\}$, with the binary operation of complex multiplication.

We also usually abbreviate and write only G for the group $(G, *)$.

Example 2.3. Let X be a set. Then $S(X) := \{\sigma : X \to X \text{ bijective}\}$ with composition of functions is a group, called the symmetric group of X.

In the case $X = \{1, 2, 3, \ldots, n\}$ we denote the symmetric group by S_n.

Example 2.4. Let V be a vector space and $\mathrm{GL}(V) = \mathrm{Aut}(V) = \{A : V \to V \text{ linear bijection}\}$ with composition of functions as the binary operation. Then $\mathrm{GL}(V)$ is a group, called the general linear group of V (or the automorphism group of V). When V is finite dimensional, $\dim(V) = n$, and a basis of V has been chosen, then $\mathrm{GL}(V)$ can be identified with the group of $n \times n$ matrices having nonzero determinant, with matrix product as the group operation.

Let $\mathbb{K}$ be the ground field and $V = \mathbb{K}^n$ the standard n-dimensional vector space. In this case we denote $\mathrm{GL}(V) = \mathrm{GL}_n(\mathbb{K})$.

Example 2.5. The group D_4 of symmetries of a square, or the dihedral group of order 8, is the group with two generators

$$r \text{ “rotation by } \pi/2\text{”} \qquad m \text{ “reflection”}$$

and relations

$$r^4 = e \qquad m^2 = e \qquad rmrm = e.$$

Definition 2.6. Let $(G_1, *_1)$ and $(G_2, *_2)$ be groups. A mapping $f : G_1 \to G_2$ is said to be a (group) homomorphism if for all $g, h \in G_1$

$$f(g *_1 h) \;=\; f(g) *_2 f(h).$$

Example 2.7. The determinant function $A \mapsto \det(A)$ from the matrix group $\mathrm{GL}_n(\mathbb{C})$ to the multiplicative group of non-zero complex numbers, is a homomorphism since $\det(A\,B) = \det(A)\,\det(B)$.

The reader should be familiar with the notions of subgroup, normal subgroup, quotient group, canonical projection, kernel, isomorphism etc.

One of the most fundamental recurrent principles in mathematics is the isomorphism theorem. We recall that in the case of groups it states the following.

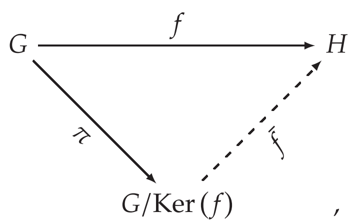
Theorem 2.8
Let G and H be groups and $f : G \to H$ a homomorphism. Then

1°) $\mathrm{Im}\,(f) := f(G) \subset H$ *is a subgroup.*

2°) $\mathrm{Ker}\,(f) := f^{-1}(\{e_H\}) \subset G$ *is a normal subgroup.*

3°) The quotient group $G/\mathrm{Ker}\,(f)$ *is isomorphic to* $\mathrm{Im}\,(f)$.

More precisely, there exists an injective homomorphism $\bar{f} : G/\mathrm{Ker}\,(f) \to \mathrm{Im}\,(f)$ *such that the following diagram commutes*



,

where $\pi : G \to G/\mathrm{Ker}\,(f)$ *is the canonical projection.*

The reader has surely encountered isomorphism theorems for several algebraic structures already — the following table summarizes the corresponding concepts in a few familiar cases

Structure	**Morphism** f	**Image** Im (f)	**Kernel** Ker (f)
group	group homomorphism	subgroup	normal subgroup
vector space	linear map	vector subspace	vector subspace
ring	ring homomorphism	subring	ideal
⋮	⋮	⋮	⋮

We will encounter isomorphism theorems for yet many other algebraic structures during this course: representations (modules), algebras, coalgebras, bialgebras, Hopf algebras, ... The idea is always the same, and the proofs only vary slightly, so we will not give full details in all cases.

A word of warning: since kernels, images, quotients etc. of different algebraic structures are philosophically so similar, we use the same notation for all. It should be clear from the context what is meant in each case. Usually, for example, Ker (ρ) would mean the kernel of a group homomorphism $\rho : G \to \mathrm{GL}(V)$ (a normal subgroup of G), whereas Ker $(\rho(g))$ would then signify the kernel of the linear map $\rho(g) : V \to V$ (a vector subspace of V, which incidentally is $\{0\}$ when $\rho(g) \in \mathrm{GL}(V)$).

2.2 Representations: Definition and first examples

Definition 2.9. Let G be a group and V a vector space. A representation of G in V is a group homomorphism $G \to \mathrm{GL}(V)$.

Suppose $\rho : G \to \mathrm{GL}(V)$ is a representation. For any $g \in G$, the image $\rho(g)$ is a linear map $V \to V$. When the representation ρ is clear from context (and maybe also when it is not), we denote the images of vectors by this linear map simply by $g.v := \rho(g)\, v \in V$, for $v \in V$. With this notation the requirement that ρ is a homomorphism reads $(g\,h).v = g.(h.v)$. It is convenient to interpret this as a left multiplication of vectors $v \in V$ by elements g of the group G. Thus interpreted, we say that V is a (left) G-module (although it would be more appropriate to call it a $\mathbb{K}[G]$-module, where $\mathbb{K}[G]$ is the group algebra of G).

Example 2.10. Let V be a vector space and set $\rho(g) = \mathrm{id}_V$ for all $g \in G$. This is called the trivial representation of G in V. If no other vector space is clear from the context, the trivial representation means the trivial representation in the one dimensional vector space $V = \mathbb{K}$.

Example 2.11. The symmetric group S_n for $n \geq 2$ has another one dimensional representation called the alternating representation. This is the representation given by $\rho(\sigma) = \mathrm{sign}(\sigma)\, \mathrm{id}_{\mathbb{K}}$, where $\mathrm{sign}(\sigma)$ is minus one when the permutation σ is the product of odd number of transpositions, and plus one when σ is the product of even number of transpositions.

Example 2.12. Let D_4 be the dihedral group of order 8, with generators r, m and relations $r^4 = e$, $m^2 = e$, $rmrm = e$. Define the matrices

$$R = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad \text{and} \qquad M = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Since $R^4 = \mathbb{I}$, $M^2 = \mathbb{I}$, $RMRM = \mathbb{I}$, there exists a homomorphism $\rho : D_4 \to \mathrm{GL}_2(\mathbb{R})$ such that $\rho(r) = R$, $\rho(m) = M$. Such a homomorphism is unique since we have given the values of it on generators r, m of D_4. If we think of the square in the plane $\mathbb{R}^2$ with vertices $A = (1, 0)$, $B = (0, 1)$, $C = (-1, 0)$, $D = (0, -1)$, then the linear maps $\rho(g)$, $g \in D_4$, are precisely the eight isometries of the plane which preserve the square $ABCD$. Thus it is very natural to represent the group D_4 in a two dimensional vector space!

A representation ρ is said to be faithful if it is injective, i.e. if Ker $(\rho) = \{e\}$. The representation of the symmetry group of the square in the last example is faithful, it could be taken as a defining representation of D_4.

When the ground field is $\mathbb{C}$, we might want to write the linear maps $\rho(g) : V \to V$ in their Jordan canonical form. But we observe immediately that the situation is as good as it could get:

Lemma 2.13
Let G be a finite group, V a finite dimensional (complex) vector space, and ρ a representation of G in V. Then, for any $g \in G$, the linear map $\rho(g) : V \to V$ is diagonalizable.

Proof. Observe that $g^n = e$ for some positive integer n (for example the order of the element g or the order of the group G). Thus we have $\rho(g)^n = \rho(g^n) = \rho(e) = \mathrm{id}_V$. This says that the minimal polynomial of $\rho(g)$ divides $x^n - 1$, which only has roots of multiplicity one. Therefore the Jordan normal form of $\rho(g)$ can only have blocks of size one. □

We still continue with an example (or definition) of representation that will serve as useful tool later.

Example 2.14. Let ρ_1, ρ_2 be two representations of a group G in vector spaces V_1, V_2, respectively. Then the space of linear maps between the two representations

$$\mathrm{Hom}(V_1, V_2) \;=\; \{T : V_1 \to V_2 \text{ linear}\}$$

becomes a representation by setting

$$g.T \;=\;= \rho_2(g) \circ T \circ \rho_1(g^{-1})$$

for all $T \in \mathrm{Hom}(V_1, V_2)$, $g \in G$. As usual, we often omit the explicit notation for the representations ρ_1, ρ_2, and write simply

$$(g.T)(v) = g.\Big(T(g^{-1}.v)\Big) \qquad \text{for any } v \in V_1.$$

To check that this indeed defines a representation, we compute

$$\Big(g_1.(g_2.T)\Big)(v) \;=\; g_1.\Big((g_2.T)(g_1^{-1}.v)\Big) \;=\; g_1.g_2.\Big(T(g_2^{-1}.g_1^{-1}.v)\Big) \;=\; g_1g_2.\Big(T\Big((g_1g_2)^{-1}.v\Big)\Big) \;=\; \Big((g_1g_2).T\Big)(v).$$

Definition 2.15. Let G be a group and V_1, V_2 two G-modules (=representations). A linear map $T : V_1 \to V_2$ is said to be a G-module map (sometimes also called a G-linear map) if $T(g.v) = g.T(v)$ for all $g \in G$, $v \in V$.

Note that $T \in \mathrm{Hom}(V_1, V_2)$ is a G-module map if and only if $g.T = T$ for all $g \in G$, when we use the representation of Example 2.14 on $\mathrm{Hom}(V_1, V_2)$. We denote by $\mathrm{Hom}_G(V_1, V_2) \subset \mathrm{Hom}(V_1, V_2)$ the space of G-module maps from V_1 to V_2.

Exercise 4 (Dual representation)
Let G be a finite group and $\rho : G \to \mathrm{GL}(V)$ be a representation of G in a finite dimensional (complex) vector space V.

(a) Show that any eigenvalue λ of $\rho(g)$, for any $g \in G$, satisfies $\lambda^{|G|} = 1$.

(b) Recall that the dual space of V is $V^* = \{f : V \to \mathbb{C} \text{ linear map}\}$. For $g \in G$ and $f \in V^*$ define $\rho'(g).f \in V^*$ by the formula

$$\langle \rho'(g).f, v\rangle = \langle f, \rho(g^{-1}).v\rangle \qquad \text{for all } v \in V.$$

Show that $\rho' : G \to \mathrm{GL}(V^*)$ is a representation.

(c) *Show that* $\mathrm{Tr}(\rho'(g))$ *is the complex conjugate of* $\mathrm{Tr}(\rho(g))$.

Exercise 5 (A two dimensional irreducible representation of S_3)
Find a two-dimensional irreducible representation of the symmetric group S_3.
Hint: *Consider the three-cycles, and see what different transpositions would do to the eigenvectors of a three-cycle.*

Definition 2.16. For G a group, an element $g_2 \in G$ is said to be conjugate to $g_1 \in G$ if there exists a $h \in G$ such that $g_2 = h\, g_1\, h^{-1}$. Being conjugate is an equivalence relation and conjugacy classes of the group G are the equivalence classes of this equivalence relation.

Exercise 6 (Dihedral group of order 8)
The group D_4 *of symmetries of the square is the group with two generators,* r *and* m*, and relations* $r^4 = e$, $m^2 = e$, $rmrm = e$.

(a) *Find the conjugacy classes of* D_4.

(b) *Find four non-isomorphic one dimensional representations of* D_4.

(c) *There exists a unique group homomorphism* $\rho : G \to \mathrm{GL}_2(\mathbb{C})$ *such that*

$$\rho(r) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad \rho(m) = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

(here, as usual, we identify linear maps $\mathbb{C}^2 \to \mathbb{C}^2$ *with their matrices in the standard basis). Check that this two dimensional representation is irreducible.*

2.3 Subrepresentations, irreducibility and complete reducibility

Definition 2.17. Let ρ be a representation of G in V. If $V' \subset V$ is a subspace and if $\rho(g)\, V' \subset V'$ for all $g \in G$ (we say that V' is an invariant subspace), then taking the restriction to the invariant subspace, $g \mapsto \rho(g)|_{V'}$ defines a representation of G in V' called a subrepresentation of ρ.

We also call V' a submodule of the G-module V.

The subspaces $\{0\} \subset V$ and $V \subset V$ are always submodules.

Example 2.18. Let $T : V_1 \to V_2$ be a G-module map. The image $\mathrm{Im}\,(T) = T(V_1) \subset V_2$ is a submodule, since a general vector of the image can be written as $w = T(v)$, and $g.w = g.T(v) = T(g.v) \in \mathrm{Im}\,(T)$. The kernel $\mathrm{Ker}\,(T) = T^{-1}(\{0\}) \subset V_1$ is a submodule, too, since if $T(v) = 0$ then $T(g.v) = g.T(v) = g.0 = 0$.

Example 2.19. When we consider $\mathrm{Hom}(V_1, V_2)$ as a representation as in Example 2.14, the subspace $\mathrm{Hom}_G(V_1, V_2) \subset \mathrm{Hom}(V_1, V_2)$ of G-module maps is a subrepresentation, which, by the remark after Definition 2.15, is a trivial representation in the sense of Example 2.10.

Definition 2.20. Let $\rho_1 : G \to \mathrm{GL}(V_1)$ and $\rho_2 : G \to \mathrm{GL}(V_2)$ be representations of G in vector spaces V_1 and V_2, respectively. Let $V = V_1 \oplus V_2$ be the direct sum vector space. The representation $\rho : G \to \mathrm{GL}(V)$ given by

$$\rho(g)(v_1 + v_2) = \rho_1(g)v_1 + \rho_2(g)v_2 \qquad \text{when } v_1 \in V_1 \subset V,\ v_2 \in V_2 \subset V$$

is called the direct sum representation of ρ_1 and ρ_2.

Both V_1 and V_2 are submodules of $V_1 \oplus V_2$.

Definition 2.21. Let $\rho_1 : G \to \mathrm{GL}(V_1)$ and $\rho_2 : G \to \mathrm{GL}(V_2)$ be two representations of G. We make the tensor product space $V_1 \otimes V_2$ a representation by setting for simple tensors

$$\rho(g)\,(v_1 \otimes v_2) \;=\; (\rho_1(g)v_1) \otimes (\rho_2(g)v_2)$$

and extending the definition linearly to the whole of $V_1 \otimes V_2$. Clearly for simple tensors we have

$$\rho(h)\rho(g)\,(v_1 \otimes v_2) \;=\; \Big(\rho_1(h)\rho_1(g)v_1\Big) \otimes \Big(\rho_2(h)\rho_2(g)v_2\Big) \;=\; \Big(\rho_1(hg)v_1\Big) \otimes \Big(\rho_2(hg)v_2\Big) \;=\; \rho(hg)\,(v_1 \otimes v_2)$$

and since both sides are linear, we have $\rho(h)\rho(g)\,t = \rho(hg)\,t$ for all $t \in V_1 \otimes V_2$, so that $\rho : G \to \mathrm{GL}(V_1 \otimes V_2)$ is indeed a representation.

A key property of representations of finite groups is that any invariant subspace has a complementary invariant subspace in the following sense. An assumption is needed of the ground field: we need to divide by the order of the group, so the order must not be a multiple of the characteristic of the field. In practise we only work with complex representations, so there is no problem.

Proposition 2.22
Let G be a finite group. If V' is a submodule of a G-module V, then there is a submodule $V'' \subset V$ such that $V = V' \oplus V''$ as a G-module.

Proof. First choose any complementary vector subspace U for V', that is $U \subset V'$ such that $V = V' \oplus U$ as a vector space. Let $\pi' : V \to V'$ be the canonical projection corresponding to this direct sum, that is

$$\pi'(v' + u) \;=\; v' \qquad \text{when } v' \in V',\ u \in U.$$

Define

$$\pi(v) \;=\; \frac{1}{|G|} \sum_{g \in G} g.\pi'(g^{-1}.v).$$

Observe that $\pi|_{V'} = \mathrm{id}_{V'}$ and $\mathrm{Im}\,(\pi) \subset V'$, in other words that π is a projection from V to V'. If we set $V'' = \mathrm{Ker}\,(\pi)$, then at least $V = V' \oplus V''$ as a vector space. To show that V'' is a subrepresentation, it suffices to show that π is a G-module map. This is checked by doing the change of summation variable $\tilde{g} = h^{-1}g$ in the following

$$\pi(h.v) \;=\; \frac{1}{|G|} \sum_{g \in G} g.\pi'(g^{-1}.h.v) \;=\; \frac{1}{|G|} \sum_{g \in G} g.\pi'\Big((h^{-1}g)^{-1}.v\Big) \;=\; \frac{1}{|G|} \sum_{\tilde{g} \in G} h\tilde{g}.\pi'\Big(\tilde{g}^{-1}.v\Big) \;=\; h.\pi(v).$$

We conclude that $V'' = \mathrm{Ker}\,(\pi) \subset V$ is a subrepresentation and thus $V = V' \oplus V''$ as a representation. □

Definition 2.23. Let $\rho : G \to \mathrm{GL}(V)$ be a representation. If there are no other subrepresentations but those corresponding to $\{0\}$ and V, then we say that ρ is an irreducible representation, or that V is a simple G-module.

Proposition 2.22, with an induction on dimension of the G-module V, gives the fundamental result about representations of finite groups called complete reducibility, as stated in the following. We will perform this induction in more detail in Proposition 3.18 when we discuss the complete reducibility and semisimplicity of algebras.

Corollary 2.24
Let G be a finite group and V a finite dimensional G-module. Then, as representations, we have

$$V \;=\; V_1 \oplus V_2 \oplus \cdots \oplus V_n,$$

where each subrepresentation $V_j \subset V$, $j = 1, 2, \ldots, n$, is an irreducible representation of G.

Exercise 7 (An example of tensor products and complete reducibility with D_4)
The group D_4 is the group with two generators, r and m, and relations $r^4 = e$, $m^2 = e$, $rmrm = e$. Recall that we have seen four one-dimensional and one two-dimensional irreducible representation of D_4 in Exercise 6. Let V be the two dimensional irreducible representation of D_4 given by

$$r \mapsto \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad m \mapsto \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Consider the four-dimensional representation $V \otimes V$, and show by an explicit choice of basis for $V \otimes V$ that it is isomorphic to a direct sum of the four one-dimensional representations.

We also mention the basic result which says that there is not much freedom in constructing G-module maps between irreducible representations. For the second statement below we need the ground field to be algebraically closed: in practise we use it only for complex representations.

Lemma 2.25 (Schur's Lemma)
If V and W are irreducible representations of a group G, and $T : V \to W$ is a G-module map, then

(i) either $T = 0$ or T is an isomorphism

(ii) if $V = W$, then $T = \lambda \, \mathrm{id}_V$ for some $\lambda \in \mathbb{C}$.

Proof. If $\mathrm{Ker}\,(T) \neq \{0\}$, then by irreducibility of V we have $\mathrm{Ker}\,(T) = V$ and therefore $T = 0$. If $\mathrm{Ker}\,(T) = \{0\}$, then T is injective and by irreducibility of W we have $\mathrm{Im}\,(T) = W$, so T is also surjective. This proves *(i)*. To prove *(ii)*, pick any eigenvalue λ of T (here we need the ground field to be algebraically closed). Now consider the G-module map $T - \lambda \mathrm{id}_V$, which has a nontrivial kernel. The kernel must be the whole space by irreducibility, so $T - \lambda \, \mathrm{id}_V = 0$. □

Exercise 8 (Irreducible representations of abelian groups) *(a) Let G be an abelian (=commutative) group. Show that any irreducible representation of G is one dimensional. Conclude that (isomorphism classes of) irreducible representations can be identified with group homomorphisms $G \to \mathbb{C}^*$.*

(b) Let $C_n \cong \mathbb{Z}/n\mathbb{Z}$ be the cyclic group of order n, i.e. the group with one generator c and relation $c^n = e$. Find all irreducible representations of C_n.

2.4 Characters

In the rest of this section G is a finite group of order $|G|$ and all representations are assumed to be finite dimensional.

We have already seen the fundamental result of complete reducibility: any representation of G is a direct sum of irreducible representations. It might nevertheless not be clear yet how to concretely work with the representations. We now introduce a very powerful tool for the representation theory of finite groups: the character theory.

Definition 2.26. For $\rho : G \to \mathrm{GL}(V)$ a representation, the character of the representation is the function $\chi_V : G \to \mathbb{C}$ given by

$$\chi_V(g) = \mathrm{Tr}(\rho(g)).$$

Observe that we have

$$\chi_V(e) = \dim(V)$$

and for two group elements that are conjugates, $g_2 = h g_1 h^{-1}$, we have

$$\chi_V(g_2) = \mathrm{Tr}(\rho(g_2)) = \mathrm{Tr}\left(\rho(h)\,\rho(g_1)\,\rho(h)^{-1}\right) = \mathrm{Tr}(\rho(g_1)) = \chi_V(g_1).$$

Thus the value of a character is constant on each conjugacy class of G (such functions $G \to \mathbb{C}$ are called class functions).

Example 2.27. We have seen three (irreducible) representations of the group S_3: the trivial representation U and the alternating representation U', both one dimensional, and the two-dimensional representation V in Exercise 5. The conjugacy classes of symmetric groups correspond to the cycle decompositions of a permutation — in particular for S_3 the conjugacy classes are

$$\begin{aligned} \text{identity} &: \{e\} \\ \text{transpositions} &: \{(12),(13),(23)\} \\ \text{3-cycles} &: \{(123),(132)\}. \end{aligned}$$

We can explicitly compute the trace of for example the transposition (12) and the three cycle (123) to get the characters of these representations

	$\chi(e)$	$\chi((12))$	$\chi((123))$
U	1	1	1
U'	1	−1	1
V	2	0	−1

Recall that we have seen how to make the dual V^* a representation (Exercise 4), how to make direct sum $V_1 \oplus V_2$ a representation (Definition 2.20) and also how to make the tensor product a representation (Definition 2.21). Let us now see how these operations affect characters.

Proposition 2.28
Let V, V_1, V_2 be representations of G. Then we have

(i) $\chi_{V^*}(g) = \overline{\chi_V(g)}$

(ii) $\chi_{V_1 \oplus V_2}(g) = \chi_{V_1}(g) + \chi_{V_2}(g)$

(iii) $\chi_{V_1 \otimes V_2}(g) = \chi_{V_1}(g)\,\chi_{V_2}(g)$.

Proof. Part (i) was done in Exercise 4. For the other two, recall first that if $\rho : G \to \mathrm{GL}(V)$ is a representation, then $\rho(g)$ is diagonalizable by Lemma 2.13. Therefore there are $n = \dim(V)$ linearly independent eigenvectors with eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$, and the trace is the sum of these $\chi_V(g) = \sum_{j=1}^n \lambda_j$. Consider the representations $\rho_1 : G \to \mathrm{GL}(V_1)$, $\rho_2 : G \to \mathrm{GL}(V_2)$. For $g \in G$, take bases of eigenvectors of $\rho_1(g)$ and $\rho_2(g)$ for V_1 and V_2, respectively: if $n_1 = \dim(V_1)$ and $n_2 = \dim(V_2)$ let $v^{(1)}_\alpha$, $\alpha = 1, 2, \ldots, n_1$, be eigenvectors of $\rho_1(g)$ with eigenvalues $\lambda^{(1)}_\alpha$, and $v^{(2)}_\beta$, $\beta = 1, 2, \ldots, n_2$, eigenvectors of $\rho_2(g)$ with eigenvalues $\lambda^{(2)}_\beta$. To prove (ii) it suffices to note that $v^{(1)}_\alpha \in V_1 \subset V_1 \oplus V_2$ and $v^{(2)}_\alpha \in V_2 \subset V_1 \oplus V_2$ are the $n_1 + n_2 = \dim(V_1 \oplus V_2)$ linearly independent eigenvectors for the direct sum representation, and the eigenvalues are $\lambda^{(1)}_\alpha$ and $\lambda^{(2)}_\beta$. To prove (iii) note that the vectors $v^{(1)}_\alpha \otimes v^{(2)}_\beta$ are the $n_1 n_2 = \dim(V_1 \otimes V_2)$ linearly independent eigenvectors of $V_1 \otimes V_2$, and the eigenvalues are the products $\lambda^{(1)}_\alpha \lambda^{(2)}_\beta$, since

$$g.(v^{(1)}_\alpha \otimes v^{(2)}_\beta) = \big(\rho_1(g).v^{(1)}_\alpha\big) \otimes \big(\rho_2(g).v^{(2)}_\beta\big) = (\lambda^{(1)}_\alpha\, v^{(1)}_\alpha) \otimes (\lambda^{(2)}_\beta\, v^{(2)}_\beta) = \lambda^{(1)}_\alpha \lambda^{(2)}_\beta\, (v^{(1)}_\alpha \otimes v^{(2)}_\beta).$$

Therefore the character of the tensor product reads

$$\chi_{V_1 \otimes V_2}(g) = \sum_{\alpha,\beta} \lambda^{(1)}_\alpha\, \lambda^{(2)}_\beta = \Big(\sum_{\alpha=1}^{n_1} \lambda^{(1)}_\alpha\Big)\Big(\sum_{\beta=1}^{n_2} \lambda^{(2)}_\beta\Big) = \chi_{V_1}(g)\,\chi_{V_2}(g).$$

□

Exercise 9 (The relation between the representations $\mathrm{Hom}(V,W)$ and $W \otimes V^*$)
Let V, W be finite dimensional vector spaces, and recall from Exercise 3 that we have an isomorphism of vector spaces $W \otimes V^* \to \mathrm{Hom}(V,W)$, which is obtained by sending $w \otimes \varphi \in W \otimes V^*$ to the linear map $v \mapsto \langle \varphi, v \rangle\, w$.

Suppose now that V and W are representations of a group G. The space $W \otimes V^*$ gets a structure of a representation of G when we use the definition of a dual representation (Exercise 4) and the definition of a tensor product representation (Definition 2.21). We have also defined a representation on $\mathrm{Hom}(V,W)$ in Example 2.14. Check that the above isomorphism of vector spaces

$$W \otimes V^* \;\cong\; \mathrm{Hom}(V,W)$$

is an isomorphism of representations of G.

How to pick the trivial part of a representation?

For V a representation of G, set

$$V^G \;=\; \left\{ v \in V \;\middle|\; g.v = v \;\forall g \in G \right\}.$$

Then $V^G \subset V$ is a subrepresentation, which is a trivial representation in the sense of Example 2.10. We define a linear map φ on V by

$$\varphi(v) \;=\; \frac{1}{|G|} \sum_{g \in G} g.v \qquad v \in V.$$

Proposition 2.29
The map φ is a projection $V \to V^G$.

Proof. Clearly if $v \in V^G$ then $\varphi(v) = v$, so we have $\varphi|_{V^G} = \mathrm{id}_{V^G}$. For any $h \in G$ and $v \in V$, use the change of variables $\tilde{g} = hg$ to compute

$$h.\varphi(v) \;=\; \frac{1}{|G|} \sum_{g \in G} hg.v \;=\; \frac{1}{|G|} \sum_{\tilde{g} \in G} \tilde{g}.v \;=\; \varphi(v),$$

so we have $\mathrm{Im}\,(\varphi) \subset V^G$. □

Thus we have an explicitly defined projection to the trivial part of any representation, and we have in particular

$$\dim\left(V^G\right) \;=\; \mathrm{Tr}(\varphi) \;=\; \frac{1}{|G|} \sum_{g \in G} \chi_V(g).$$

Now suppose that V and W are two representations of G and consider the representation $\mathrm{Hom}(V,W)$. We have seen in Exercise 9 that $\mathrm{Hom}(V,W) \cong W \otimes V^*$ as a representation. In particular, we know how to compute the character

$$\chi_{\mathrm{Hom}(V,W)}(g) \;=\; \chi_{W \otimes V^*}(g) \;=\; \chi_W(g)\,\chi_{V^*}(g) \;=\; \overline{\chi_V(g)}\,\chi_W(g).$$

We've also seen that the trivial part of this representation consists of the G-module maps between V and W,

$$\mathrm{Hom}(V,W)^G \;=\; \mathrm{Hom}_G(V,W),$$

and we get the following almost innocent looking consequence

$$\dim\left(\mathrm{Hom}_G(V,W)\right) \;=\; \mathrm{Tr}(\varphi) \;=\; \frac{1}{|G|} \sum_{g \in G} \overline{\chi_V(g)}\,\chi_W(g).$$

Suppose now that V and W are irreducible. Then Schur's lemma says that when V and W are not isomorphic, there are no nonzero G-module maps $V \to W$, whereas the G-module maps from an irreducible representation to itself are scalar multiples of the identity, i.e.

$$\dim\left(\mathrm{Hom}_G(V,W)\right) = \begin{cases} 1 & \text{if } V \cong W \\ 0 & \text{otherwise} \end{cases}.$$

We have in fact obtained a very powerful result.

Theorem 2.30
The following statements hold for irreducible representations of a finite group G.

(i) If V and W are irreducible representations, then

$$\frac{1}{|G|}\sum_{g\in G}\overline{\chi_V(g)}\,\chi_W(g) = \begin{cases} 1 & \text{if } V \cong W \\ 0 & \text{otherwise} \end{cases}.$$

(ii) Characters of (non-isomorphic) irreducible representations are linearly independent.

(iii) The number of (isomorphism classes of) irreducible representations is at most the number of conjugacy classes of G.

Remark 2.31. In fact there is an equality in (iii), the number of irreducible representations of a finite group is precisely the number of its conjugacy classes. This will be proven in Exercise 13.

Proof of Theorem 2.30. The statement (i) was proved above. We can interpret it as saying that the characters of irreducible representations are orthonormal with respect to the natural inner product $(\psi,\phi) = \frac{1}{|G|}\sum_{g\in G}\overline{\psi(g)}\,\phi(g)$ on the space $\mathbb{C}^G$ of $\mathbb{C}$-valued functions on G. The linear independence, (ii), follows at once. Since a character has constant value on each conjugacy class, an obvious upper bound on the number of linearly independent characters gives (iii). □

We proceed with further consequences.

Corollary 2.32
Let W_α, $\alpha = 1,2,\ldots,k$, be the distinct irreducible representations of G. Let V be any representation, and let m_α be the multiplicity of W_α when we use complete reducibility:

$$V = \bigoplus_\alpha m_\alpha\, W_\alpha$$

Then we have

(i) The character χ_V determines V (up to isomorphism).

(ii) The multiplicities are given by

$$m_\alpha = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_{W_\alpha}(g)}\,\chi_V(g).$$

(iii) We have

$$\frac{1}{|G|}\sum_{g\in G}|\chi_V(g)|^2 = \sum_\alpha m_\alpha^2.$$

(iv) The representation V is irreducible if and only if

$$\frac{1}{|G|}\sum_{g\in G}|\chi_V(g)|^2 = 1.$$

Proof. The character of V is by Proposition 2.28 given by $\chi_V(g) = \sum_\alpha m_\alpha \chi_{W_\alpha}(g)$. Now (ii) is obtained by taking the orthogonal projection to χ_{W_α}. In particular we obtain the (anticipated) fact that in complete reducibility the direct sum decomposition is unique up to permutation of the irreducible summands. We also see (i) immediately, and (iii) follows from the same formula combined with $\overline{\chi_V(g)}\,\chi_V(g) = |\chi_V(g)|^2$. Then (iv) is obvious in view of (iii). □

We get some more nice consequences when we consider the representation given in the following examples.

Example 2.33. Consider the vector space $\mathbb{C}^G$ with basis $\{e_g \,|\, g \in G\}$. For any $g, h \in G$, set

$$h.e_g = e_{hg}$$

and extend linearly. This defines a $|G|$-dimensional representation called the regular representation of G. We denote the regular representation here by $\mathbb{C}[G]$ because later we will put an algebra structure on this vector space to obtain the group algebra of G, and then this notation is standard.

Example 2.34. More generally, following the same idea, if the group G acts on a set X, then we can define a representation on the vector space $\mathbb{C}^X$ with basis $\{e_x | x \in X\}$ by a linear extension of $g.e_x = e_{(g.x)}$. These kind of represetations are called permutation representations.

It is obvious, when we write matrices in the basis $(e_x)_{x\in X}$ and compute traces, that $\chi_{\mathbb{C}^X}(g)$ is the number of elements $x \in X$ which are fixed by the action of g. In particular the character of the regular representation is

$$\chi_{\mathbb{C}[G]}(g) = \begin{cases} |G| & \text{if } g = e \\ 0 & \text{if } g \neq e \end{cases}.$$

We can then use Corollary 2.32 (ii) and compute, for any irreducible W_α,

$$m_\alpha = \frac{1}{|G|} \sum_{g\in G} \overline{\chi_{W_\alpha}(g)}\,\chi_{\mathbb{C}[G]}(g) = \frac{1}{|G|}\,\overline{\chi_{W_\alpha}(e)}\,|G| = \dim(W_\alpha).$$

Thus any irreducible representation appears in the regular representation by multiplicity given by its dimension

$$\mathbb{C}[G] = \bigoplus_\alpha m_\alpha W_\alpha \qquad \text{where} \qquad m_\alpha = \dim(W_\alpha).$$

Considering in particular the dimensions of the two sides, and recalling $\dim(\mathbb{C}[G]) = |G|$, we get the following formula

$$\sum_\alpha \dim(W_\alpha)^2 = |G|.$$

Example 2.35. The above formula can give useful and nontrivial information. Consider for example the group S_4, whose order is $|S_4| = 4! = 24$. We have seen the trivial and alternating representations of S_4, and since there are five conjugacy classes (identity, transposition, two disjoint transpositions, three-cycle, four-cycle), we know that there are at most three other irreducible representations S_4. From the above formula we see that the sum of squares of their dimensions is $|S_4| - 1^2 - 1^2 = 22$. Since 22 is not a square, there must remain more than one irreducible, and since 22 is also not a sum of two squares, there must in fact be three other irreducibles. The only way to write 22 as a sum of three squares is $22 = 2^2 + 3^2 + 3^2$, so we see that the three remaining irreducible representations have dimensions $2, 3, 3$.

Exercise 10 (Characters of the group of symmetries of the square)
Let D_4 be the group with two generators, r and m, and relations $r^4 = e$, $m^2 = e$, $rmrm = e$. Recall that we have considered the representations of D_4 in Exercise 6.

(a) *Find a complete list of irreducible representations of* D_4*, and compute the characters of all the irreducible representations.*

(b) *Let* V *be the two-dimensional irreducible representation of* D_4 *introduced in Exercise 6. Verify using character theory that the representation* $V \otimes V$ *is isomorphic to the direct sum of four one dimensional representations (see also Exercise 7).*

Exercise 11 (The standard representation of S_4)
Consider the symmetric group S_4 *on four elements, and define a four-dimensional representation* V *with basis* e_1, e_2, e_3, e_4 *by*

$$\sigma.e_j = e_{\sigma(j)} \qquad \text{for } \sigma \in S_4,\ j = 1,2,3,4.$$

(a) *Compute the character of* V*.*

(b) *Show that the subspace spanned by* $e_1 + e_2 + e_3 + e_4$ *is a trivial subrepresentation of* V *and show that the complementary subrepresentation to it is an irreducible three-dimensional representation of* S_4*.*

(c) *Find the entire character table of* S_4*, that is, characters of all irreducible representations. (*Hint: *You should already know a couple of irredubibles. Try taking tensor products of these, and using orthonormality of irreducible characters.)*

Exercise 12 (Example of tensor products of representations of S_3)
Recall that there are three irreducible representations of S_3*, the trivial representation* U*, the alternating representation* U' *and the two-dimensional irreducible representation* V *found in Exercise 5. Consider the representation* $V^{\otimes n}$*, the* n*-fold tensor product of* V *with itself. Find the multiplicities of* U*,* U' *and* V *when* $V^{\otimes n}$ *is written as a direct sum of irreducible representations.*

Chapter 3

Algebras, coalgebras, bialgebras and Hopf algebras

Here we first define the algebraic structures to be studied in the rest of the course.

3.1 Algebras

By the standard definition, an algebra (which for us will mean an associative unital algebra) is a triple $(A, *, 1_A)$, where A is a vector space (over a field $\mathbb{K}$, usually $\mathbb{K} = \mathbb{C}$ the field of complex numbers) and $*$ is a binary operation on A

$$* : A \times A \to A \qquad (a, b) \mapsto a * b$$

called the product or multiplication, and 1_A is an element of A, the unit, such that the following hold:

"Bilinearity": the map $* : A \times A \to A$ is bilinear

"Associativity": $a_1 * (a_2 * a_3) = (a_1 * a_2) * a_3$ for all $a_1, a_2, a_3 \in A$

"Unitality": for all $a \in A$ we have $a * 1_A = a = 1_A * a$

We usually omit the notation for the binary operation $*$ and write simply $ab := a * b$. The algebra is said to be commutative if $ab = ba$ for all $a, b \in A$.

We usually abbreviate and write only A for the algebra $(A, *, 1_A)$. An algebra $(A, *, 1_A)$ is said to be finite dimensional if the $\mathbb{K}$-vector space A is finite dimensional. Note that even for commutative algebras we reserve the additive symbol + for the vector space addition in A, so the product in an algebra is never denoted additively (unlike for groups).

For an element $a \in A$, a left inverse of a is an element a' such that $a' * a = 1_A$ and a right inverse of a is an element a'' such that $a * a'' = 1_A$. An element is said to be invertible if it has both left and right inverses. In such a case the two have to be equal since

$$a'' \; = \; 1_A * a'' \; = \; (a' * a) * a'' \; = \; a' * (a * a'') \; = \; a' * 1_A \; = \; a',$$

and we denote by a^{-1} the (left and right) inverse of a. This trivial observation about equality of left and right inverses will come in handy a bit later.

Similarly, the unit 1_A is uniquely determined by the unitality property.

Example 3.1. Any field $\mathbb{K}$ is an algebra over itself (and moreover commutative).

Example 3.2. The algebra of polynomials (with coefficients in $\mathbb{K}$) in one indeterminate x is denoted by

$$\mathbb{K}[x] \;:=\; \left\{ c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n \;\middle|\; n \in \mathbb{N},\ c_0, c_1, \ldots, c_n \in \mathbb{K} \right\}.$$

The product is the usual product of polynomials (commutative).

Example 3.3. Let V be a vector space and $\mathrm{End}(V) = \mathrm{Hom}(V, V) = \{T : V \to V \text{ linear}\}$ the set of endomorphisms of V. Then $\mathrm{End}(V)$ is an algebra, with composition of functions as the binary operation, and the identity map id_V as the unit. When V is finite dimensional, $\dim(V) = n$, and a basis of V has been chosen, then $\mathrm{End}(V)$ can be identified with the algebra of $n \times n$ matrices, with matrix product as the binary operation.

Example 3.4. For G a group, let $\mathbb{K}[G]$ be the vector space with basis $(e_g)_{g \in G}$ over the ground field $\mathbb{K}$ (usually we take $\mathbb{K} = \mathbb{C}$, the field of complex numbers) and define the product by bilinearly extending

$$e_g * e_h \;=\; e_{gh}.$$

Then, $\mathbb{K}[G]$ is an algebra called the group algebra of G, the unit is e_e, where $e \in G$ is the neutral element of the group.

Definition 3.5. Let $(A_1, *_1, 1_{A_1})$ and $(A_2, *_2, 1_{A_2})$ be algebras. A mapping $f : A_1 \to A_2$ is said to be a homomorphism of (unital) algebras if f is linear and $f(1_{A_1}) = 1_{A_2}$ and for all $a, b \in A_1$

$$f(a *_1 b) \;=\; f(a) *_2 f(b).$$

Definition 3.6. For A an algebra, a vector subspace $A' \subset A$ is called a subalgebra if $1_A \in A'$ and for all $a', b' \in A'$ we have $a'b' \in A'$. A vector subspace $J \subset A$ is called a left ideal (resp. right ideal, resp. two-sided ideal or simply ideal) if for all $a \in A$ and $k \in J$ we have $ak \in J$ (resp. $ka \in J$, resp. both).

For J an ideal, the quotient vector space A/J becomes an algebra by setting

$$(a + J)(b + J) \;=\; ab + J,$$

which is well defined since the three last terms in $(a + k)(b + k') = ab + ak' + kb + kk'$, and are in the ideal if k and k' are. The unit of A/J is the equivalence class of the unit of A, that is $1_A + J$.

The isomorphism theorem for algebras now states the following.

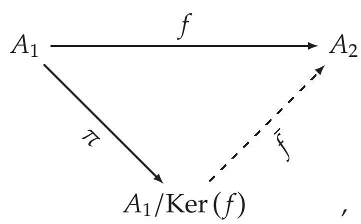
Theorem 3.7
Let A_1 and A_2 be algebras and $f : A_1 \to A_2$ a homomorphism. Then

1°) $\mathrm{Im}(f) := f(A_1) \subset A_2$ *is a subalgebra.*

2°) $\mathrm{Ker}(f) := f^{-1}(\{0\}) \subset A_1$ *is an ideal.*

3°) The quotient algebra $A_1/\mathrm{Ker}(f)$ *is isomorphic to* $\mathrm{Im}(f)$.

More precisely, there exists an injective algebra homomorphism $\bar{f} : A_1/\mathrm{Ker}(f) \to A_2$ *such that the following diagram commutes*



,

where $\pi : A_1 \to A_1/\mathrm{Ker}(f)$ *is the canonical projection to the quotient,* $\pi(a) = a + \mathrm{Ker}(f)$.

Proof. The assertions (1°) and (2°) are easy. For (3°), take $\bar{f}$ to be the injective linear map that one gets from the isomorphism theorem of vector spaces applied to the present case. Notice that this $\bar{f}$ is an algebra homomorphism since

$$\bar{f}\Big((a + \mathrm{Ker}\, f)(b + \mathrm{Ker}\, f)\Big) = \bar{f}(ab + \mathrm{Ker}\, f) = f(ab) = f(a)\, f(b) = \bar{f}(a + \mathrm{Ker}\, f)\ \bar{f}(b + \mathrm{Ker}\, f)$$

and

$$\bar{f}\,(1_{A_1} + \mathrm{Ker}\,(f)) = f(1_{A_1}) = 1_{A_2}.$$

□

We also recall the following definition.

Definition 3.8. The center of an algebra A is the set $Z \subset A$ of elements that commute with the whole algebra, i.e.

$$Z = \Big\{ z \in A \,\Big|\, za = az \;\; \forall a \in A \Big\}.$$

3.2 Representations of algebras

The definition of a representation is analogous to the one for groups:

Definition 3.9. For A an algebra and V a vector space, a representation of A in V is an algebra homomorphism $\rho : A \to \mathrm{End}(V)$.

In such a case we often call V an A-module (more precisely, a left A-module) and write $a.v = \rho(a)v$ for $a \in A$, $v \in V$.

Definition 3.10. Let A be an algebra and $\rho_V : A \to \mathrm{End}(V)$, $\rho_W : A \to \mathrm{End}(W)$ two representations of A. A linear map $T : V \to W$ is called and A-module map (or sometimes A-linear or A-homomorphism) if for all $a \in A$, $v \in V$

$$\rho_W(a)\Big(T(v)\Big) = T\Big(\rho_V(a)(v)\Big).$$

In the module notation the condition for a map to be an A-module map reads

$$a.T(v) = T(a.v) \qquad \text{for all } a \in A,\ v \in V.$$

Given an algebra $A = (A, *, 1_A)$, the opposite algebra A^{op} is the algebra $A^{\mathrm{op}} = (A, *^{\mathrm{op}}, 1_A)$ with the product operation reversed

$$a *^{\mathrm{op}} b = b * a \qquad \text{for all } a, b \in A.$$

Representations of the opposite algebra correspond to right A-modules, that is, vector spaces V with a right multiplication by elements of A which satisfy $v.1_A = v$ and $(v.a).b = v.(ab)$ for all $v \in V$, $a, b \in A$.

Subrepresentations (submodules), irreducible representations (simple modules), quotient representations (quotient modules) and direct sums of representations (direct sums of modules) are defined in the same way as before. For representations of algebras in complex vector spaces, Schur's lemma continues to hold and the proof is the same as before.

The most obvious example of a representation of an algebra is the algebra itself:

Example 3.11. The algebra A is a left A-module by $a.b = ab$ (for all a in the algebra A and b in the module A), and a right A-module by the same formula (then we should read that a is in the module A and b in the algebra A).

Also the dual of an algebra is easily equipped with a representation structure.

Example 3.12. The dual A^* becomes a left A-module if we define $a.f \in A^*$ by

$$\langle a.f, x \rangle = \langle f, xa \rangle$$

for $f \in A^*$, $a, x \in A$. Indeed, the property $1_A.f = f$ is evident and we check

$$\langle a.(b.f), x \rangle = \langle b.f, xa \rangle = \langle f, (xa)b \rangle = \langle f, x(ab) \rangle = \langle (ab).f, x \rangle.$$

Similarly, the dual becomes a right A-module by the definition

$$\langle f.a, x \rangle = \langle f, ax \rangle$$

Example 3.13. Representations of a group G correspond in a rather obvious way to representations of the group algebra $\mathbb{C}[G]$. Indeed, given a representation of the group, $\rho_G : G \to \mathrm{GL}(V)$, there is a unique linear extension of it from the values on the basis vectors, $e_g \mapsto \rho_G(g) \in \mathrm{GL}(V) \subset \mathrm{End}(V)$, which defines a representation of the group algebra. The other way around, given an algebra representation $\rho_A : \mathbb{C}[G] \to \mathrm{End}(V)$, we observe that $\rho_A(e_g)$ is an invertible linear map with inverse $\rho_A(e_{g^{-1}})$, so we set $g \mapsto \rho_A(e_g)$ to define a representation of the group. Both ways the homomorphism property of the constructed map obviously follows from the homomorphism property of the original map.

Exercise 13 (The center of the group algebra)
Let G be a finite group and $A = \mathbb{C}[G]$ its group algebra, i.e. the complex vector space with basis $(e_g)_{g \in G}$ equipped with the product $e_g\, e_h = e_{gh}$ (extended bilinearly).

(a) Show that the element

$$a = \sum_{g \in G} \alpha(g)\, e_g \in A$$

is in the center of the group algebra if and only if $\alpha(g) = \alpha(hgh^{-1})$ for all $g, h \in G$.

(b) Suppose that $\alpha : G \to \mathbb{C}$ is a function which is constant on each conjugacy class, and suppose furthermore that α is orthogonal (with respect to the inner product $(\psi, \phi) = |G|^{-1} \sum_{g \in G} \overline{\psi(g)} \phi(g)$) to the characters of all irreducible representations of G. Show that for any representation $\rho : G \to \mathrm{GL}(V)$ the map $\sum_g \alpha(g)\rho(g) : V \to V$ is the zero map. Conclude that α has to be zero.

(c) Using (b) and the earlier results about irreducible representations of finite groups, show that the number of irreducible representations of the group G is equal to the number of conjugacy classes of G

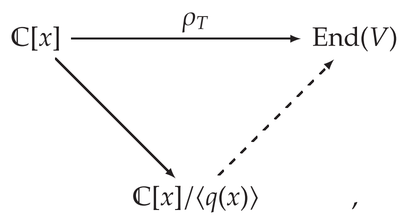
Recall that in Theorem 2.30 we had showed that the number of irreducible representations of a finite group is at most the number of conjugacy classes of the group — this exercise shows that the numbers are in fact equal.

Example 3.14. Let V be a vector space over $\mathbb{K}$ and $T \in \mathrm{End}(V)$ a linear map of V into itself. Since the polynomial algebra $\mathbb{K}[x]$ is the free (commutative) algebra with one generator x, there exists a unique algebra morphism $\rho_T : \mathbb{K}[x] \to \mathrm{End}(V)$ such that $x \mapsto T$, namely

$$\rho_T\Big(c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n\Big) = c_0 + c_1 T + c_2 T^2 + \cdots + c_n T^n.$$

Thus any endomorphism T of a vector space defines a representation ρ_T of the algebra $\mathbb{K}[x]$. Likewise, any $n \times n$ matrix with entries in $\mathbb{K}$, interpreted as an endomorphism of $\mathbb{K}^n$, defines a representation of the polynomial algebra.

Example 3.15. Let V be a complex vector space, and $T \in \mathrm{End}(V)$ as above and let $q(x) \in \mathbb{C}[x]$ be a polynomial. Consider the algebra $\mathbb{C}[x]/\langle q(x)\rangle$, where $\langle q(x)\rangle$ is the ideal generated by $q(x)$. The above representation map $\rho_T : \mathbb{C}[x] \to \mathrm{End}(V)$ factors through the quotient algebra $\mathbb{C}[x]/\langle q(x)\rangle$



,

if and only if the ideal $\langle q(x)\rangle$ is contained in the ideal Ker ρ_T. The ideal Ker ρ_T is generated by the minimal polynomial of T (recall that the polynomial algebra is a principal ideal domain: any ideal is generated by one element, a lowest degree nonzero polynomial contained in the ideal). Thus the above factorization through quotient is possible if and only if the minimal polynomial of T divides $q(x)$. We conclude that the representations of the algebra $\mathbb{C}[x]/\langle q(x)\rangle$ correspond to endomorphisms whose minimal polynomial divides $q(x)$ — or equivalently, to endomorphisms T such that $q(T) = 0$.

The Jordan decomposition of complex matrices gives a direct sum decomposition of this representation with summands corresponding to the invariant subspaces of each Jordan block. The direct summands are indecomposable (not themself expressible as direct sum of two proper subreprentations) but those corresponding to blocks of size more than one are not irreducible (they contain proper subrepresentations, for example the one dimensional eigenspace within the block). We see that whenever $q(x)$ has roots of multiplicity greater than one, there are representations of the algebra $\mathbb{C}[x]/\langle q(x)\rangle$ which are not completely reducible.

On semisimplicity

Definition 3.16. Let A be an algebra. An A-module W is called simple (or irreducible) if the only submodules of W are $\{0\}$ and W. An A-module V is called completely reducible if V is isomorphic to a direct sum of finitely many simple A-modules. An algebra A is called semisimple if all finite dimensional A-modules are completely reducible.

The terms "simple module" and "irreducible representation" seem standard, but we will also speak of irreducible modules with the same meaning.

Definition 3.17. An A-module V is called indecomposable if it can not be written as a direct sum of two nonzero submodules.

In particular any irreducible module is indecomposable. And for semisimple algebras the two concepts are the same.

The following classical result gives equivalent conditions for semisimplicity, which are often practical.

Proposition 3.18
Let A be an algebra. The following conditions are equivalent.

(i) A is semisimple, i.e. any finite dimensional A-module is isomorphic to a finite direct sum of irreducible A-modules.

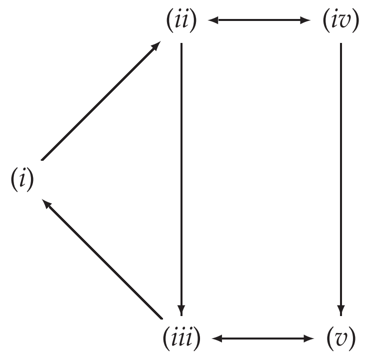
(ii) For any finite dimensional A-module V and any submodule $W \subset V$ there exists a submodule $W' \subset V$ (complementary submodule) such that $V = W \oplus W'$ as an A-module.

(iii) For any finite dimensional A-module V and any irreducible submodule $W \subset V$ there exists a submodule $W' \subset V$ such that $V = W \oplus W'$ as an A-module.

(iv) For any finite dimensional A-module V and any submodule $W \subset V$ there exists an A-module map $\pi : V \to W$ such that $\pi|_W = \mathrm{id}_W$ (an A-linear projection to the submodule).

(v) For any finite dimensional A-module V and any irreducible submodule $W \subset V$ there exists an A-module map $\pi : V \to W$ such that $\pi|_W = \mathrm{id}_W$.

Proof. We will do the proofs of the following implications:



Clearly *(ii)* $\Rightarrow$ *(iii)* and *(iv)* $\Rightarrow$ *(v)*.

Let us show that *(ii)* and *(iv)* are equivalent, in the same way one shows that *(iii)* and *(v)* are equivalent. Assume *(ii)*, that any submodule $W \subset V$ has a complementary submodule W', that is $V = W \oplus W'$. Then if π is the projection to W with respect to this direct sum decomposition, we have that for all $w \in W$, $w' \in W'$, $a \in A$

$$\pi\left(a \cdot (w + w')\right) \;=\; \pi(a \cdot w + a \cdot w') \;=\; a \cdot w \;=\; a \cdot \pi(w + w'),$$

which shows that the projection is A-linear. Conversely, assume *(iv)* that for any submodule $W \subset V$ there is an A-linear projection $\pi : V \to W$. The subspace $W' = \mathrm{Ker}\,(\pi)$ is a submodule complementary to $W = \mathrm{Ker}\,(1 - \pi)$.

We must still show that *(iii)* $\Rightarrow$ *(i)* and *(i)* $\Rightarrow$ *(ii)*.

Assume *(iii)* and let V be a finite dimensional A-module (we may assume immediately that $V \neq \{0\}$). Consider a non-zero submodule $W_1 \subset V$ of smallest dimension, it is necessarily irreducible. If $W_1 = V$ we're done, if not by property *(iii)* we have a complementary submodule $V_1 \subset V$ with $\dim V_1 < \dim V$ and $V = W_1 \oplus V_1$. Continue recursively to find the non-zero irreducible submodules $W_n \subset V_{n-1}$ and their complementaries V_n in V_{n-1}, that is $V_{n-1} = W_n \oplus V_n$. The dimensions of the latter are strictly decreasing,

$$\dim V > \dim V_1 > \dim V_2 > \cdots,$$

so for some $n_0 \in \mathbb{N}$ we have $W_n = V_{n-1}$ and

$$V = W_1 \oplus W_2 \oplus \cdots \oplus W_{n_0},$$

proving *(i)*.

Let us finally prove that *(i)* implies *(ii)*. Suppose $V = \bigoplus_{i \in I} W_i$, where I is a finite index set and for all $i \in I$ the submodule W_i is irreducible. Suppose $W \subset V$ is a submodule, and choose a subset $J \subset I$ such that

$$W \cap \left(\bigoplus_{j \in J} W_j \right) \;=\; \{0\}\,, \tag{3.1}$$

but that for all $i \in I \setminus J$

$$W \cap \left(W_i \oplus \bigoplus_{j \in J} W_j \right) \neq \{0\} . \tag{3.2}$$

Denote by $W' = \bigoplus_{j \in J} W_j$ the submodule thus obtained. By Equation (3.1) the sum of W and W' is direct, and we will prove that it is the entire module V. For that, note that by Equation (3.2) for all $i \in I \setminus J$ there exists $w \in W \setminus \{0\}$ such that $w = w_i + w'$ with $w_i \in W_i \setminus \{0\}$, $w' \in W'$. Therefore the submodule $W \oplus W'$ contains the nonzero vector $w_i \in W_i$, and by irreducibility we get $W_i \subset W \oplus W'$. We get this inclusion for all $i \in I \setminus J$, and also evidently $W_j \subset W \oplus W'$ for all $j \in J$, so we conclude

$$V = \bigoplus_{i \in I} W_i \subset W \oplus W',$$

which finishes the proof. □

3.3 Another definition of algebra

In our definitions of algebras, coalgebras and Hopf algebras we will from here on take the ground field to be the field $\mathbb{C}$ of complex numbers, although much of the theory could be developed for other fields, too.

The following "tensor flip" will be used occasionally. For V and W vector spaces, let us denote by $S_{V,W}$ the linear map that switches the components

$$S_{V,W} : V \otimes W \to W \otimes V \qquad \text{such that} \qquad S_{V,W}(v \otimes w) = w \otimes v \qquad \forall\, v \in V, w \in W. \tag{3.3}$$

By the bilinearity axiom for algebras, the product could be factorized through $A \otimes A$, namely there exists a linear map $\mu : A \otimes A \to A$ such that

$$\mu(a \otimes b) = a\,b \qquad \forall\, a, b \in A.$$

We can also encode the unit in a linear map

$$\eta : \mathbb{C} \to A \qquad \lambda \mapsto \lambda\, 1_A.$$

The axioms of associativity and unitality then read

$$\mu \circ (\mu \otimes \mathrm{id}_A) = \mu \circ (\mathrm{id}_A \otimes \mu) \tag{H1}$$
$$\mu \circ (\eta \otimes \mathrm{id}_A) = \mathrm{id}_A = \mu \circ (\mathrm{id}_A \otimes \eta), \tag{H2}$$

where (H1) expresses the equality of two maps $A \otimes A \otimes A \to A$, when we make the usual identifications

$$(A \otimes A) \otimes A \cong A \otimes A \otimes A \cong A \otimes (A \otimes A)$$

and (H2) expresses the equality of three maps $A \to A$, when we make the usual identifications

$$\mathbb{C} \otimes A \cong A \cong A \otimes \mathbb{C}.$$

We take this as our definition (it is equivalent to the standard definition).

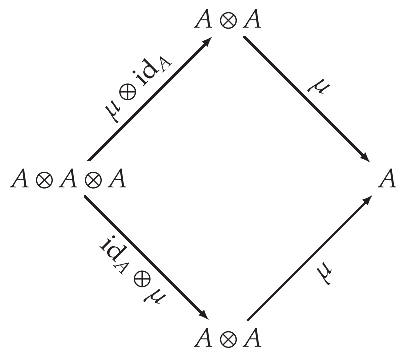
Definition 3.19. An (associative unital) algebra is a triple (A, μ, η), where A is a vector space and

$$\mu : A \otimes A \to A \qquad \eta : \mathbb{C} \to A$$

are linear maps, such that "associativity" (H1) and "unitality" (H2) hold.

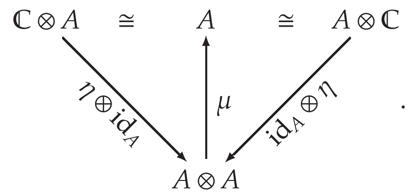
Example 3.20. If (A, μ, η) is an algebra, then setting $\mu^{op} = \mu \circ S_{A,A}$, i.e. $\mu^{op}(a \otimes b) = b\,a$, one obtains the opposite algebra $A^{op} = (A, \mu^{op}, \eta)$. An algebra is called commutative if $\mu^{op} = \mu$.

The axiom of associativity can also be summarized by the following commutative diagram



(H1)

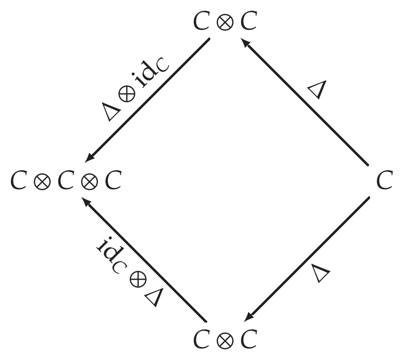
and unitality by



(H2)

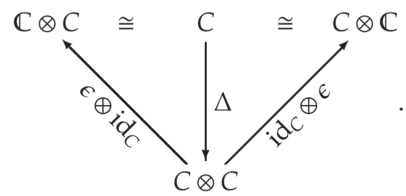
3.4 Coalgebras

A coalgebra is defined by reversing the directions of all arrows in the commutative diagrams defining algebras. Namely, we impose an axiom of "coassociativity"



(H1′)

and "counitality"



(H2′)

Definition 3.21. A coalgebra is a triple (C, Δ, ϵ), where C is a vector space and

$$\Delta : C \to C \otimes C \qquad \epsilon : C \to \mathbb{C}$$

are linear maps such that "coassociativity" (H1′) and "counitality" (H2′) hold. The maps Δ and ϵ are called coproduct and counit, respectively.

The axioms for coalgebras can also be written as

$$(\Delta \otimes \mathrm{id}_C) \circ \Delta \;=\; (\mathrm{id}_C \otimes \Delta) \circ \Delta \tag{H1'}$$
$$(\epsilon \otimes \mathrm{id}_C) \circ \Delta \;=\; \mathrm{id}_C \;=\; (\mathrm{id}_C \otimes \epsilon) \circ \Delta. \tag{H2'}$$

Example 3.22. If (C, Δ, ϵ) is a coalgebra, then with the opposite coproduct $\Delta^{\mathrm{cop}} = S_{C,C} \circ \Delta$ one obtains the (co-)opposite coalgebra $C^{\mathrm{cop}} = (C, \Delta^{\mathrm{cop}}, \epsilon)$. A coalgebra is called cocommutative if $\Delta^{\mathrm{cop}} = \Delta$.

Exercise 14 (A coalgebra from trigonometric addition formulas)
Let C be a vector space with basis $\{c, s\}$. Define $\Delta : C \to C \otimes C$ by linear extension of

$$c \;\mapsto\; c \otimes c - s \otimes s \quad , \qquad s \;\mapsto\; c \otimes s + s \otimes c.$$

Does there exist $\epsilon : C \to \mathbb{C}$ such that (C, Δ, ϵ) becomes a coalgebra?

Sweedler's sigma notation

For practical computations with coalgebras it's important to have manageable notational conventions. We will follow what is known as the Sweedler's sigma notation. By usual properties of the tensor product, we can for any $a \in C$ write the coproduct of a as a linear combination of simple tensors

$$\Delta(a) \;=\; \sum_{j=1}^{n} a'_j \otimes a''_j.$$

In such expressions the choice of simple tensors, or the choice of $a'_j, a''_j \in C$, or even the number n of terms, are of course not unique! It is nevertheless convenient to keep this property in mind and use the notation

$$\Delta(a) \;=\; \sum_{(a)} a_{(1)} \otimes a_{(2)}$$

to represent any of the possible expressions for $\Delta(a) \in C \otimes C$. Likewise, when $a \in C$, and we write some expression involving a sum $\sum_{(a)}$ and bilinear dependency on the pair $(a_{(1)}, a_{(2)})$, it is to be interpreted so that any linear combination of simple tensors that gives the coproduct of a could be used. For example, if $g : C \to V$ and $h : C \to W$ are linear maps, then

$$\sum_{(a)} g(a_{(1)}) \otimes h(a_{(2)}) \qquad \text{represents} \qquad (g \otimes h)(\Delta(a)) \in V \otimes W.$$

The opposite coproduct of Example 3.22 is written in this notation as

$$\Delta^{\mathrm{cop}}(a) \;=\; S_{C,C}(\Delta(a)) \;=\; \sum_{(a)} a_{(2)} \otimes a_{(1)}.$$

Another example is the counitality axiom, which reads

$$\sum_{(a)} \epsilon(a_{(1)})\, a_{(2)} \;=\; a \;=\; \sum_{(a)} \epsilon(a_{(2)})\, a_{(1)}. \tag{H2'}$$

The coassociativity axiom states that

$$\sum_{(a)} \sum_{(a_{(1)})} (a_{(1)})_{(1)} \otimes (a_{(1)})_{(2)} \otimes a_{(2)} \;=\; \sum_{(a)} \sum_{(a_{(2)})} a_{(1)} \otimes (a_{(2)})_{(1)} \otimes (a_{(2)})_{(2)}. \tag{H1'}$$

By a slight abuse of notation we write the above quantity as $\sum_{(a)} a_{(1)} \otimes a_{(2)} \otimes a_{(3)}$, and more generally we write the $n-1$-fold coproduct as

$$(\Delta \otimes \mathrm{id}_C \otimes \cdots \otimes \mathrm{id}_C) \circ \;\ldots\; \circ (\Delta \otimes \mathrm{id}_C) \circ \Delta(a) \;=\; \sum_{(a)} a_{(1)} \otimes a_{(2)} \otimes \cdots \otimes a_{(n)} \;=\; \Delta^{(n)}(a).$$

So when reading an expression involving the Sweedler's notation $\sum_{(a)}$, one should always check what is the largest subscript index of the $a_{(j)}$ in order to know how many coproducts are successively applied to a. By coassociativity, however, it doesn't matter to which components we apply the coproducts.

Subcoalgebras, coideals, quotient coalgebras and isomorphism theorem

As for other algebraic structures, maps that preserve the structure are called homomorphisms, and one can define substructures and quotient structures, and one has an isomorphism theorem.

Definition 3.23. Let $(C_j, \Delta_j, \epsilon_j)$, $j = 1, 2$, be two coalgebras. A homomorphism of coalgebras is linear map $f : C_1 \to C_2$ which preserves the coproduct and counit in the following sense

$$\Delta_2 \circ f = (f \otimes f) \circ \Delta_1 \qquad \text{and} \qquad \epsilon_2 \circ f = \epsilon_1 .$$

Definition 3.24. For $C = (C, \Delta, \epsilon)$ a coalgebra, a vector subspace $C' \subset C$ is called a subcoalgebra if

$$\Delta(C') \subset C' \otimes C'.$$

A vector subspace $J \subset C$ is called a coideal if

$$\Delta(J) \subset J \otimes C + C \otimes J \qquad \text{and} \qquad \epsilon\big|_J = 0.$$

For $J \subset C$ a coideal, the quotient vector space C/J becomes a coalgebra by the coproduct and counit

$$\Delta_{C/J}(a + J) = \sum_{(a)} (a_{(1)} + J) \otimes (a_{(2)} + J) \qquad \text{and} \qquad \epsilon_{C/J}(a + J) = \epsilon(a),$$

whose well-definedness is again due to the coideal properties of J.

The isomorphism theorem for coalgebras is the following (unsurprising) statement.

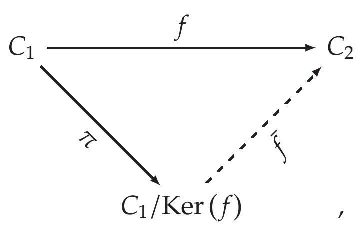
Theorem 3.25
Let $C_1 = (C_1, \Delta_1, \epsilon_1)$ and $C_2 = (C_2, \Delta_2, \epsilon_2)$ be coalgebras and $f : C_1 \to C_2$ a homomorphism of coalgebras. Then

1°) $\mathrm{Im}\,(f) := f(C_1) \subset C_2$ *is a subcoalgebra.*

2°) $\mathrm{Ker}\,(f) := f^{-1}(\{0\}) \subset C_1$ *is a coideal.*

3°) The quotient coalgebra $C_1/\mathrm{Ker}\,(f)$ *is isomorphic to* $\mathrm{Im}\,(f)$.

More precisely, there exists an injective homomorphism of coalgebras $\bar{f} : C_1/\mathrm{Ker}\,(f) \to C_2$ such that the following diagram commutes



,

where $\pi : C_1 \to C_1/\mathrm{Ker}\,(f)$ is the canonical projection to the quotient, $\pi(a) = a + \mathrm{Ker}\,(f)$.

Proof. To prove (1°), suppose $b \in \mathrm{Im}(f)$, that is $b = f(a)$ for some $a \in C_1$, and use the homomorphism property of f to get

$$\Delta_2(b) \;=\; \Delta_2(f(a)) \;=\; (f \otimes f)(\Delta_1(a)) \;=\; \sum_{(a)} f(a_{(1)}) \otimes f(a_{(2)}) \;\subset \mathrm{Im}(f) \otimes \mathrm{Im}(f)\,.$$

To prove (2°), suppose $a \in \mathrm{Ker}(f)$, that is $f(a) = 0$. Then

$$\epsilon_1(a) \;=\; \epsilon_2(f(a)) \;=\; \epsilon_2(0) \;=\; 0$$

so the condition $\epsilon_1\big|_{\mathrm{Ker}(f)} = 0$ is satisfied. Also we have

$$0 \;=\; \Delta_2(0) \;=\; \Delta_2(f(a)) \;=\; (f \otimes f)(\Delta_1(a)) \;=\; \sum_{(a)} f(a_{(1)}) \otimes f(a_{(2)}),$$

from which it is easy to see, for example by taking a basis for $\mathrm{Ker}(f)$ and completing it to a basis of C_1, that $\Delta_1(a) = \sum_{(a)} a_{(1)} \otimes a_{(2)} \subset \mathrm{Ker}(f) \otimes C_1 + C_1 \otimes \mathrm{Ker}(f)$. For the proof of (3°), one takes the injective linear map $\bar{f}$ provided by the isomorphism theorem of vector spaces, and checks that this $\bar{f}$ is a homomorphism of coalgebras. Indeed, using the fact that f is a homomorphism of coalgebras we get

$$\epsilon_2\Big(\bar{f}(c + \mathrm{Ker}\, f)\Big) \;=\; \epsilon_2(f(c)) \;=\; \epsilon_1(c)$$

and

$$\begin{aligned} \Delta_2\Big(\bar{f}(c + \mathrm{Ker}\, f)\Big) &= \Delta_2(f(c)) \;=\; (f \otimes f)(\Delta_1(c)) \;=\; \sum_{(c)} f(c_{(1)}) \otimes f(c_{(2)}) \\ &= \sum_{(c)} \bar{f}(c_{(1)} + \mathrm{Ker}\, f) \otimes \bar{f}(c_{(2)} + \mathrm{Ker}\, f) \end{aligned}$$

for any $c \in C_1$. □

3.5 Bialgebras and Hopf algebras

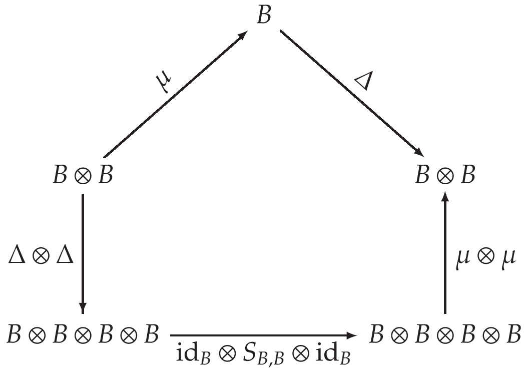
Definition 3.26. A bialgebra is a quintuple $(B, \mu, \Delta, \eta, \epsilon)$ where B is a vector space and

$$\mu : B \otimes B \to B \qquad \Delta : B \to B \otimes B$$
$$\eta : \mathbb{C} \to B \qquad \epsilon : B \to \mathbb{C}$$

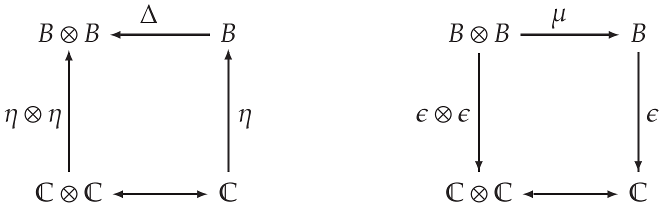
are linear maps so that (B, μ, η) is an algebra, (B, Δ, ϵ) is a coalgebra and the following further axioms hold

$$\Delta \circ \mu \;=\; (\mu \otimes \mu) \circ (\mathrm{id}_B \otimes S_{B,B} \otimes \mathrm{id}_B) \circ (\Delta \otimes \Delta) \tag{H4}$$
$$\Delta \circ \eta \;=\; \eta \otimes \eta \tag{H5}$$
$$\epsilon \circ \mu \;=\; \epsilon \otimes \epsilon \tag{H5'}$$
$$\epsilon \circ \eta \;=\; \mathrm{id}_{\mathbb{C}}. \tag{H6}$$

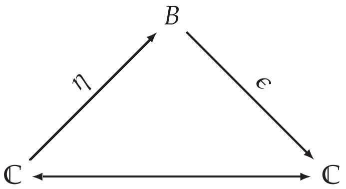
The following commutative diagrams visualize the new axioms:



(H4)



(H5 and H5′)



(H6)

In the following exercise it is checked that the axioms (H4), (H5), (H5′), (H6) state alternatively that Δ and ϵ are homomorphisms of algebras, or that μ and η are homomorphisms of coalgebras. We will soon also motivate this definition with properties of representations.

Exercise 15 (Alternative definitions of bialgebra)
Let B be a vector space and suppose that

$$\mu : B \otimes B \to B \qquad \eta : \mathbb{C} \to B$$
$$\Delta : B \to B \otimes B \qquad \epsilon : B \to \mathbb{C}$$

are linear maps such that (B, μ, η) is an algebra and (B, Δ, ϵ) is a coalgebra.
Show that the following conditions are equivalent:

(i) Both Δ and ϵ are homomorphisms of algebras.

(ii) Both μ and η are homomorphisms of coalgebras.

(iii) $(B, \mu, \Delta, \eta, \epsilon)$ is a bialgebra.

Above we of course needed algebra and coalgebra structures on $\mathbb{C}$ and on $B \otimes B$. The algebra structure on $\mathbb{C}$ is using the product of complex numbers. The coalgebra structure on $\mathbb{C}$ is such that the coproduct and counit are both identity maps of $\mathbb{C}$, when we identify $\mathbb{C} \otimes \mathbb{C} \cong \mathbb{C}$ (for the coproduct) and note that $\mathbb{C}$ itself is the ground field (for the counit). The algebra structure on $B \otimes B$ is the tensor product of two copies of the algebra B, i.e. with the product determined by $(b' \otimes b'')(b''' \otimes b'''') = b'b''' \otimes b''b''''$. The coalgebra structure in $B \otimes B$ is the tensor product of two copies of the coalgebra B, i.e. when $\Delta(b') = \sum b'_{(1)} \otimes b'_{(2)}$ and $\Delta(b'') = \sum b''_{(1)} \otimes b''_{(2)}$ then the coproduct of $b' \otimes b''$ is $\sum \left(b'_{(1)} \otimes b''_{(1)}\right) \otimes \left(b'_{(2)} \otimes b''_{(2)}\right)$ and counit is simply $b' \otimes b'' \mapsto \epsilon(b')\,\epsilon(b'')$.

Hopf algebras have one more structural map and one more axiom:

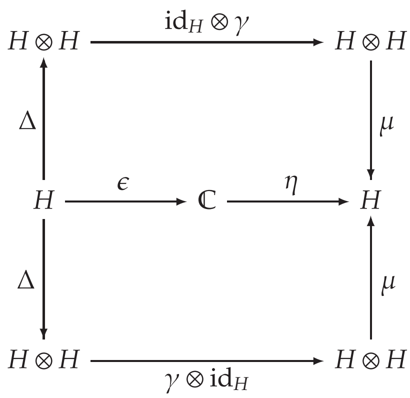
Definition 3.27. A Hopf algebra is a sextuple $(H, \mu, \Delta, \eta, \epsilon, \gamma)$, where H is a vector space and

$$\begin{aligned} \mu &: H \otimes H \to H & \Delta &: H \to H \otimes H \\ \eta &: \mathbb{C} \to H & \epsilon &: H \to \mathbb{C} \\ \gamma &: H \to H \end{aligned}$$

are linear maps such that $(H, \mu, \Delta, \eta, \epsilon)$ is a bialgebra and the following further axiom holds

$$\mu \circ (\gamma \otimes \mathrm{id}_H) \circ \Delta \; = \; \eta \circ \epsilon \; = \; \mu \circ (\mathrm{id}_H \otimes \gamma) \circ \Delta. \tag{H3}$$

The map $\gamma : H \to H$ is called antipode. The corresponding commutative diagram is



(H3)

In the Sweedler's sigma notation the axiom concerning the antipode reads

$$\sum_{(a)} \gamma(a_{(1)})\, a_{(2)} \; = \; \epsilon(a)\, 1_H \; = \; \sum_{(a)} a_{(1)}\, \gamma(a_{(2)}) \qquad \forall\, a \in H, \tag{H3}$$

where $1_H = \eta(1)$ is the unit of the algebra (H, μ, η) and we use the usual notation for products in the algebra, $a\, b := \mu(a \otimes b)$.

To construct antipodes for bialgebras, the following lemma occasionally comes in handy.

Exercise 16 (A lemma for construction of antipode)
Let $B = (B, \mu, \Delta, \eta, \epsilon)$ be a bialgebra. Suppose that as an algebra B is generated by a collection of elements $(g_i)_{i \in I}$. Suppose furthermore that we are given a linear map $\gamma : B \to B$, which is a homomorphism of algebras from $B = (B, \mu, \eta)$ to $B^{\mathrm{op}} = (B, \mu^{\mathrm{op}}, \eta)$, and which satisfies

$$\Big(\mu \circ (\gamma \otimes \mathrm{id}_B) \circ \Delta\Big)(g_i) \; = \; \epsilon(g_i)\, 1_B \; = \; \Big(\mu \circ (\mathrm{id}_B \otimes \gamma) \circ \Delta\Big)(g_i) \qquad \text{for all } i \in I.$$

Show that $(B, \mu, \Delta, \eta, \epsilon, \gamma)$ is a Hopf algebra.

We will later see that the antipode is always a homomorphism of algebras to the opposite algebra, so the conditions for γ in the exercise are also necessary.

With the help of Exercises 15 and 16 one easily constructs examples of Hopf algebras, such as the following two.

Example 3.28. The group algebra $\mathbb{C}[G]$ of a group G becomes a Hopf algebra with the definitions

$$\Delta(e_g) \; = \; e_g \otimes e_g\,, \qquad \epsilon(e_g) \; = \; 1\,, \qquad \gamma(e_g) \; = \; e_{g^{-1}} \qquad \text{(extended linearly).}$$

We call this Hopf algebra the Hopf algebra of the group G, and continue to use the notation $\mathbb{C}[G]$ for it.

Example 3.29. The algebra of polynomials $\mathbb{C}[x]$ becomes a Hopf algebra with the definitions

$$\Delta(x^n) = \sum_{k=0}^{n} \binom{n}{k} x^k \otimes x^{n-k} , \qquad \epsilon(x^n) = \delta_{n,0} , \qquad \gamma(x^n) = (-1)^n \, x^n \qquad \text{(extended linearly)},$$

where

$$\binom{n}{k} = \frac{n!}{k! \, (n-k)!}$$

are the binomial coefficients, and we've used the Kronecker delta symbol

$$\delta_{n,m} = \begin{cases} 1 & \text{if } n = m \\ 0 & \text{if } n \neq m \end{cases} .$$

We call this Hopf algebra the binomial Hopf algebra.

Motivated by the above examples, we give names to some elements whose coproduct resembles one of the two examples.

Definition 3.30. Let (C, Δ, ϵ) be a coalgebra. A non-zero element $a \in C$ is said to be grouplike if $\Delta(a) = a \otimes a$. Let $(B, \mu, \Delta, \eta, \epsilon)$ be a bialgebra. A non-zero element $x \in B$ is said to be primitive if $\Delta(x) = x \otimes 1_B + 1_B \otimes x$.

All the basis vectors e_g, $g \in G$, in the Hopf algebra $\mathbb{C}[G]$ of a group G are grouplike. In fact, they are the only grouplike elements of $\mathbb{C}[G]$, as follows from the exercise below.

Exercise 17 (Linear independence of grouplike elements)
Show that the grouplike elements in a coalgebra are linearly independent.

Here is one obvious example more.

Example 3.31. If $(B, \mu, \eta, \Delta, \epsilon)$ is a bialgebra, then the unit $1_B = \eta(1) \in B$ is grouplike by the property (H5).

Any scalar multiple of the indeterminate x in the binomial Hopf algebra $\mathbb{C}[x]$ is primitive. In fact, it is easy to see that the primitive elements of a bialgebra form a vector subspace. A typical example comes from a natural Hopf algebra structure for the universal enveloping algebra $\mathcal{U}(\mathfrak{g})$ of a Lie algebra $\mathfrak{g}$, where the subspace of primitive elements is precisely $\mathfrak{g} \subset \mathcal{U}(\mathfrak{g})$.

Exercise 18 (Grouplike and primitive elements)
Let $(B, \mu, \eta, \Delta, \epsilon)$ be a bialgebra. Show that:

(a) for any grouplike element $a \in B$ we have $\epsilon(a) = 1$

(b) for any primitive element $x \in B$ we have $\epsilon(x) = 0$.

If B furthermore admits a Hopf algebra structure with the antipode $\gamma : B \to B$ then show:

(c) any grouplike element $a \in B$ is invertible and we have $\gamma(a) = a^{-1}$

(d) for any primitive element $x \in B$ we have $\gamma(x) = -x$.

Definition 3.32. Let $B_1 = (B_1, \mu_1, \Delta_1, \eta_1, \epsilon_1)$ and $B_2 = (B_2, \mu_2, \Delta_2, \eta_2, \epsilon_2)$ be two bialgebras. A linear map $f : B_1 \to B_2$ is said to be a homomorphism of bialgebras if f is a homomorphism of algebras from (B_1, μ_1, η_1) to (B_2, μ_2, η_2), and a homomorphism of coalgebras from $(B_1, \Delta_1, \epsilon_1)$ to $(B_2, \Delta_2, \epsilon_2)$.

In other words, a homomorphism of bialgebras is a linear map f that preserves the structural maps in the following sense

$$f \circ \mu_1 = \mu_2 \circ (f \otimes f), \qquad f \circ \eta_1 = \eta_2, \qquad (f \otimes f) \circ \Delta_1 = \Delta_2 \circ f, \qquad \epsilon_1 = \epsilon_2 \circ f.$$

Definition 3.33. Let $H_1 = (H_1, \mu_1, \Delta_1, \eta_1, \epsilon_1, \gamma_1)$ and $H_2 = (H_2, \mu_2, \Delta_2, \eta_2, \epsilon_2, \gamma_2)$ be two Hopf algebras. A linear map $f : H_1 \to H_2$ is said to be a homomorphism of Hopf algebras if f is a homomorphism of bialgebras from $(H_1, \mu_1, \Delta_1, \eta_1, \epsilon_1)$ to $(H_2, \mu_2, \Delta_2, \eta_2, \epsilon_2)$ and furthermore

$$f \circ \gamma_1 = \gamma_2 \circ f.$$

In fact, one can show that in the definition of a homomorphism of Hopf algebras the condition that f respects the antipode already follows from the properties of a homomorphism of bialgebras.

As usual, an isomorphism is a bijective homomorphism. One can explicitly classify low dimensional bialgebras and Hopf algebras up to isomorphism.

Exercise 19 (Two dimensional bialgebras)

(a) Classify all two-dimensional bialgebras up to isomorphism.

(b) Which of the two-dimensional bialgebras admit a Hopf algebra structure?

Motivation for the definitions from representations

Recall that for a finite group we were able not only to take direct sums of representations, but also we made the tensor product of representations a representation, the one dimensional vector space a trivial representation, and the dual of a representation a representation.

Suppose now A is an algebra and $\rho_V : A \to \mathrm{End}(V)$ and $\rho_W : A \to \mathrm{End}(W)$ are representations of A in V and W, respectively. Taking direct sums of the representations works just like before: we set

$$a.(v + w) = \rho_V(v) + \rho_W(w) \qquad \text{for all } v \in V \subset V \oplus W \text{ and } w \in W \subset V \oplus W.$$

Trivial representation

Can we make the ground field $\mathbb{C}$ a trivial representation? For a general algebra there is no canonical way of doing so — one needs some extra structure. Conveniently, the *counit* is exactly what is needed. Indeed, when we interpret $\mathrm{End}(\mathbb{C}) \cong \mathbb{C}$, identifying a linear map $\mathbb{C} \to \mathbb{C}$ with its sole eigenvalue, a map $\epsilon : A \to \mathbb{C}$ becomes a one dimensional representation if and only if the axioms (H5′) and (H6) hold. So when we have a counit ϵ we set

$$a.z = \epsilon(a)\, z \in \mathbb{C} \qquad \text{for } z \in \mathbb{C}, \tag{3.4}$$

and call this the trivial representation. Note that using the counit of the Hopf algebra of a group, Example 3.28, the trivial representation of a group is what we defined it to be before.

Tensor product representation

It seems natural to ask how to take tensor products of representations of algebras, and again the answer is that one needs some extra structure. Now the *coproduct* $\Delta : A \to A \otimes A$ with the axioms (H4) and (H5) precisely guarantees that the formula

$$\rho_{V \otimes W} = (\rho_V \otimes \rho_W) \circ \Delta$$

defines a representation of A on $V \otimes W$. With Sweedler's sigma notation this reads

$$a.(v \otimes w) = \sum_{(a)} (a_{(1)}.v) \otimes (a_{(2)}.w) \qquad \text{for } v \in V,\ w \in W. \tag{3.5}$$

In particular, using the coproduct of the Hopf algebra of a group, Example 3.28, this definition coincides with the definition of tensor product representation we gave when discussing groups.

Exercise 20 (Trivial representation and tensor product representation)
Check that the formulas (3.4) and (3.5) define representations if we assume the axioms mentioned. Compare with Exercise 15. Check also that with the Hopf algebra structure on $\mathbb{C}[G]$ given in Example 3.28, these definitions agree with the corresponding representations of groups.

Dual representation and the representation $\mathrm{Hom}(V, W)$

How about duals then? For any representation V we'd like to make $V^* = \mathrm{Hom}(V, \mathbb{C})$ a representation. This can be seen as a particular case of $\mathrm{Hom}(V, W)$, where both V and W are representations — we take W to be the trivial one dimensional representation $\mathbb{C}$. When we have not only a bialgebra, but also an antipode satisfying (H3), then the formula

$$a.T = \sum_{(a)} \rho_W(a_{(1)}) \circ T \circ \rho_V(\gamma(a_{(2)})) \tag{3.6}$$

turns out to work, as we will verify a little later. Again, the antipode of Example 3.28 leads to the definitions we gave for groups.

Exercise 21 (Dual representation and the relation of $W \otimes V^*$ and $\mathrm{Hom}(V, W)$ for Hopf algebras)

(a) *Let $\rho_V : A \to \mathrm{End}(V)$ be a representation of a Hopf algebra $A = (A, \mu, \Delta, \eta, \epsilon, \gamma)$. Check that the formula one gets for the dual representation $V^* = \mathrm{Hom}(V, \mathbb{C})$ from Equation (3.6) is*

$$a.\varphi = \Big(\rho_V(\gamma(a))\Big)^*(\varphi) \qquad \text{for all } a \in A,\ \varphi \in V^*, \tag{3.7}$$

that is, any $a \in A$ acts on the dual by the transposis of the action of the antipode of a.

(b) *Check that when V and W are finite dimensional representations of a Hopf algebra A, then the representations $W \otimes V^*$ and $\mathrm{Hom}(V, W)$ are isomorphic, with the isomorphism as in Exercise 3.*

Although we have given a representation theoretic interpretation for the coproduct Δ, the counit ϵ, and the antipode γ, the role of the axioms (H1') and (H2') of a coalgebra hasn't been made clear yet. It is easy to see, however, that the canonical linear isomorphism between the triple tensor products

$$(V_1 \otimes V_2) \otimes V_3 \qquad \text{and} \qquad V_1 \otimes (V_2 \otimes V_3)$$

becomes an isomorphism of representations with the definition (3.5) when coassociativity (H1') is imposed. Likewise, the canonical identifications of V with

$$V \otimes \mathbb{C} \qquad \text{and} \qquad \mathbb{C} \otimes V$$

become isomorphisms of representations with the definition (3.4) when counitality (H2') is imposed.

Thus we see that the list of nine axioms (H1), (H1'), (H2), (H2'), (H3), (H4), (H5), (H5'), (H6) is very natural in view of standard operations that we want to perform for representations.

One more remark is in order: the "flip"

$$S_{V,W} : V \otimes W \to W \otimes V \qquad v \otimes w \mapsto w \otimes v$$

gives a rather natural vector space isomorphism between $V \otimes W$ and $W \otimes V$. With the definition (3.5), it would be an isomorphism of representations if we required the coproduct to be cocommutative, i.e. that the coproduct Δ is equal to the opposite coproduct $\Delta^{cop} := S_{A,A} \circ \Delta$. However, we choose *not* to require cocommutativity in general — in fact the most interesting examples of Hopf algebras are certain quantum groups, where instead of "flipping" the factors of tensor product by $S_{V,W}$ we can do "braiding" on the factors. We will return to this point later on in the course.

3.6 The dual of a coalgebra

When $f : V \to W$ is a linear map, its transpose is the linear map $f^* : W^* \to V^*$ given by

$$\langle f^*(\varphi), v\rangle = \langle \varphi, f(v)\rangle \qquad \text{for all } \varphi \in W^*, v \in V.$$

Recall also that we have the inclusion $V^* \otimes W^* \subset (V \otimes W)^*$ with the interpretation

$$\langle \psi \otimes \varphi, v \otimes w\rangle = \langle \psi, v\rangle \langle \varphi, w\rangle \qquad \text{for } \psi \in V^*, \varphi \in W^*, v \in V, w \in W,$$

and observe that the dual of the ground field can be naturally identified with the ground field itself

$$\mathbb{C}^* \cong \mathbb{C} \qquad \text{via} \qquad \mathbb{C}^* \ni \phi \leftrightarrow \langle \phi, 1\rangle \in \mathbb{C}.$$

Theorem 3.34
Let C be a coalgebra, with coproduct $\Delta : C \to C \otimes C$ and counit $\epsilon : C \to \mathbb{C}$. Set $A = C^*$ and

$$\mu = \Delta^*\big|_{C^* \otimes C^*} : A \otimes A \to A \qquad , \qquad \eta = \epsilon^* : \mathbb{C} \to A.$$

Then (A, μ, η) is an algebra.

Proof. Denote $1_A = \eta(1)$. Compute for $\varphi \in C^* = A$ and $c \in C$, using (H2') in the last step,

$$\langle \varphi\, 1_A, c\rangle = \langle \varphi \otimes 1_A, \Delta(c)\rangle = \sum_{(c)} \langle \varphi, c_{(1)}\rangle \langle 1_A, c_{(2)}\rangle = \langle \varphi, \sum_{(c)} c_{(1)} \epsilon(c_{(2)})\rangle = \langle \varphi, c\rangle$$

to obtain $\varphi\, 1_A = \varphi$. Similarly one proves $1_A\, \varphi = \varphi$ and gets unitality for A. Associativity of $\mu = \Delta^*$ is also easy to show using the coassociativity (H2') of Δ. □

In fact taking the dual is a contravariant functor from the category of coalgebras to the category of algebras, as follows from the following observation.

Lemma 3.35
Let $C_j = (C_j, \Delta_j, \epsilon_j)$, $j = 1, 2$, be two coalgebras and let $f : C_1 \to C_2$ be a homomorphism of coalgebras. Let $f^* : C_2^* \to C_1^*$ be the transpose of f. Then f^* is a homomorphism of algebras from $(C_2^*, \Delta_2^*, \epsilon_2^*)$ to $(C_1^*, \Delta_1^*, \epsilon_1^*)$

Remark 3.36. If $f : C_1 \to C_2$ and $g : C_2 \to C_3$ are linear maps, then the transposes of course satisfy $(g \circ f)^* = f^* \circ g^*$.

Proof. The property of being a homomorphism of coalgebras means $(f \otimes f) \circ \Delta_1 = \Delta_2 \circ f : C_1 \to C_2 \otimes C_2$ and $\epsilon_1 = \epsilon_2 \circ f : C_1 \to \mathbb{C}$. Taking the transpose of the latter we get the equality $\epsilon_1^* = f^* \circ \epsilon_2^*$ of linear maps $\mathbb{C}^* \to C_1^*$. With the usual identification $\mathbb{C}^* \cong \mathbb{C}$, this states that the image under f^* of the unit of C_2^* is the unit of C_1^*. Similarly, we take the transpose of the first property, and obtain $\Delta_1^* \circ (f \otimes f)^* = f^* \circ \Delta_2^*$, for maps $(C_2 \otimes C_2)^* \to C_1^*$. Note that $C_2^* \otimes C_2^* \subset (C_2 \otimes C_2)^*$, and on this subspace the maps $(f \otimes f)^*$ and $f^* \otimes f^*$ coincide. We conclude that the image under f^* of a product in C_2^* is a product in C_1^* of images under f^*. □

3.7 Convolution algebras

One of the main goals of this section is to prove the following facts about the antipode.

Theorem 3.37
Let $H = (H, \mu, \Delta, \eta, \epsilon, \gamma)$ be a Hopf algebra.

(!) The antipode γ is unique in the following sense: if $\gamma' : H \to H$ is another linear map which satisfies (H3), then $\gamma' = \gamma$.

(i) The map $\gamma : H \to H$ is a homomorphism of algebras from $H = (H, \mu, \eta)$ to $H^{\mathrm{op}} = (H, \mu^{\mathrm{op}}, \eta)$.

(ii) The map $\gamma : H \to H$ is a homomorphism of coalgebras from $H = (H, \Delta, \epsilon)$ to $H^{\mathrm{cop}} = (H, \Delta^{\mathrm{cop}}, \epsilon)$.

In other words the property (i) says that we have

$$\gamma(1_H) \;=\; 1_H \qquad \text{and} \qquad \gamma(a\, b) \;=\; \gamma(b)\, \gamma(a) \qquad \forall a, b \in H.$$

The property (ii) says that we have

$$\gamma(\Delta(a)) \;=\; \sum_{(a)} \gamma(a_{(2)})\, \gamma(a_{(1)}) \qquad \text{and} \qquad \epsilon(\gamma(a)) \;=\; \epsilon(a) \qquad \forall a \in H.$$

Definition 3.38. Let $C = (C, \Delta, \epsilon)$ be a coalgebra and $A = (A, \mu, \eta)$ an algebra. For f, g linear maps $C \to A$ define the convolution product of f and g as the linear map

$$f \star g \;=\; \mu \circ (f \otimes g) \circ \Delta \;:\; C \to A,$$

and the convolution unit $1_\star$ as the linear map

$$1_\star \;=\; \eta \circ \epsilon \;:\; C \to A.$$

The convolution algebra associated with C and A is the vector space $\mathrm{Hom}(C, A)$ equipped with product $\star$ and unit $1_\star$. The convolution algebra of a bialgebra $B = (B, \mu, \Delta, \eta, \epsilon)$ is the convolution algebra associated with the coalgebra (B, Δ, ϵ) and the algebra (B, μ, η), and the convolution algebra of a Hopf algebra is defined similarly.

Proposition 3.39
The convolution algebra is an associative unital algebra.

Sketch of a proof. Associativity for the convolution algebra follows easily from the associativity of A and coassociativity of C, and unitality of the convolution algebra follows easily from the unitality of A and counitality of C. □

Concolution algebras have applications for example in combinatorics. For now, we will use them to prove properties of the antipode.

Proof of Theorem 3.37. Let us first prove the uniqueness (!). By (H3), the antipode $\gamma \in \mathrm{Hom}(H, H)$ is the two-sided convolutive inverse of $\mathrm{id}_H \in \mathrm{Hom}(H, H)$ in the convolution algebra of the Hopf algebra H, that is we have

$$\gamma \star \mathrm{id}_H = 1_\star = \mathrm{id}_H \star \gamma.$$

In an associative algebra a left inverse has to coincide with a right inverse if both exist. Indeed suppose that γ' would also satisfy (H3) so that in particular $\mathrm{id}_H \star \gamma' = 1_\star$. Then we compute

$$\gamma \;=\; \gamma \star 1_\star \;=\; \gamma \star (\mathrm{id}_H \star \gamma') \;=\; (\gamma \star \mathrm{id}_H) \star \gamma' \;=\; 1_\star \star \gamma' \;=\; \gamma'.$$

Then let us prove (i): the antipode is a homomorphism of algebras to the opposite algebra. We must show that the antipode preserves the unit, $\gamma \circ \eta = \eta$, and that it reverses the product, $\gamma \circ \mu = \mu^{\mathrm{op}} \circ (\gamma \otimes \gamma)$. Preserving unit is easily seen: recall that 1_H is grouplike, $\Delta(1_H) = 1_H \otimes 1_H$ and then apply (H3) to 1_H to see that

$$1_H \overset{\text{(H3)}}{=} \Big(\mu \circ (\gamma \otimes \mathrm{id}_H)\Big)(1_H \otimes 1_H)) \;=\; \gamma(1_H)\, 1_H \overset{\text{(H2)}}{=} \gamma(1_H).$$

Now consider the convolution algebra $\mathrm{Hom}(H \otimes H, H)$ associated with the coalgebra $H \otimes H$ with coproduct and counit as follows

$$\begin{aligned} \Delta_2(a \otimes b) \;&=\; \sum_{(a),(b)} a_{(1)} \otimes b_{(1)} \otimes a_{(2)} \otimes b_{(2)} \;=\; \Big((\mathrm{id}_H \otimes S_{H,H} \otimes \mathrm{id}_H) \circ (\Delta \otimes \Delta)\Big)(a \otimes b) \\ \epsilon_2(a \otimes b) \;&= \epsilon(a)\, \epsilon(b) \end{aligned}$$

and with the algebra $H = (H, \mu, \eta)$. Note that we can write $\Delta_2 = (\mathrm{id}_H \otimes S_{H,H} \otimes \mathrm{id}_H) \circ (\Delta \otimes \Delta)$ and $\epsilon_2 = \epsilon \otimes \epsilon$. We will show (a) that $\mu \in \mathrm{Hom}(H \otimes H, H)$ has a right convolutive inverse $\gamma \circ \mu^{\mathrm{op}}$, and (b) that μ has a left convolutive inverse $\mu \circ (\gamma \otimes \gamma)$. To prove (a), compute for $a, b \in H$

$$\begin{aligned} \mu \star (\gamma \circ \mu) \;&= \mu \circ \Big(\mu \otimes (\gamma \circ \mu)\Big) \circ \Delta_2 \\ &= \mu \circ (\mathrm{id}_H \otimes \gamma) \circ (\mu \otimes \mu) \circ (\mathrm{id}_H \otimes S_{H,H} \otimes \mathrm{id}_H) \circ (\Delta \otimes \Delta) \\ &\overset{\text{(H4)}}{=} \mu \circ (\mathrm{id}_H \otimes \gamma) \circ \Delta \circ \mu \\ &\overset{\text{(H3)}}{=} \eta \circ \epsilon \circ \mu \\ &\overset{\text{(H5')}}{=} \eta \circ (\epsilon \otimes \epsilon) \;=\; \eta \circ \epsilon_2 \;=\; 1_\star \end{aligned}$$

To prove (b), compute in the Sweedler's sigma notation

$$\begin{aligned} \Big(\Big(\mu \circ S_{H,H} \circ (\gamma \otimes \gamma)\Big) \star \mu\Big)(a \otimes b) \;&=\; \sum_{(a),(b)} \Big(\gamma(b_{(1)})\, \gamma(a_{(1)})\Big) \Big(a_{(2)}\, b_{(2)}\Big) \\ &\overset{\text{(H3) for } a}{=} \epsilon(a) \sum_{(b)} \gamma(b_{(1)})\, 1_H\, b_{(2)} \\ &\overset{\text{(H3) for } b}{=} \epsilon(a)\epsilon(b)\; 1_H, \end{aligned}$$

which is the value of $1_\star = \eta \circ \epsilon_2$ on the element $a \otimes b$. Now a right inverse of μ has to coincide with a left inverse of μ, so we get

$$\gamma \circ \mu \;=\; \mu \circ S_{H,H} \circ (\gamma \otimes \gamma),$$

as we wanted.

We leave it as an exercise for the reader to prove (ii) by finding appropriate formulas for right and left inverses of Δ in the convolution algebra $\mathrm{Hom}(H, H \otimes H)$. □

Corollary 3.40
For $H = (H, \mu, \Delta, \eta, \epsilon, \gamma)$ a Hopf algebra, V and W representations of (H, μ, η), the space $\mathrm{Hom}(V, W)$ of linear maps between the representations becomes a representation by the formula of Equation (3.6),

$$\Big(a.T\Big)(v) \;=\; \sum_{(a)} a_{(1)}.\Big(T(\gamma(a_{(2)}).v)\Big) \qquad \textit{for } a \in H,\, T \in \mathrm{Hom}(V, W),\, v \in V.$$

Proof. The property $1_H.T = T$ is obvious in view of $\Delta(1_H) = 1_H \otimes 1_H$ and $\gamma(1_H) = 1_H$. Using the facts that $\gamma : H \to H^{\mathrm{op}}$ and $\Delta : H \to H \otimes H$ are homomorphisms of algebras, we also check

$$\begin{aligned}\Big(a.(b.T)\Big)(v) &= \sum_{(a)} a_{(1)}.\Big((b.T)(\gamma(a_{(2)}).v)\Big) = \sum_{(a),(b)} a_{(1)}.b_{(1)}.\Big(T(\gamma(b_{(2)})\gamma(a_{(2)}).v)\Big) \\ &\overset{\gamma \text{ homom.}}{=} \sum_{(a),(b)} (a_{(1)}b_{(1)}).\Big(T(\gamma(a_{(2)}b_{(2)}).v)\Big) \overset{\Delta \text{ homom.}}{=} \sum_{(ab)} (ab)_{(1)}.\Big(T(\gamma((ab)_{(2)}).v)\Big) \\ &= \Big((ab).T\Big)(v).\end{aligned}$$

□

Corollary 3.41
Suppose that $H = (H, \mu, \Delta, \eta, \epsilon, \gamma)$ is a Hopf algebra which is either commutative or cocommutative. Then the antipode is involutive, that is $\gamma \circ \gamma = \mathrm{id}_H$.

Proof. Assume that A is commutative. Now, since γ is a morphism of algebras $A \to A^{\mathrm{op}}$ we have

$$\begin{aligned}\gamma^2 \star \gamma &= \mu \circ (\gamma^2 \otimes \gamma) \circ \Delta \\ &= \gamma \circ \mu^{\mathrm{op}} \circ (\gamma \otimes \mathrm{id}_A) \circ \Delta \\ &= \gamma \circ \mu \circ (\gamma \otimes \mathrm{id}_A) \circ \Delta \\ &= \gamma \circ \eta \circ \epsilon = \eta \circ \epsilon = 1_\star.\end{aligned}$$

We conclude that γ^2 is a left inverse of γ in the convolution algebra (one could easily show that γ^2 is in fact a two-sided inverse). But id_A is a right (in fact two-sided) inverse of γ, and as usually in associative algebras we therefore get $\gamma^2 = \mathrm{id}_A$. The case of a cocommutative Hopf algebra is handled similarly. □

Above we showed that the antipode is an involution if the Hopf algebra is commutative or cocommutative. The cocommutativity $\Delta(x) = \Delta^{\mathrm{cop}}(x)$ will later be generalized a little: braided Hopf algebras have $\Delta(x)$ and $\Delta^{\mathrm{cop}}(x)$ conjugates of each other and we will show that the antipode is always invertible in such a case — in fact we will see that the square of the antipode is an inner automorphism of a braided Hopf algebra. It can also be shown that the antipode of a finite dimensional Hopf algebra is always invertible. The following exercise characterizes invertibility of the antipode in terms of the existence of antipodes for the opposite and co-opposite bialgebras.

Exercise 22 (Opposite and co-opposite bialgebras and Hopf algebras)
Suppose that $A = (A, \mu, \Delta, \eta, \epsilon)$ is a bialgebra.

(a) *Show that all of the following are bialgebras:*

- *the opposite bialgebra $A^{\mathrm{op}} = (A, \mu^{\mathrm{op}}, \Delta, \eta, \epsilon)$*
- *the co-opposite bialgebra $A^{\mathrm{cop}} = (A, \mu, \Delta^{\mathrm{cop}}, \eta, \epsilon)$*
- *the opposite co-opposite bialgebra $A^{\mathrm{op,cop}} = (A, \mu^{\mathrm{op}}, \Delta^{\mathrm{cop}}, \eta, \epsilon)$.*

Suppose furthermore that $\gamma : A \to A$ satisfies (H3) so that $(A, \mu, \Delta, \eta, \epsilon, \gamma)$ is a Hopf algebra.

(b) *Show that $A^{\mathrm{op,cop}} = (A, \mu^{\mathrm{op}}, \Delta^{\mathrm{cop}}, \eta, \epsilon, \gamma)$ is a Hopf algebra, called the the opposite co-opposite Hopf algebra.*

(c) *Show that the following conditions are equivalent*

- *the opposite bialgebra A^{op} admits an antipode $\tilde{\gamma}$*
- *the co-opposite bialgebra A^{cop} admits an antipode $\tilde{\gamma}$*
- *the antipode $\gamma : A \to A$ is an invertible linear map, with inverse $\tilde{\gamma}$.*

Convolution algebras are practical also for checking that any map that preserves a bialgebra structure must in fact preserve a Hopf algebra structure (this is in fact a generalization of the uniqueness of the antipode).

Lemma 3.42
Let $H = (H, \mu, \Delta, \eta, \epsilon, \gamma)$ and $H' = (H', \mu', \Delta', \eta', \epsilon', \gamma')$ be Hopf algebras, and let $f : H \to H'$ be a homomorphism of bialgebras. Then we have $f \circ \gamma = \gamma' \circ f$.

Proof. Consider the convolution algebra $\mathrm{Hom}(H, H')$ associated to the coalgebra (H, Δ, ϵ) and algebra (H', μ', η'). It is easy to show that both $f \circ \gamma$ and $\gamma' \circ f$ are inverses of f in this convolution algebra, and consequently they must be equal. □

Exercise 23 (The incidence coalgebra and incidence algebra of a poset)
A partially ordered set (poset) is a set P together with a binary relation $\leq$ on P which is reflexive ($x \leq x$ for all $x \in P$), antisymmetric (if $x \leq y$ and $y \leq x$ then $x = y$) and transitive (if $x \leq y$ and $y \leq z$ then $x \leq z$). Notation $x \prec y$ means $x \leq y$ and $x \neq y$. Notation $x \geq y$ means $y \leq x$. If $x, y \in P$ and $x \leq y$, then we call the set

$$[x, y] \; = \; \{z \in P \mid x \leq z \text{ and } z \leq y\}$$

an interval in P.

Suppose that P is a poset such that all intervals in P are finite (a locally finite poset). Let I_P be the set of intervals of P, and let C_P be the vector space with basis I_P. Define $\Delta : C_P \to C_P \otimes C_P$ and $\epsilon : C_P \to \mathbb{C}$ by linear extension of

$$\Delta([x, y]) \; = \sum_{z \in [x,y]} [x, z] \otimes [z, y] \quad , \qquad \epsilon([x, y]) \; = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{if } x \prec y \end{cases} .$$

(a) *Show that $C_P = (C_P, \Delta, \epsilon)$ is a coalgebra (we call C_P the incidence coalgebra of P).*

The incidence algebra A_P of the poset P is the convolution algebra associated with the coalgebra C_P and the algebra $\mathbb{C}$. Define $\zeta \in A_P$ by its values on basis vectors $\zeta([x, y]) = 1$ for all intervals $[x, y] \in I_P$.

(b) *Show that ζ is invertible in A_P, with inverse m (called the Möbius function of P) whose values on the basis vectors are determined by the recursions*

$m([x, x]) = 1$ *for all* $x \in P$
$m([x, y]) = -\sum_{z : x \leq z \prec y} m([x, z])$ *for all* $x \in P$, $y \geq x$.

(c) *Let $f : P \to \mathbb{C}$ be a function and suppose that there is a $p \in P$ such that $f(x) = 0$ unless $x \geq p$. Prove the Möbius inversion formula: if*

$$g(x) \; = \sum_{y \leq x} f(y)$$

then

$$f(x) \; = \sum_{y \leq x} g(y) \; m([y, x]).$$

(Hint: *It may be helpful to define a $\hat{f} \in A_P$ with the property $\hat{f}([p, x]) = f(x)$ and $\hat{g} = \hat{f} \star \zeta$.)*

3.8 Representative forms

Let $A = (A, \mu, \eta)$ be an algebra.

Suppose that V is a finite dimensional A-module, and that $u_1, u_2, \ldots, u_n$ is a basis of V. Note that for any $a \in A$ we can write $a.u_j \; = \; \sum_{i=1}^{n} \lambda_{i,j} \, u_i$ with $\lambda_{i,j} \in \mathbb{C}$, $i, j = 1, 2, \ldots, n$. The coefficients depend linearly on a, and thus they define elements of the dual $\lambda_{i,j} \in A^*$ called the representative forms of the A-module V with respect to the basis $u_1, u_2, \ldots, u_n$. The left multiplication of the basis vectors by elements of A now takes the form

$$a.u_j \;=\; \sum_{i=1}^{n} \langle \lambda_{i,j}, a\rangle \, u_i.$$

The A-module property gives

$$\sum_{i=1}^{n} \langle \lambda_{i,j}, ab\rangle \, u_i \;=\; (ab).v \;=\; a.(b.v) \;=\; \sum_{i,k=1}^{n} \langle \lambda_{i,k}, a\rangle \, \langle \lambda_{k,j}, b\rangle \, u_i,$$

that is

$$\langle \lambda_{i,j}, ab\rangle \;=\; \sum_{k=1}^{n} \langle \lambda_{i,k}, a\rangle \, \langle \lambda_{k,j}, b\rangle \qquad \text{for all } i,j = 1,2,\ldots,n. \tag{3.8}$$

3.9 The restricted dual of algebras and Hopf algebras

Recall that for C a coalgebra, the dual space C^* becomes an algebra with the structural maps (product and unit) which are the transposes of the structural maps (coproduct and counit) of the coalgebra.

It then seems natural to ask whether the dual of an algebra $A = (A, \mu, \eta)$ is a coalgebra. When we take the transposes of the structural maps

$$\eta : \mathbb{C} \to A \qquad \text{and} \qquad \mu : A \otimes A \to A,$$

we get

$$\eta^* : \mathbb{C}^* \to A^*$$

which could serve as a counit when we identify $\mathbb{C}^* \cong \mathbb{C}$, but the problem is that the candidate for a coproduct

$$\mu^* : A^* \to (A \otimes A)^* \;\supset\; A^* \otimes A^*,$$

takes values in the space $(A \otimes A)^*$ which in general is larger than the second tensor power of the dual, $A^* \otimes A^*$. The cure to the situation is to restrict attention to the preimage of the second tensor power of the dual.

Definition 3.43. The restricted dual of an algebra $A = (A, \mu, \eta)$ is the subspace $A^\circ \subset A^*$ defined as

$$A^\circ \;=\; (\mu^*)^{-1}(A^* \otimes A^*).$$

Example 3.44. Let V be a finite dimensional A-module with basis $u_1, u_2, \ldots, u_n$, and denote by $\lambda_{i,j} \in A^*$, $i,j = 1,2,\ldots,n$, the representative forms. Then from Equation (3.8) we get for any $a, b \in A$

$$\langle \mu^*(\lambda_{i,j}), a \otimes b\rangle \;=\; \langle \lambda_{i,j}, \mu(a \otimes b)\rangle \;=\; \langle \lambda_{i,j}, ab\rangle \;=\; \sum_{k=1}^{n} \langle \lambda_{i,k}, a\rangle \, \langle \lambda_{k,j}, b\rangle \;=\; \sum_{k=1}^{n} \langle \lambda_{i,k} \otimes \lambda_{k,j}, a \otimes b\rangle.$$

We conclude that

$$\mu^*(\lambda_{i,j}) \;=\; \sum_{k=1}^{n} \lambda_{i,k} \otimes \lambda_{k,j} \;\in\; A^* \otimes A^*, \tag{3.9}$$

and therefore $\lambda_{i,j} \in A^\circ$.

The example shows that all representative forms of finite dimensional A-modules are in the restricted dual, and we will soon see that the restricted dual is spanned by these.

The goal of this section is to prove the following results.

Theorem 3.45
For $A = (A, \mu, \eta)$ an algebra, the restricted dual

$$(A^\circ, \mu^*|_{A^\circ}, \eta^*|_{A^\circ})$$

is a coalgebra.

Theorem 3.46
For $H = (H, \mu, \Delta, \eta, \epsilon, \gamma)$ a Hopf algebra, the restricted dual

$$(H^\circ, \Delta^*|_{H^\circ \times H^\circ}, \mu^*|_{H^\circ}, \epsilon^*, \eta^*|_{H^\circ}, \gamma^*|_{A^\circ})$$

is a Hopf algebra.

Admitting the above results, we notice that one-dimensional representations of an algebra admit the following characterization.

Exercise 24 (Grouplike elements of the restricted dual)
Let $A = (A, \mu, \eta)$ be an algebra and consider its restricted dual $A^\circ = (\mu^*)^{-1}(A^* \otimes A^*)$ with the coproduct $\Delta = \mu^*|_{A^\circ}$ and counit $\epsilon = \eta^*|_{A^\circ}$. Show that for a linear map $f : A \to \mathbb{C}$ the following are equivalent:

- *The function f is a homomorphism of algebras.*
  *(*Remark: *An interpretation is that f defines a one-dimensional representation of A.)*
- *The element f is grouplike in A°.*

Before starting with the proofs of Theorems 3.45 and 3.46, we need some preparations.

Lemma 3.47
Let $A = (A, \mu, \eta)$ be an algebra and equip the dual A^* with the left A-module structure of Example 3.12. Then for any $f \in A^*$ we have

$$f \in A^\circ \qquad \text{if and only if} \qquad \dim (A.f) < \infty,$$

where $A.f \subset A^*$ is the submodule generated by f.

In other words, the elements of the restricted dual are precisely those that generate a finite dimensional submodule of A^*.

Remark 3.48. Observe that $A^\circ = (\mu^*)^{-1}(A^* \otimes A^*) = ((\mu^{\mathrm{op}})^*)^{-1}(A^* \otimes A^*)$. Thus the analogous property holds for the right A-module structure of Example 3.12: we have $f \in A^\circ$ if and only if $f.A \subset A^*$ is finite dimensional.

Proof of Lemma 3.47. Suppose first that $f \in A^\circ$, so that $\mu^*(f) = \sum_{i=1}^n g_i \otimes h_i$, for some $n \in \mathbb{N}$ and $g_i, h_i \in A^*$, $i = 1, 2, \ldots, n$. Then for any $a, x \in A$ we get

$$\begin{aligned} \langle a.f, x \rangle &= \langle f, xa \rangle = \langle f, \mu(x \otimes a) \rangle = \langle \mu^*(f), x \otimes a \rangle \\ &= \sum_{i=1}^n \langle g_i \otimes h_i, x \otimes a \rangle = \sum_{i=1}^n \langle g_i, x \rangle \langle h_i, a \rangle = \Big\langle \sum_{i=1}^n \langle h_i, a \rangle \, g_i, x \Big\rangle. \end{aligned}$$

This shows that

$$a.f = \sum_{i=1}^{n} \left\langle h_i, a \right\rangle g_i$$

and thus $A.f$ is contained in the linear span of $g_1, \ldots, g_n$, and in particular $A.f$ is finite dimensional. Suppose then that $\dim\,(A.f) < \infty$. Let $(g_i)_{i=1}^r$ be a basis of $A.f$, and observe that writing $a.f$ in this basis we get $a.f = \sum_{i=1}^r \left\langle h_i, a \right\rangle g_i$ for some $h_i \in A^*$, $i = 1, 2, \ldots, r$. We can then compute for any $x, y \in A$

$$\left\langle \mu^*(f), x \otimes y \right\rangle = \left\langle f, xy \right\rangle = \left\langle y.f, x \right\rangle = \sum_i \left\langle h_i, y \right\rangle \left\langle g_i, x \right\rangle$$

to conclude that $\mu^*(f) = \sum_{i=1}^r g_i \otimes h_i \in A^* \otimes A^*$. □

It follows from the proof that for $f \in A^\circ$, the rank of $\mu^*(f) \subset A^* \otimes A^*$ is equal to the dimension of $A.f$. We in fact easily see that when $\mu^*(f) = \sum_{i=1}^r g_i \otimes h_i \in A^* \otimes A^*$ with r minimal, then $(g_i)_{i=1}^r$ is a basis of $A.f$ and $(h_i)_{i=1}^r$ is a basis of $f.A$.

Corollary 3.49
If $f \in A^\circ$, then we have $\mu^*(f) \subset (A.f) \otimes (f.A) \subset A^\circ \otimes A^\circ$ and therefore

$$\mu^*(A^\circ) \subset A^\circ \otimes A^\circ.$$

Proof. In the above proof we've written $\mu^*(f) = \sum_i g_i \otimes h_i$ with $g_i \in A.f$ and $h_i \in f.A$, so the first inclusion follows. But we clearly have also $A.f \subset A^\circ$ since for any $a \in A$ the submodule of A^* generated by the element $a.f$ is contained in $A.f$, and is therefore also finite dimensional. Similarly one gets $f.A \subset A^\circ$. □

We observe the following.

Corollary 3.50
The restricted dual A° is spanned by the representative forms of finite dimensional A-modules.

Proof. In Example 3.44 we have seen that the representative forms are always in the restricted dual. We must now show that any $f \in A^\circ$ can be written as a linear combination of representative forms. To this end we consider the finite dimensional submodule $A.f$ of A^*. Let $(g_i)_{i=1}^n$ be a basis of $A.f$, and assume without loss of generality that $g_1 = f$ and $g_i = b_i.f$ with $b_i \in A$, $i = 1, 2, \ldots, n$.

As above we observe that there exists $(h_i)_{i=1}^n$ in A^* such that $a.f = \sum_{i=1}^n \left\langle h_i, a \right\rangle g_i$ for all $a \in A$. We compute

$$a.g_j = (a\, b_j).f = \sum_{i=1}^{n} \left\langle h_i, a\, b_j \right\rangle g_i = \sum_{i=1}^{n} \left\langle b_j.h_i, a \right\rangle g_i,$$

so that the representative forms of $A.f$ in the basis (g_i) are $\lambda_{i,j} = b_j.h_i$. In particular since $b_1 = 1_A$ we have $h_i = \lambda_{i,1}$. It therefore suffices to show that f can be written as a linear combination of the elements h_i. But this is evident, since the (right) submodule $f.A$ of A^* contains f and is spanned by (h_i). □

We may write the conclusion above even more concretely as

$$f = f.1_A = \sum_i \left\langle g_i, 1_A \right\rangle h_i = \sum_i \left\langle g_i, 1_A \right\rangle \lambda_{i,1}.$$

Now note that the restricted dual may in fact be trivial.

Exercise 25 (Representations of the canonical commutation relations of quantum mechanics)
Let A be the algebra with two generators x and y, and one relation

$$x\,y - y\,x \;=\; 1 \qquad \text{("canonical commutation relation").}$$

(a) Show that there are no finite-dimensional representations of A except from the zero vector space $V = \{0\}$.

(b) Conclude that $A^\circ = \{0\}$ and that it is impossible to equip A with a Hopf algebra structure.

Proof of Theorem 3.45. From Corollary 3.49 we see that we can interpret the structural maps as maps between the correct spaces,

$$\Delta = \mu^*\big|_{A^\circ} : A^\circ \to A^\circ \otimes A^\circ \qquad \text{and} \qquad \epsilon = \eta^*\big|_{A^\circ} : A^\circ \to \mathbb{C}.$$

To prove counitality, take $f \in A^\circ$ and write as before $\Delta(f) = \mu^*(f) = \sum_i g_i \otimes h_i$, and compute for any $x \in A$

$$\langle (\epsilon \otimes \mathrm{id}_{A^\circ})(\Delta(f)), x\rangle \;=\; \sum_i \epsilon(g_i)\, \langle h_i, x\rangle \;=\; \sum_i \langle g_i, 1_A\rangle\, \langle h_i, x\rangle \;=\; \langle \mu^*(f), 1_A \otimes x\rangle \;=\; \langle f, 1_A x\rangle \;=\; \langle f, x\rangle,$$

which shows $(\epsilon \otimes \mathrm{id}_{A^\circ})(\Delta(f)) = f$, and a similar computation shows $(\mathrm{id}_{A^\circ} \otimes \epsilon)(\Delta(f)) = f$. Coassociativity of μ^* follows from taking the transpose of the associativity of μ once one notices that the transpose maps have the appropriate alternative expressions

$$(\mathrm{id}_A \otimes \mu)^*\big|_{A^*\otimes A^*} \;=\; \mathrm{id}_A^* \otimes \mu^* \;=\; \mathrm{id}_{A^*} \otimes \mu^* \qquad \text{and} \qquad (\mu \otimes \mathrm{id}_A)^*\big|_{A^*\otimes A^*} \;=\; \mu^* \otimes \mathrm{id}_A^* \;=\; \mu^* \otimes \mathrm{id}_{A^*}$$

on the subspaces where we need them. □

Exercise 26 (Taking the restricted dual is a contravariant functor)
Let A and B be two algebras and $f : A \to B$ a homomorphism of algebras, and let f^* be its transpose map $B^* \to A^*$.

(a) Show that for any $\varphi \in B^\circ$ we have $f^*(\varphi) \in A^\circ$.

(b) Show that $f^*|_{B^\circ} : B^\circ \to A^\circ$ is a homomorphism of coalgebras.

To handle restricted duals of Hopf algebras, we present yet a few lemmas which say that the structural maps take values in the appropriate subspaces.

Lemma 3.51
Let $B = (B, \mu, \Delta, \eta, \epsilon)$ be a bialgebra. Then we have $\Delta^*(B^\circ \otimes B^\circ) \subset B^\circ$. Also we have $\mu^*(\epsilon^*(1)) = \epsilon^*(1) \otimes \epsilon^*(1)$ so that $\epsilon^*(1) \in B^\circ$.

Proof. Suppose $f_1, f_2 \in B^\circ$, and write

$$\mu^*(f_k) \;=\; \sum_i g_i^{(k)} \otimes h_i^{(k)} \qquad \text{for } k = 1, 2.$$

To show that $\Delta^*(f_1 \otimes f_2) \in B^\circ$, by definition we need to show that $\mu^*(\Delta^*(f_1 \otimes f_2)) \in B^* \otimes B^*$. Let

$a, b \in B$ and notice that the axiom (H4) saves the day in the following calculation:

$$\begin{aligned}
\langle \mu^*\Big(\Delta^*(f_1 \otimes f_2)\Big), a \otimes b\rangle &= \langle f_1 \otimes f_2, \Delta\Big(\mu(a \otimes b)\Big)\rangle \\
&\overset{\text{(H4)}}{=} \sum_{(a),(b)} \langle f_1 \otimes f_2, a_{(1)}b_{(1)} \otimes a_{(2)}b_{(2)}\rangle \\
&= \sum_{(a),(b)} \langle f_1, a_{(1)}b_{(1)}\rangle \, \langle f_2, a_{(2)}b_{(2)}\rangle \\
&= \sum_{(a),(b)} \sum_{i,j} \langle g_i^{(1)}, a_{(1)}\rangle \, \langle h_i^{(1)}, b_{(1)}\rangle \, \langle g_j^{(2)}, a_{(2)}\rangle \, \langle h_j^{(2)}, b_{(2)}\rangle \\
&= \sum_{i,j} \langle g_i^{(1)} \otimes g_j^{(2)}, \Delta(a)\rangle \, \langle h_i^{(1)} \otimes h_j^{(2)}, \Delta(b)\rangle \\
&= \sum_{i,j} \langle \Delta^*(g_i^{(1)} \otimes g_j^{(2)}) \otimes \Delta^*(h_i^{(1)} \otimes h_j^{(2)}), a \otimes b\rangle \, .
\end{aligned}$$

We conclude that

$$\mu^*\Big(\Delta^*(f_1 \otimes f_2)\Big) = \sum_{i,j} \underbrace{\Delta^*\Big(g_i^{(1)} \otimes g_j^{(2)}\Big)}_{\in B^*} \otimes \underbrace{\Delta^*\Big(h_i^{(1)} \otimes h_j^{(2)}\Big)}_{\in B^*} \in B^* \otimes B^*,$$

and since the images under $\Delta^*|_{B^\circ \otimes B^\circ}$ of simple tensors are in B°, the assertion about Δ^* follows. This computation also shows that axiom (H4) holds in the restricted dual.

To prove the assertion about ϵ^*, note first that with the usual identifications $\langle \epsilon^*(1), a\rangle = \langle 1, \epsilon(a)\rangle = \epsilon(a)$. Take $a, b \in B$ and compute

$$\langle \mu^*(\epsilon^*(1)), a \otimes b\rangle = \langle 1, \epsilon(ab)\rangle = \epsilon(a)\,\epsilon(b) = \langle \epsilon^*(1) \otimes \epsilon^*(1), a \otimes b\rangle.$$

In fact this also shows that axiom (H5) holds in the restricted dual. □

Lemma 3.52
Let $H = (H, \mu, \Delta, \eta, \epsilon, \gamma)$ be a Hopf algebra. Then we have $\gamma^*(H^\circ) \subset H^\circ$.

Proof. Let $f \in H^\circ$, and for $a, b \in H$ compute

$$\begin{aligned}
\langle \mu^*(\gamma^*(f)), a \otimes b\rangle &= \langle f, \gamma(ab)\rangle = \langle f, \gamma(b)\gamma(a)\rangle = \langle \mu^*(f), \gamma(b) \otimes \gamma(a)\rangle \\
&= \sum_i \langle g_i, \gamma(b)\rangle \, \langle h_i, \gamma(a)\rangle = \sum_i \langle \gamma^*(g_i), b\rangle \, \langle \gamma^*(h_i), a\rangle = \sum_i \langle \gamma^*(h_i) \otimes \gamma^*(g_i), a \otimes b\rangle.
\end{aligned}$$

Thus we have

$$\mu^*(\gamma^*(f)) = \sum_i \gamma^*(h_i) \otimes \gamma^*(g_i) \in H^* \otimes H^*.$$

□

Sketch of a proof of Theorem 3.46. We have checked that the structural maps take values in the appropriate spaces (restricted dual or its tensor powers) when their domains of definition are restricted to the appropriate spaces. Taking transposes of all axioms of Hopf algebras, and noticing that the transposes of tensor product maps coincide with the tensor product maps of transposes on the subspaces of our interest, one can mechanically check all the axioms for the Hopf algebra H°. □

Exercise 27 (Representative forms in a representation of the Laurent polynomial algebra)
Let $A = \mathbb{C}[t, t^{-1}] \cong \mathbb{C}[\mathbb{Z}]$ be the algebra of Laurent polynomials

$$A = \left\{ \sum_{n=-N}^{N} c_n t^n \;\middle|\; N \in \mathbb{N}, c_{-N}, c_{-N+1}, \ldots, c_{N-1}, c_N \in \mathbb{C} \right\}.$$

Define the $s \in A^*$ *and* $g_z \in A^*$, *for* $z \in \mathbb{C} \setminus \{0\}$, *by the formulas*

$$\langle g_z, t^n \rangle \;=\; z^n \qquad \langle s, t^n \rangle \;=\; n.$$

(a) Show that $s \in A^\circ$ *and* $g_z \in A^\circ$.

Let us equip A *with the Hopf algebra structure such that* $\Delta(t) \;=\; t \otimes t$.

(b) Let $z \in \mathbb{C} \setminus \{0\}$. *Consider the finite dimensional* A*-module* V *with basis* $u_1, u_2, \ldots, u_n$ *such that*

$$t.u_j \;=\; z\, u_j + u_{j-1} \quad \forall\, j > 1 \qquad \text{and} \qquad t.u_1 \;=\; z u_1.$$

Define the representative forms $\lambda_{i,j} \in A^\circ$ *by* $a.u_j \;=\; \sum_{i=1}^n \langle \lambda_{i,j}, a \rangle\, u_i$. *Show that we have the following equalities in the Hopf algebra* A°:

$$\lambda_{i,j} \;=\; \begin{cases} 0 & \text{if } i > j \\ g_z & \text{if } i = j \\ \frac{z^{i-j}}{(j-i)!}\, s\,(s-1) \cdots (s+i-j+1)\, g_z & \text{if } i < j \end{cases}.$$

Exercise 28 (The restricted dual of the binomial Hopf algebra)
Given two Hopf algebras $(A_i, \mu_i, \Delta_i, \eta_i, \epsilon_i, \gamma_i)$, $i = 1, 2$, *we can form the tensor product of Hopf algebras by equipping* $A_1 \otimes A_2$ *with the structural maps*

$$\mu \;= (\mu_1 \otimes \mu_2) \circ (\mathrm{id}_{A_1} \otimes S_{A_2,A_1} \otimes \mathrm{id}_{A_2}) \qquad \Delta \;= (\mathrm{id}_{A_1} \otimes S_{A_1,A_2} \otimes \mathrm{id}_{A_2}) \circ (\Delta_1 \otimes \Delta_2)$$

$$\eta \;= \eta_1 \otimes \eta_2 \qquad \epsilon \;= \epsilon_1 \otimes \epsilon_2 \qquad \gamma \;= \gamma_1 \otimes \gamma_2.$$

Let $A = \mathbb{C}[x]$ *be the algebra of polynomials in the indeterminate* x, *equipped with the unique Hopf algebra structure such that* $\Delta(x) = 1 \otimes x + x \otimes 1$ *(the binomial Hopf algebra). Show that we have an isomorphism of Hopf algebras*

$$A^\circ \;\cong\; A \otimes \mathbb{C}[\mathbb{C}],$$

that is, the restricted dual of A *is isomorphic to the tensor product of the Hopf algebra* A *with the Hopf algebra of the additive group of complex numbers.*

3.10 A semisimplicity criterion for Hopf algebras

We will later in the course discuss the representation theory of a quantum group $\mathcal{U}_q(\mathfrak{sl}_2)$ (for q not a root of unity). We will explicitly find all irreducible representations, and then the task is to verify complete reducibility.

It is fortunate that to verify semisimplicity of a Hopf algebra, it is sufficient to verify only a particularly simple case. In this section we describe such a semisimplicity criterion for Hopf algebras, which mimicks a standard algebraic proof of complete reducibility of semisimple Lie algebras, and will be used for $\mathcal{U}_q(\mathfrak{sl}_2)$ later in the course.

Proposition 3.53
Suppose that A *is a Hopf algebra for which the following criterion holds:*

- *Whenever* R *is an* A*-module and* $R_0 \subset R$ *is a submodule such that* R/R_0 *is isomorphic to the one-dimensional trivial* A*-module, then* R_0 *has a complementary submodule* P *(which then must be one-dimensional and trivial).*

Then A *is semisimple.*

Remark 3.54. Actually the criterion can be stated in a superficially weaker form: it suffices that whenever R is an A-module and $R_0 \subset R$ is an *irreducible* submodule of codimension one such that R/R_0 is a trivial module, then there is a complementary submodule P to R_0. Indeed, assuming this weaker condition we can perform an induction on dimension to get to the general case. If R_0 is not irreducible, take a nontrivial irreducible submodule $S_0 \subset R_0$. Then consider the module R/S_0 and its submodule R_0/S_0 of codimension one, which is trivial since $(R/S_0)/(R_0/S_0) \cong R/R_0$. The dimensions of the modules in question are strictly smaller, so by induction we can assume that there is a trivial complementary submodule Q/S_0 of dimension one so that $R/S_0 = R_0/S_0 \oplus Q/S_0$ (here $Q \subset R$ is a submodule containing S_0, and $\dim Q = \dim S_0 + 1$). Now, since S_0 is irreducible, we can use the weak form of the criterion to write $Q = S_0 \oplus P$ with P trivial one-dimensional submodule of Q. One concludes that $R = R_0 \oplus P$.

In the proof of Proposition 3.53, we will consider the A-module of linear maps

$$\mathrm{Hom}(V,W) \qquad : \qquad (a.f)(v) \;=\; \sum_{(a)} a_{(1)}.f(\gamma(a_{(2)}).v) \quad \text{for } a \in A,\; v \in V,\; f \in \mathrm{Hom}(V,W)$$

associated to two A-modules V and W. The subspace $\mathrm{Hom}_A(V,W) \subset \mathrm{Hom}(V,W)$ of A-module maps from V to W is

$$\mathrm{Hom}_A(V,W) \;=\; \{f : V \to W \text{ linear} \mid f(a.v) = a.f(v) \text{ for all } v \in V,\, a \in A\}.$$

Generally, for any A-module V, the trivial part V^A of V is defined as

$$V^A \;=\; \{v \in V \mid a.v = \epsilon(a)\, v \text{ for all } a \in A\}.$$

The trivial part of the A-module $\mathrm{Hom}(V,W)$ happens to consist precisely of the A-module maps.

Lemma 3.55
A map $f \in \mathrm{Hom}(V,W)$ is an A-module map if and only if $a.f = \epsilon(a)\, f$ for all $a \in A$. In other words, we have $\mathrm{Hom}_A(V,W) = \mathrm{Hom}(V,W)^A$.

Proof. Assuming that f is an A-module map we calculate

$$(a.f)(v) \;=\; \sum_{(a)} a_{(1)}.f(\gamma(a_{(2)}.v)) \;=\; \sum_{(a)} a_{(1)}\gamma(a_{(2)}).f(v) \;=\; \epsilon(a)\; f(v),$$

which shows the "only if" part. To prove the "if" part, suppose that $a.f = \epsilon(a)\, f$ for all $a \in A$. Then calculate

$$\begin{aligned} f(a.v) \;&=\; f\Big(\sum_{(a)} \epsilon(a_{(1)})a_{(2)}.v\Big) \;=\; \sum_{(a)} \epsilon(a_{(1)})\; f(a_{(2)}.v) \\ &=\; \sum_{(a)} (a_{(1)}.f)(a_{(2)}.v) \;=\; \sum_{(a)} a_{(1)}.f\Big(\gamma(a_{(2)})a_{(3)}.v\Big) \\ &=\; \sum_{(a)} a_{(1)}.f(\epsilon(a_{(2)})\, v) \;=\; a.f(v). \end{aligned}$$

□

The observation that allows us to reduce general semisimplicity to the codimension one criterion concerns the module $\mathrm{Hom}(V,W)$ in the particular case when W is a submodule of V. We are searching for an A-linear projection to W.

Lemma 3.56
Let V be an A-module and $W \subset V$ a submodule. Let

$$r : \mathrm{Hom}(V,W) \to \mathrm{Hom}(W,W)$$

be the restriction map given by $r(f) = f|_W$ *for all* $f : V \to W$. *Denote by* R *the subspace of maps whose restriction is a multiple of the identity of* W, *that is*

$$R = r^{-1}(\mathbb{C}\,\mathrm{id}_W).$$

Then we have

(a) $\mathrm{Im}\,(r|_R) = \mathbb{C}\,\mathrm{id}_W$

(b) $R \subset \mathrm{Hom}(V, W)$ *is a submodule*

(c) $\mathrm{Ker}\,(r|_R) \subset R$ *is a submodule*

(d) $R/\mathrm{Ker}\,(r|_R)$ *is a trivial one dimensional module.*

Proof. The assertion (a) is obvious, since $\mathrm{Im}\,(r|_R) \subset \mathbb{C}\,\mathrm{id}_W$ by definition and the image of any projection $p : V \to W$ is id_W. It follows directly also that $R/\mathrm{Ker}\,(r|_R)$ is a one-dimensional vector space. All the rest of the properties are consequences of the following calculation: if $f \in R$ so that there is a $\lambda \in \mathbb{C}$ such that $f(w) = \lambda\, w$ for all $w \in W$, then for any $a \in A$ we have

$$(a.f)(w) = \sum_{(a)} a_{(1)}.f\big(\gamma(a_{(2)}).w\big) = \sum_{(a)} a_{(1)}.\big(\lambda\, \gamma(a_{(2)}).w\big) = \lambda \sum_{(a)} a_{(1)}\gamma(a_{(2)}).w = \lambda\epsilon(a)\, w.$$

Indeed, this directly implies (b): $(a.f)|_W = \lambda\epsilon(a)\,\mathrm{id}_W$. For (c), note that $\mathrm{Ker}\,(r)$ corresponds to the case $\lambda = 0$, in which case also $(a.f)|_W = 0$. For (d), rewrite the rightmost expression once more to get $(a.f)|_W = \epsilon(a)\, f|_W$ and thus $a.f = \epsilon(a)\, f + g$ where $g = a.f - \epsilon(a)\, f$ and note that $g|_W = 0$. □

We are now ready to give a proof of the semisimplicity criterion.

Proof of Proposition 3.53. Assume the property that all codimension one submodules with trivial quotient modules have complements. We will establish semisimplicity by verifying property (iv) of Proposition 3.18. Suppose therefore that V is a finite dimensional A-module and $W \subset V$ is a submodule. Consider $R \subset \mathrm{Hom}(V, W)$ consisting of those $f : V \to W$ for which the restriction $f|_W$ to W is a multiple of identity, and R_0 consisting of those $f : V \to W$ which are zero on W. By the above lemma $R_0 \subset R \subset \mathrm{Hom}(V, W)$ are submodules and R/R_0 is the one dimensional trivial A-module. By the assumption, then, R_0 has a complementary submodule P, which is one dimensional and trivial. Choose a non-zero $\pi \in P$ normalized so that $\pi|_W = 1\,\mathrm{id}_W$. Then $\pi : V \to W$ is a projection to W. Since P is a trivial module, we have $a.\pi = \epsilon(a)\,\pi$, so by Lemma 3.55 the projection $\pi : V \to W$ is an A-module map. Thus property (iv) of Proposition 3.18 holds, and by the same Proposition, A is semisimple. □

Chapter 4

Quantum groups

4.1 A building block of quantum groups

This section discusses a Hopf algebra H_q, which is an important building block of quantum groups — a kind of "quantum" version of a Borel subalgebra of the Lie algebra $\mathfrak{sl}_2$.

q-integers, q-factorials and q-binomial coefficients

For $n \in \mathbb{N}$ and $0 \leq k \leq n$, define the following rational (in fact polynomial) functions of q:

$$\text{the } q\text{-integer} \qquad [\![n]\!] = 1 + q + q^2 + \cdots + q^{n-1} = \frac{1-q^n}{1-q} \tag{4.1}$$

$$\text{the } q\text{-factorial} \qquad [\![n]\!]! = [\![1]\!]\,[\![2]\!] \cdots [\![n-1]\!]\,[\![n]\!] \tag{4.2}$$

$$\text{the } q\text{-binomial coefficient} \qquad \begin{bmatrix} n \\ k \end{bmatrix} = \frac{[\![n]\!]!}{[\![k]\!]!\,[\![n-k]\!]!}, \tag{4.3}$$

and when $q \in \mathbb{C} \setminus \{0\}$, denote the values of these functions at q by

$$[\![n]\!]_q, \qquad [\![n]\!]_q!, \qquad \begin{bmatrix} n \\ k \end{bmatrix}_q,$$

respectively.

When $q = 1$, one recovers the usual integers, factorials and binomial coefficients.

As simple special cases one has

$$[\![0]\!] = 0, \qquad [\![1]\!] = 1 \qquad \text{and} \qquad [\![0]\!]! = [\![1]\!]! = 1$$

and for all $n \in \mathbb{N}$

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = \begin{bmatrix} n \\ n \end{bmatrix} = 1 \qquad \text{and} \qquad \begin{bmatrix} n \\ 1 \end{bmatrix} = \begin{bmatrix} n \\ n-1 \end{bmatrix} = [\![n]\!].$$

The following exercise shows that the q-binomial coefficients are indeed analoguous to the ordinary binomial coefficients in a particular noncommutative setting.

Exercise 29 (The q-binomial formula)
Suppose A is an algebra and $a, b \in A$ are two elements which satisfy the relation

$$a\,b = q\,b\,a$$

for some $q \in \mathbb{C} \setminus \{0\}$.

(a) *Show that for any* $n \in \mathbb{N}$ *we have*

$$(a+b)^n \;=\; \sum_{k=0}^{n} \left[\!\left[\begin{array}{c} n \\ k \end{array} \right]\!\right]_q b^{n-k}\, a^k.$$

(b) *If* $q = e^{i2\pi/n}$, *show that* $(a+b)^n \;=\; a^n + b^n$.

When q is a root of unity, degeneracies arise. Let p be the smallest positive integer such that $q^p = 1$. Then we have

$$[\![mp]\!]_q \;=\; 0 \quad \forall m \in \mathbb{N} \qquad \text{and} \qquad [\![n]\!]_q! \;=\; 0 \quad \forall n \geq p.$$

The values of the q-binomial coefficients at roots of unity are described in the following exercise.

Exercise 30 (The q-binomial coefficients at roots of unity)
Let $q \in \mathbb{C}$ *be a primitive* p^{th} *root of unity, that is,* $q^p = 1$ *and* $q, q^2, q^3, \ldots, q^{p-1} \neq 1$. *Show that the values of the* q*-binomial coefficients are then described as follows: if the quotients and remainders modulo* p *of* n *and* k *are* $n = p\,D(n) + R(n)$ *and* $k = p\,D(k) + R(k)$ *with* $D(n), D(k) \in \mathbb{N}$ *and* $R(n), R(k) \in \{0, 1, 2, \ldots, p-1\}$, *then*

$$\left[\!\left[\begin{array}{c} n \\ k \end{array} \right]\!\right]_q \;=\; \binom{D(n)}{D(k)} \times \left[\!\left[\begin{array}{c} R(n) \\ R(k) \end{array} \right]\!\right]_q .$$

In particular $\left[\!\left[\begin{array}{c} n \\ k \end{array} \right]\!\right]_q$ *is non-zero only if the remainders satisfy* $R(k) \leq R(n)$.

The Hopf algebra H_q

Let $q \in \mathbb{C} \setminus \{0\}$ and let H_q be the algebra with three generators a, a', b and relations

$$a\,a' \;=\; a'\,a \;=\; 1 \qquad , \qquad a\,b \;=\; q\,b\,a.$$

Because of the first relation we can write $a' = a^{-1}$ in H_q. The collection $(b^m\, a^n)_{m\in\mathbb{N},\, n\in\mathbb{Z}}$ is a vector space basis for H_q. The product in this basis is easily seen to be

$$\mu(b^{m_1}a^{n_1} \otimes b^{m_2}a^{n_2}) \;=\; q^{n_1 m_2}\; b^{m_1+m_2}a^{n_1+n_2}.$$

Exercise 31 (The Hopf algebra structure of H_q)
Show that there is a unique Hopf algebra structure on H_q *such that the coproducts of* a *and* b *are given by*

$$\Delta(a) \;=\; a \otimes a \qquad \text{and} \qquad \Delta(b) \;=\; a \otimes b + b \otimes 1.$$

Show also that the following formulas hold in this Hopf algebra

$$\Delta(b^m a^n) \;=\; \sum_{k=0}^{m} \left[\!\left[\begin{array}{c} m \\ k \end{array} \right]\!\right]_q b^k a^{m-k+n} \otimes b^{m-k} a^n \tag{4.4}$$

$$\epsilon(b^m a^n) \;=\; \delta_{m,0} \tag{4.5}$$

$$\gamma(b^m a^n) \;=\; (-1)^m\; q^{-m(m+1)/2-nm}\; b^m\, a^{-n-m}. \tag{4.6}$$

We will assume from here on that $q \neq 1$. Then the Hopf algebra H_q is clearly neither commutative nor cocommutative. In fact, H_q also serves as an example of a Hopf algebra where the antipode is not involutive: we have for example

$$\gamma(\gamma(b)) \;=\; -q^{-1}\,\gamma(ba^{-1}) \;=\; q^{-1}\, b \;\neq\; b.$$

About the restricted dual of H_q

Let us now consider the restricted dual H_q°. By Corollary 3.50, it is spanned by the representative forms of finite dimensional H_q-modules, so let us start concretely from low-dimensional modules. In particular, Exercise 24 tells us that one-dimensional representations of H_q correspond precisely to grouplike elements of H_q°.

One-dimensional representations of H_q

Suppose $V = \mathbb{C}\, v$ is a one-dimensional H_q module with basis vector v. We have

$$a.v \;=\; z\, v$$

for some complex number z, which must be non-zero since $a \in H_q$ is invertible. Note that

$$a.(b.v) \;=\; q\, b.(a.v) \;=\; qz\, b.v, \tag{4.7}$$

which means that $b.v$ is an eigenvector of a with a different eigenvalue, $qz \neq z$. Eigenvectors corresponding to different eigenvalues would be linearly independent, so in the one dimensional module we must have $b.v = 0$. It is now straighforward to compute the action of $b^m a^n$,

$$b^m a^n.v \;=\; \delta_{m,0}\, z^n\, v,$$

from which we can read the only representative form $\lambda_{1,1} \in H_q^\circ$ in this case. We define $g_z \in H_q^\circ$ as that representative form

$$\langle g_z, b^m a^n\rangle \;=\; \delta_{m,0}\, z^n.$$

By Exercise 24, the one-dimensional representations correspond to grouplike elements of H_q°, and indeed it is easy to verify by direct computation or as a special case of Equation (3.9) that

$$\mu^*(g_z) \;=\; g_z \otimes g_z.$$

To compute the products of two elements of this type, we use Equation (4.4):

$$\begin{aligned}\langle \Delta^*(g_z \otimes g_w), b^m a^n\rangle \;&=\langle g_z \otimes g_w, \Delta(b^m a^n)\rangle \;=\; \sum_{k=0}^{m} \left[\!\!\left[\begin{matrix} m \\ k \end{matrix} \right]\!\!\right]_q \langle g_z, b^k a^{m-k+n}\rangle\, \langle g_w, b^{m-k} a^n\rangle \\ &= \sum_{k=0}^{m} \left[\!\!\left[\begin{matrix} m \\ k \end{matrix} \right]\!\!\right]_q \delta_{k,0}\, \delta_{m-k,0}\, z^{m-k+n}\, w^n \;=\; \delta_{m,0}\, (zw)^n \;=\; \langle g_{zw}, b^m a^n\rangle,\end{aligned}$$

that is, the product in H_q° of these elements reads

$$\Delta^*(g_z \otimes g_w) \;=\; g_{zw}.$$

We see that the linear span of $(g_z)_{z\in\mathbb{C}\setminus\{0\}}$ in H_q° is isomorphic to the group algebra of the multiplicative group of non-zero complex numbers $\mathbb{C}[\mathbb{C} \setminus \{0\}]$.

We also remark that there is the trivial one-dimensional representation, explicitly determined by Equation (4.5),

$$b^m a^n.v \;=\; \epsilon(b^m a^n)\, v \;=\; \delta_{m,0}\, v \;=\; \langle g_1, b^m a^n\rangle\, v,$$

and the corresponding grouplike element of the restricted dual is the unit of the restricted dual Hopf algebra, $1_{H_q^\circ} = \epsilon^*(1) = g_1$.

Two-dimensional representations of H_q

Let V be a two-dimensional H_q-module, and choose a basis v_1, v_2 in which a is in Jordan canonical form. Let $z_1, z_2 \in \mathbb{C} \setminus \{0\}$ be the (different or equal) eigenvalues of a. Recall that if v is an eigenvector of a of eigenvalue z, then either $b.v = 0$ or $b.v$ is a nonzero eigenvector of a with eigenvalue qz, as we saw in Equation (4.7). We continue to assume $q \neq 0$ and $q \neq 1$, but let us also assume that $q \neq -1$, so that b has to annihilate at least one eigenvector of a and let us without loss of generality suppose that

$$a.v_1 = z_1\, v_1 \qquad \text{and} \qquad b.v_1 = 0.$$

There are a few possible cases. Either a is diagonalizable or there is a size two Jordan block of a (in the latter case the eigenvalues of a must coincide), and either $b.v_2 = 0$ or $b.v_2$ is a nonzero multiple of v_1 (in which case we must have $z_1 = qz_2 \neq z_2$ by the above argument).

Consider first the case when a is diagonalizable and $b.v_2 = 0$. Then $a.v_2 = z_2\, v_2$ and we easily compute

$$b^m a^n.v_1 = \delta_{m,0}\, z_1^n\, v_1 \qquad \text{and} \qquad b^m a^n.v_2 = \delta_{m,0}\, z_2^n\, v_2.$$

We read that the representative forms are of the same type as before,

$$\lambda_{1,1} = g_{z_1}, \qquad \lambda_{2,1} = 0, \qquad \lambda_{1,2} = 0, \qquad \lambda_{2,2} = g_{z_2}.$$

Consider then the case when a is not diagonalizable. We may assume a normalization of the basis vectors such that $a.v_1 = z_1\, v_1$ and $a.v_2 = z_1\, v_2 + v_1$. We observe that

$$\begin{aligned}(a - z_1)^2.v_2 &= 0 \qquad \text{and therefore}\\ (a - qz_1)^2 b.v_2 &= b(qa - qz_1)^2.v_2 \;=\; q^2\, b(a - z_1)^2.v_2 \;=\; 0.\end{aligned}$$

Thus $b.v_2$ would have a generalized eigenvalue qz_1, which is impossible, so we must have $b.v_2 = 0$, too. It is now easy to compute the action of the whole algebra on the module,

$$b^m a^n.v_1 = \delta_{m,0}\, z_1^n\, v_1 \qquad \text{and} \qquad b^m a^n.v_2 = \delta_{m,0}\left(z_1^n\, v_2 + n\, z_1^{n-1}\, v_1\right).$$

Here we find one new representative form: define $g'_z \in H_q^\circ$, for $z \in \mathbb{C} \setminus \{0\}$, by

$$\langle g'_z, b^m a^n \rangle = \delta_{m,0}\, n\, z^{n-1}.$$

Then the representative forms are

$$\lambda_{1,1} = g_{z_1}, \qquad \lambda_{2,1} = 0, \qquad \lambda_{1,2} = g'_{z_1}, \qquad \lambda_{2,2} = g_{z_1}.$$

The coproduct in H_q° of the newly found element can be read from Equation (3.9), with the result

$$\mu^*(g'_z) = g_z \otimes g'_z + g'_z \otimes g_z.$$

This could of course also be verified by the following direct calculation

$$\begin{aligned}\langle \mu^*(g'_z), b^{m_1}a^{n_1} \otimes b^{m_2}a^{n_2} \rangle &= \langle g'_z, b^{m_1}a^{n_1} b^{m_2}a^{n_2} \rangle \;=\; q^{n_1 m_2}\, \langle g'_z, b^{m_1+m_2} a^{n_1+n_2} \rangle\\ &= q^{n_1 m_2}\, \delta_{m_1+m_2,0}\, (n_1 + n_2)\, z^{n_1+n_2-1}\\ &= q^0\, \delta_{m_1,0}\, \delta_{m_2,0} \left(n_1\, z^{n_1-1}\, z^{n_2} + z^{n_1}\, n_2\, z^{n_2-1}\right)\\ &= \langle g'_z \otimes g_z + g_z \otimes g'_z, b^{m_1}a^{n_1} \otimes b^{m_2}a^{n_2} \rangle.\end{aligned}$$

Consider finally the case when a is diagonalizable and $b.v_2$ is a nonzero multiple of v_1. This requires $z_1 = qz_2$, and we may assume a normalization of the basis vectors such that

$$a.v_1 = qz_2\, v_1, \qquad a.v_2 = z_2\, v_2, \qquad b.v_1 = 0, \qquad b.v_2 = v_1.$$

We then have

$$b^m a^n.v_1 = \delta_{m,0}\, (qz_2)^n\, v_1 \qquad \text{and} \qquad b^m a^n.v_2 = \delta_{m,0}\, z_2^n\, v_2 + \delta_{m,1}\, z_2^n\, v_1,$$

so we find one new representative form again. Defining $h_z^{(1)} \in H_q^\circ$, for $z \in \mathbb{C} \setminus \{0\}$, by

$$\langle h_z^{(1)}, b^m a^n \rangle = \delta_{m,1}\, z^n,$$

the representative forms in this case read

$$\lambda_{1,1} = g_{qz_2}, \qquad \lambda_{2,1} = 0, \qquad \lambda_{1,2} = h^{(1)}_{z_2}, \qquad \lambda_{2,2} = g_{z_2}.$$

From Equation (3.9) we get the coproduct

$$\mu^*(h^{(1)}_z) \;=\; g_{qz} \otimes h^{(1)}_z + h^{(1)}_z \otimes g_z. \tag{4.8}$$

Since H°_q is also a Hopf algebra, we would want to know also products of the newly found elements. We will only make explicit the subalgebra generated by $h^{(1)}_z$, leaving it as an exercise to compute the products for elements g'_z. It will turn out useful to define for any $k \in \mathbb{N}$ and $z \in \mathbb{C} \setminus \{0\}$ the elements $h^{(k)}_z$ of the dual by

$$\langle h^{(k)}_z, b^m a^n \rangle \;=\; \delta_{m,k}\, z^n,$$

of which we have considered the special cases $h^{(1)}_z$ and $h^{(0)}_z = g_z$. The products are calculated as follows, using Equation (4.4),

$$\begin{aligned}
\langle \Delta^*(h^{(k)}_z \otimes h^{(l)}_w), b^m a^n \rangle \;&=\; \langle h^{(k)}_z \otimes h^{(l)}_w, \Delta(b^m a^n)\rangle \;=\; \sum_{j=0}^{m} \left[\!\!\left[\begin{matrix} m \\ j \end{matrix} \right]\!\!\right]_q \langle h^{(k)}_z, b^j a^{m-j+n}\rangle\, \langle h^{(l)}_w, b^{m-j} a^n\rangle \\
&= \sum_{j=0}^{m} \left[\!\!\left[\begin{matrix} m \\ j \end{matrix} \right]\!\!\right]_q \delta_{j,k}\, z^{m-j+n}\, \delta_{m-j,l}\, w^n \;=\; \left[\!\!\left[\begin{matrix} k+l \\ k \end{matrix} \right]\!\!\right]_q z^{l+n}\, w^n\, \delta_{m,k+l} \\
&= z^l \left[\!\!\left[\begin{matrix} k+l \\ k \end{matrix} \right]\!\!\right]_q \langle h^{(k+l)}_{zw}, b^m a^n\rangle,
\end{aligned}$$

with the result

$$h^{(k)}_z\, h^{(l)}_w \;=\; z^l \left[\!\!\left[\begin{matrix} k+l \\ k \end{matrix} \right]\!\!\right]_q h^{(k+l)}_{zw}. \tag{4.9}$$

The restricted dual of H_q contains a copy of H_q

Having done the calculations with one and two dimensional H_q-modules, we are ready to show that the Hopf algebra H°_q contains a copy of H_q when q is not a root of unity.

Lemma 4.1
Let $q \in \mathbb{C} \setminus \{0\}$ be such that $q^N \neq 1$ for all $N \in \mathbb{Z} \setminus \{0\}$. Then the algebra H_q can be embedded to its restricted dual by the linear map such that $b^m a^n \mapsto \tilde{b}^m \tilde{a}^n$, where

$$\tilde{a} \;=\; g_q \qquad \text{and} \qquad \tilde{b} \;=\; h^{(1)}_1.$$

This embedding is an injective homomorphism of Hopf algebras.

Proof. First, $\tilde{a}$ is grouplike and thus invertible. Second, one sees from Equation (4.9) that

$$\tilde{a}\tilde{b} \;=\; q\, h^{(1)}_q \;=\; q\, \tilde{b}\tilde{a},$$

which shows that the needed relations are satisfied, and the given embedding is an algebra homomorphism. Denote by $\tilde{1} = \epsilon^*(1) = g_1$ the unit of the restricted dual Hopf algebra. From Equation (4.8) we also read that

$$\mu^*(\tilde{b}) \;=\; \tilde{a} \otimes \tilde{b} + \tilde{b} \otimes \tilde{1},$$

and by the computations in Exercise 31 the values of the coproduct μ^*, the counit η^* and the antipode γ^* on the elements $\tilde{b}^m \tilde{a}^n$ are uniquely determined by these conditions. Finally, the images of the basis elements $b^m a^n$ can be computed using Equation (4.9) with the result

$$\tilde{b}^m \tilde{a}^n \;=\; [\![m]\!]_q!\, h^{(m)}_{q^n}.$$

These are non-zero and linearly independent elements of the dual when q is not a root of unity, so the embedding is indeed injective. □

4.2 Braided bialgebras and braided Hopf algebras

In this section we discuss the braiding structure that is characteristic of quantum groups in addition to just Hopf algebra structure.

Recall that if A is a bialgebra, then we're able to equip tensor products of A-modules with an A-module structure, and the one dimensional vector space $\mathbb{C}$ with a trivial module structure. The coalgebra axioms guarantee in addition that the canonical vector space isomorphisms

$$(V_1 \otimes V_2) \otimes V_3 \;\cong\; V_1 \otimes (V_2 \otimes V_3)$$

and

$$V \otimes \mathbb{C} \;\cong\; V \;\cong\; \mathbb{C} \otimes V$$

become isomorphisms of A-modules. If A is cocommutative, $\Delta^{\mathrm{op}} = \Delta$, and if V and W are A-modules, then also the tensor flip

$$S_{V,W} : V \otimes W \to W \otimes V$$

becomes an isomorphism of A-modules. The property "braided" is a generalization of "cocommutative": we will not require equality of the coproduct and opposite coproduct, but only ask the two to be related by conjugation, and we will be able to keep weakened forms of some of the good properties of cocommutative bialgebras — in particular we obtain natural A-module isomorphisms

$$c_{V,W} : V \otimes W \to W \otimes V$$

that "braid" the tensor components.

The braid groups

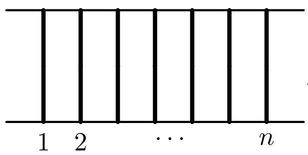
Let us start by discussing what braiding usually means.

Definition 4.2. For n a positive integer, the braid group on n strands is the group B_n with generators $\sigma_1, \sigma_2 \ldots, \sigma_{n-1}$ and relations

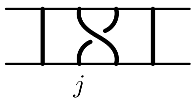
$$\sigma_j \, \sigma_{j+1} \, \sigma_j \; = \sigma_{j+1} \, \sigma_j \, \sigma_{j+1} \qquad \text{for } 1 \leq j < n \qquad (4.10)$$

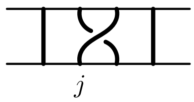
$$\sigma_j \, \sigma_k \; = \sigma_k \, \sigma_j \qquad \text{for } |j - k| > 1. \qquad (4.11)$$

To see why this is called braiding, we visualize the elements as operations on n vertical strands, which we draw next to each other from bottom to top



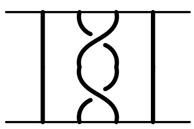
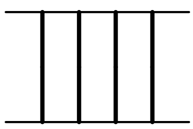
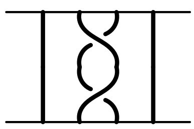
The operations are continuation of the strands from the top, the generators and their inverses being visualized as follows

σ_j = 

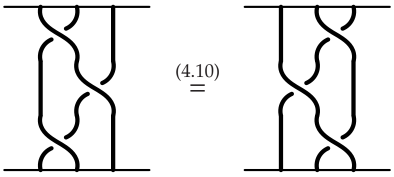
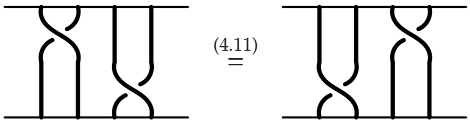
and σ_j^{-1} = 

.

Having visualized the generators in this way, the equations $\sigma_j^{-1} \, \sigma_j = e = \sigma_j \, \sigma_j^{-1}$ tell us to identify the following kinds of pictures

 =  =  .

The braid group relations tell us to identify pictures for example as shown below


and


Remark 4.3. In the symmetric group S_n, the transpositions of consequtive elements satisfy the relations (4.10) and (4.11). Such transpositions generate S_n, so there exists a surjective group homomorphism $B_n \to S_n$ such that $\sigma_j \mapsto (j\ \ j+1)$. In other words, the symmetric group is isomorphic to a quotient of the braid group. In this quotient one only keeps track of the endpoints of the strands (permutation), forgetting about their possible entanglement (braid). The kernel of this group homomorphism is a normal subgroup of B_n called the pure braid group: its elements do not permute the order of the strands from bottom to top, but the strands can be entangled with each other.

The Yang-Baxter equation

A collection of complex numbers $(r^{k,l}_{i,j})_{i,j,k,l \in \{1,2,\ldots,d\}}$ is said to satisfy the Yang-Baxter equation if

$$\sum_{a,b,c=1}^{d} r^{l,m}_{a,b}\, r^{b,n}_{c,k}\, r^{a,c}_{i,j} \;=\; \sum_{a,b,c=1}^{d} r^{m,n}_{a,b}\, r^{l,a}_{i,c}\, r^{c,b}_{j,k} \qquad \text{for all } i,j,k,l,m,n \in \{1,2,\ldots,d\}\,. \tag{4.12}$$

Observe that there are d^6 equations imposed on d^4 complex numbers.
Let V be a vector space with basis $(v_i)_{i=1}^d$ and define

$$\check{R} : V \otimes V \to V \otimes V \qquad \text{by} \qquad \check{R}(v_i \otimes v_j) \;=\; \sum_{k,l=1}^{d} r^{k,l}_{i,j}\, v_k \otimes v_l.$$

Then the Yang-Baxter equation is equivalent with

$$\check{R}_{12} \circ \check{R}_{23} \circ \check{R}_{12} \;=\; \check{R}_{23} \circ \check{R}_{12} \circ \check{R}_{23}, \tag{YBE}$$

where $\check{R}_{12}, \check{R}_{23} : V \otimes V \otimes V \to V \otimes V \otimes V$ are defined as $\check{R}_{12} = \check{R} \otimes \mathrm{id}_V$ and $\check{R}_{23} = \mathrm{id}_V \otimes \check{R}$. This equation has obvious resemblance with the braid group relation (4.10).

Example 4.4. If we set $\check{R}(v_i \otimes v_j) = v_i \otimes v_j$ for all $i, j \in \{1,2,\ldots,d\}$, that is $r^{k,l}_{i,j} = \delta_{i,k}\delta_{j,l}$ and $\check{R} = \mathrm{id}_{V\otimes V}$, then $\check{R}$ satisfies the Yang-Baxter equation since both sides of Equation (YBE) become $\mathrm{id}_{V\otimes V\otimes V}$.

Example 4.5. If we set $\check{R}(v_i \otimes v_j) = v_j \otimes v_i$ for all $i, j \in \{1,2,\ldots,d\}$, that is $r^{k,l}_{i,j} = \delta_{i,l}\delta_{j,k}$ and $\check{R} = S_{V,V}$, then $\check{R}$ satisfies the Yang-Baxter equation, as is verified by the following calculation on simple tensors

$$\begin{array}{lllllll} v_i \otimes v_j \otimes v_k & \overset{S_{V,V}\otimes \mathrm{id}_V}{\mapsto} & v_j \otimes v_i \otimes v_k & \overset{\mathrm{id}_V \otimes S_{V,V}}{\mapsto} & v_j \otimes v_k \otimes v_i & \overset{S_{V,V}\otimes \mathrm{id}_V}{\mapsto} & v_k \otimes v_j \otimes v_i \\ v_i \otimes v_j \otimes v_k & \overset{\mathrm{id}_V \otimes S_{V,V}}{\mapsto} & v_i \otimes v_k \otimes v_j & \overset{S_{V,V}\otimes \mathrm{id}_V}{\mapsto} & v_k \otimes v_i \otimes v_j & \overset{\mathrm{id}_V \otimes S_{V,V}}{\mapsto} & v_k \otimes v_j \otimes v_i. \end{array}$$

Exercise 32 (A solution to the Yang-Baxter equation)
Let V be a vector space with basis $v_1, v_2, \ldots, v_d$ and let $q \in \mathbb{C} \setminus \{0\}$. Define a linear map

$$\check{R} : V \otimes V \to V \otimes V \qquad \textit{by} \qquad \check{R}(v_i \otimes v_j) \;=\; \begin{cases} q\, v_i \otimes v_j & \textit{if } i = j \\ v_j \otimes v_i & \textit{if } i < j \\ v_j \otimes v_i + \left(q - q^{-1}\right) v_i \otimes v_j & \textit{if } i > j \end{cases}.$$

(a) Verify that we have the following equality of linear maps $V \otimes V \otimes V \to V \otimes V \otimes V$

$$\check{R}_{12} \circ \check{R}_{23} \circ \check{R}_{12} \;=\; \check{R}_{23} \circ \check{R}_{12} \circ \check{R}_{23}. \tag{YBE}$$

(b) Verify also that

$$(\check{R} - q\, \mathrm{id}_{V\otimes V}) \circ (\check{R} + q^{-1}\, \mathrm{id}_{V\otimes V}) \;=\; 0.$$

The notations $\check{R}_{12} = \check{R} \otimes \mathrm{id}_V$ and $\check{R}_{23} = \mathrm{id}_V \otimes \check{R}$ are a special case of acting on chosen tensor components. More generally, if $T : V \otimes V \to V \otimes V$ is a linear map, then on

$$V^{\otimes n} \;=\; \underbrace{V \otimes V \otimes \cdots \otimes V}_{n \text{ times}}$$

we define T_{ij}, $1 \le i, j \le n$, $i \ne j$, as the linear map that acts as T on the i^{th} and j^{th} tensor components and as identity on the rest. Explicitly, if

$$T(v_k \otimes v_{k'}) \;=\; \sum_{l,l'=1}^{d} t^{l,l'}_{k,k'}\, v_l \otimes v_{l'},$$

then (assuming $i < j$ for definiteness)

$$T_{ij}(v_{k_1} \otimes \cdots \otimes v_{k_n}) \;=\; \sum_{l,l'=1}^{d} t^{l,l'}_{k_i,k_j}\, v_{k_1} \otimes \cdots \otimes v_{k_{i-1}} \otimes v_l \otimes v_{k_{i+1}} \otimes \cdots \otimes v_{k_{j-1}} \otimes v_{l'} \otimes v_{k_{j+1}} \otimes \cdots \otimes v_{k_n}.$$

Exercise 33 (Two ways of writing the Yang-Baxter equation)
Let V be a vector space, and let R and $\check{R}$ be linear maps $V \otimes V \to V \otimes V$ related by

$$\check{R} \;=\; S_{V,V} \circ R.$$

Show that the following equalities of linear maps $V \otimes V \otimes V \to V \otimes V \otimes V$ are equivalent

$$\text{(i)} \qquad \check{R}_{12} \circ \check{R}_{23} \circ \check{R}_{12} = \check{R}_{23} \circ \check{R}_{12} \circ \check{R}_{23}$$
$$\text{(ii)} \qquad R_{12} \circ R_{13} \circ R_{23} = R_{23} \circ R_{13} \circ R_{12}. \tag{YBE$'$}$$

Note that here we could have taken the following as definitions

$$\begin{aligned} R_{12} &= R \otimes \mathrm{id}_V \\ R_{23} &= \mathrm{id}_V \otimes R \\ R_{13} &= (\mathrm{id}_V \otimes S_{V,V}) \circ (R \otimes \mathrm{id}_V) \circ (\mathrm{id}_V \otimes S_{V,V}). \end{aligned}$$

Proposition 4.6
If $\check{R} : V \otimes V \to V \otimes V$ is bijective and satisfies the Yang-Baxter equation (YBE), then on $V^{\otimes n}$ there is a representation $\rho : B_n \to \mathrm{Aut}(V^{\otimes n})$ of the braid group B_n, such that $\rho(\sigma_j) = \check{R}_{j\,j+1}$ for all $j = 1, 2, \ldots, n-1$.

Proof. First, if $\check{R}$ is bijective, then clearly $\check{R}_{j\,j+1} \in \mathrm{Aut}(V^{\otimes n})$ for all j. To show existence of a group homomorphism ρ with the given values on the generators σ_j, we need to verify the relations (4.10) and (4.11) for the images $\check{R}_{j\,j+1}$. The first relation follows from the Yang-Baxter equation (YBE), and the second is obvious since when $|j - k| > 1$, the matrix $\check{R}_{j\,j+1}$ acts as identity on the tensor components k and $k+1$, and vice versa. □

Universal R-matrix and braided bialgebras

The universal R-matrix is an algebra element, which in representations becomes a solution to the Yang-Baxter equation. Let A be an algebra (in what follows always in fact a bialgebra or a Hopf algebra), and equip $A \otimes A$ and $A \otimes A \otimes A$ as usually with the algebra structures given by componentwise products, for example $(a \otimes a')\,(b \otimes b') = ab \otimes a'b'$ for all $a, a', b, b' \in A$. Suppose that we have an element $R \in A \otimes A$, which we write as a sum of elementary tensors

$$R = \sum_{i=1}^{r} s_i \otimes t_i,$$

with some $s_i, t_i \in A$, $i = 1, 2, \ldots, r$. Then we use the notations

$$R_{12} = \sum_i s_i \otimes t_i \otimes 1_A \qquad R_{13} = \sum_i s_i \otimes 1_A \otimes t_i \qquad R_{23} = \sum_i 1_A \otimes s_i \otimes t_i.$$

Definition 4.7. Let A be a bialgebra (or a Hopf algebra). An element $R \in A \otimes A$ is called a universal R-matrix for A if

(R0) R is invertible in the algebra $A \otimes A$

(R1) for all $x \in A$ we have $\Delta^{\mathrm{op}}(x) = R\,\Delta(x)\,R^{-1}$

(R2) $(\Delta \otimes \mathrm{id}_A)(R) = R_{13}\,R_{23}$

(R3) $(\mathrm{id}_A \otimes \Delta)(R) = R_{13}\,R_{12}$.

A pair (A, R) as above is called a braided bialgebra (or braided Hopf algebra, if A is a Hopf algebra).

Instead of the terms "braided bialgebra" or "braided Hopf algebra", Drinfeld originally used the terms "quasitriangular bialgebra" and "quasitriangular Hopf algebra". That is why one occasionally encounters these terms in the literature.

Example 4.8. If A is a commutative bialgebra, $\Delta = \Delta^{\mathrm{op}}$, then $R = 1_A \otimes 1_A$ is a universal R-matrix. Thus braided bialgebras generalize cocommutative bialgebras.

Exercise 34 (Coproducts commute with a full twist)
Show that $R_{21}\,R\,\Delta(x) = \Delta(x)\,R_{21}\,R$ *for all* $x \in A$.

Exercise 35 (A universal R-matrix for the Hopf algebra of cyclic group)
Let $A = \mathbb{C}[\mathbb{Z}/N\mathbb{Z}]$ *be the group algebra of the cyclic group of order* N*, generated by one element* θ *such that* $\theta^N = 1_A$*. Denote also* $\omega = \exp(2\pi \mathrm{i}/N)$*. Show that the element*

$$R = \frac{1}{N} \sum_{k,l=0}^{N-1} \omega^{kl}\, \theta^k \otimes \theta^l$$

is a universal R-matrix for A*.*
Hint: *To find the inverse element, Exercise 37 may help.*

Exercise 36 (Another universal R-matrix)
Show that if R *is a universal R-matrix for a bialgebra* A*, then* $R_{21}^{-1} = S_{A,A}(R^{-1})$ *is also a universal R-matrix for* A*.*

A few properties of braided bialgebras are listed in the following.

Proposition 4.9
Let (A, R) be a braided bialgebra. Then we have

- $(\epsilon \otimes \mathrm{id}_A)(R) = 1_A$ *and* $(\mathrm{id}_A \otimes \epsilon)(R) = 1_A$
- $R_{12}\, R_{13}\, R_{23} \;=\; R_{23}\, R_{13}\, R_{12}$.

Proof. To prove the second property, write

$$\begin{aligned} R_{12}\, R_{13}\, R_{23} &\overset{(R2)}{=} R_{12}\, (\Delta \otimes \mathrm{id}_A)(R) \overset{(R1)}{=} (\Delta^{\mathrm{op}} \otimes \mathrm{id}_A)(R)\, R_{12} \\ &= \Big((S_{A,A} \otimes \mathrm{id}_A) \circ (\Delta \otimes \mathrm{id}_A)(R)\Big) R_{12} \overset{(R2)}{=} \Big((S_{A,A} \otimes \mathrm{id}_A)(R_{13} R_{23})\Big) R_{12} \\ &= R_{23}\, R_{13}\, R_{12}. \end{aligned}$$

To prove the first formula of the first property, we use two different ways to rewrite the expression

$$(\epsilon \otimes \mathrm{id}_A \otimes \mathrm{id}_A) \circ (\Delta \otimes \mathrm{id}_A)(R). \tag{4.13}$$

On the one hand, we could simply use $(\epsilon \otimes \mathrm{id}) \circ \Delta = \mathrm{id}$ to write (4.13) as R. On the other hand, if we denote $r = (\epsilon \otimes \mathrm{id}_B)(R) \in A$ and use property (R2) of R-matrices, we get

$$(4.13) \overset{(R2)}{=} (\epsilon \otimes \mathrm{id}_A \otimes \mathrm{id}_A)(R_{13} R_{23}) \;=\; (1_A \otimes r)\, R.$$

The equality of the two simplified expressions, $R = (1_A \otimes r)R$, implies $1_A \otimes r = 1_A \otimes 1_A$ since R is invertible, and therefore we get $r = 1_A$ as claimed.

The case of $(\mathrm{id}_A \otimes \epsilon)(R)$ is handled similarly by considering the expression $(\mathrm{id} \otimes \mathrm{id} \otimes \epsilon) \circ (\mathrm{id} \otimes \Delta)(R)$ instead of (4.13). □

The promised braiding isomorphism of tensor product representations in two different orders goes as follows. Let A be a braided bialgebra (or braided Hopf algebra) with universal R-matrix $R \in A \otimes A$, and suppose that V and W are two A-modules, with $\rho_V : A \to \mathrm{End}(V)$ and $\rho_W : A \to \mathrm{End}(W)$ the respective representations. Recall that the vector spaces $V \otimes W$ and $W \otimes V$ are equipped with the representations of A given by $\rho_{V \otimes W} = (\rho_V \otimes \rho_W) \circ \Delta$ and $\rho_{W \otimes V} = (\rho_W \otimes \rho_V) \circ \Delta$.

Proposition 4.10
Let A be a braided bialgebra with universal R-matrix $R \in A \otimes A$. The linear map $c_{V,W} : V \otimes W \to W \otimes V$ defined by

$$c_{V,W} \;=\; S_{V,W} \circ \Big((\rho_V \otimes \rho_W)(R)\Big)$$

is an isomorphism of A-modules. The collection $(c_{V,W})_{V,W\ A\text{-modules}}$ of isomorphisms of A-modules is natural in the sense that if $f : V \to V'$ and $g : W \to W'$ are A-module maps, then we have

$$c_{V',W'} \circ (f \otimes g) \;=\; (g \otimes f) \circ c_{V,W} \qquad \text{as maps } V \otimes W \to W' \otimes V'.$$

Proof. The map $(\rho_V \otimes \rho_W)(R) : V \otimes W \to V \otimes W$ is bijective, with inverse $(\rho_V \otimes \rho_W)(R^{-1})$. Since $S_{V,W} : V \otimes W \to W \otimes V$ is obviously also bijective, the map $c_{V,W}$ is indeed a bijective linear map. We must only show that it respects the A-module structures. Let $x \in A$ and compute

$$\begin{aligned} c_{V,W} \circ \rho_{V \otimes W}(x) &= S_{V,W} \circ \Big((\rho_V \otimes \rho_W)(R)\Big) \circ \Big((\rho_V \otimes \rho_W)(\Delta(x))\Big) \\ &= S_{V,W} \circ \Big((\rho_V \otimes \rho_W)(R\Delta(x))\Big) \\ &\overset{(R1)}{=} S_{V,W} \circ \Big((\rho_V \otimes \rho_W)(\Delta^{\mathrm{op}}(x)R)\Big) \\ &= S_{V,W} \circ \Big((\rho_V \otimes \rho_W)(\Delta^{\mathrm{op}}(x))\Big) \circ \Big((\rho_V \otimes \rho_W)(R)\Big) \\ &= \Big((\rho_W \otimes \rho_V)(\Delta(x))\Big) \circ S_{V,W} \circ \Big((\rho_V \otimes \rho_W)(R)\Big) \\ &= \rho_{W \otimes V}(x) \circ c_{V,W}. \end{aligned}$$

This shows that the action by x in the different modules is preserved by $c_{V,W}$.

The naturality follows from an obvious calculation, which just uses the A-linearity of $f : V \to V'$ and $g : W \to W'$. Write the universal R-matrix as $R = \sum_i s_i \otimes t_i \in A \otimes A$. Let $v \in V$ and $w \in W$, and calculate

$$\begin{aligned}
\big(c_{V',W'} \circ (f \otimes g)\big)(v \otimes w) &= c_{V',W'}\big((f(v) \otimes g(w)\big) \\
&= S_{V',W'}\Big(\sum_i s_i.f(v) \otimes t_i.g(w)\Big) = S_{V',W'}\Big(\sum_i f(s_i.v) \otimes g(t_i.w)\Big) \\
&= \big(S_{V',W'} \circ (f \otimes g)\big)\Big(\sum_i (s_i.v) \otimes (t_i.w)\Big) = \big((g \otimes f) \circ S_{V,W}\big)\Big(\sum_i (s_i.v) \otimes (t_i.w)\Big) \\
&= \big((g \otimes f) \circ c_{V,W}\big)(v \otimes w).
\end{aligned}$$

□

We next show that braiding with the trivial representation does nothing, and that the braiding respects tensor products: one can braid the the components of a tensor product one at a time in the following sense.

Lemma 4.11
Let U, V, W be three representations of a braided bialgebra A. Then we have

(i)	$c_{\mathbb{C}\otimes V} = \mathrm{id}_V$ *and* $c_{V\otimes\mathbb{C}} = \mathrm{id}_V$	*as maps* $V \to V$
(ii)	$c_{U\otimes V,W} = (c_{U,W} \otimes \mathrm{id}_V) \circ (\mathrm{id}_U \otimes c_{V,W})$	*as a map* $U \otimes V \otimes W \to W \otimes U \otimes V$
(iii)	$c_{U,V\otimes W} = (\mathrm{id}_V \otimes c_{U,W}) \circ (c_{U,V} \otimes \mathrm{id}_W)$	*as a map* $U \otimes V \otimes W \to V \otimes W \otimes U.$

Proof. The claims in (i) are of course with identifications $\mathbb{C} \otimes V \cong V$ and $V \otimes \mathbb{C} \cong V$. With the universal R-matrix written as $R = \sum_i s_i \otimes t_i \in A \otimes A$, and with $v \in V$ we calculate for example

$$c_{\mathbb{C}\otimes V}(1 \otimes v) = S_{\mathbb{C},V}\Big(\sum_i (s_i.1) \otimes (t_i.v)\Big) = S_{\mathbb{C},V}\Big(\sum_i \epsilon(s_i) \otimes (t_i.v)\Big)$$

With the identification $\mathbb{C} \otimes V \cong V$ the last expression is

$$\sum_i \epsilon(s_i)\; t_i.v.$$

Using the first part of Proposition 4.9, this is finally just $1_A.v$, that is v. The other claim in (i) is similar.

Assertions (ii) and (iii) are direct consequences of the axioms (R2) and (R3), respectively. Consider for example the assertion (iii). Let $u \in U$, $v \in V$, $w \in W$. We have

$$\begin{aligned}
c_{U,V\otimes W}(u \otimes v \otimes w) &= S_{U,V\otimes W}\Big(\sum_i \big(s_i.u\big) \otimes \big(t_i.(v \otimes w)\big)\Big) \\
&= \sum_i \big(t_i.(v \otimes w)\big) \otimes \big(s_i.u\big) \\
&= \sum_i \Big(\sum_{(t_i)} ((t_i)_{(1)}.v \otimes (t_i)_{(2)}.w)\Big) \otimes \big(s_i.u\big)
\end{aligned}$$

Recall property (R3), which we write in the following form

$$\sum_i \sum_{(t_i)} s_i \otimes (t_i)_{(1)} \otimes (t_i)_{(2)} = (\mathrm{id}_A \otimes \Delta)(R) \overset{(R3)}{=} R_{13}\, R_{12} = \sum_{j,k} s_j s_k \otimes t_k \otimes t_j.$$

With this formula we continue the calculation of the braiding of U with $V \otimes W$, and we get

$$\begin{aligned} c_{U,V\otimes W}(u \otimes v \otimes w) &= \sum_{j,k} (t_k.v) \otimes (t_j.w) \otimes (s_j s_k.u) \\ &= \sum_k (t_k.v) \otimes \Big(c_{U,W}(s_k.u \otimes w) \Big) \\ &= (\mathrm{id}_V \otimes c_{U,W}) \Big(\sum_k (t_k.v) \otimes (s_k.u) \otimes w \Big) \\ &= \Big((\mathrm{id}_V \otimes c_{U,W}) \circ (c_{U,V} \otimes \mathrm{id}_W) \Big) \Big(v \otimes u \otimes w \Big). \end{aligned}$$

The proof of assertion (ii) is entirely parallel, using the axiom (R2) instead. □

Note that the last property in Proposition 4.9 above is like the Yang-Baxter equation (YBE'), but for algebra elements. When acting on representations, all components need not be the same, so we get a slight generalization of the Yang-Baxter equation.

Proposition 4.12
Let U, V, W be three representations of a braided bialgebra A. Then we have

$$(c_{V,W} \otimes \mathrm{id}_U) \circ (\mathrm{id}_V \otimes c_{U,W}) \circ (c_{U,V} \otimes \mathrm{id}_W) = (\mathrm{id}_W \otimes c_{U,V}) \circ (c_{U,W} \otimes \mathrm{id}_V) \circ (\mathrm{id}_U \otimes c_{V,W})$$

as linear maps

$$U \otimes V \otimes W \to W \otimes V \otimes U.$$

Proof. Just like the above algebra version of the Yang-Baxter equation, this follows from Lemma 4.11. We first reckognize on the left hand side a piece which can be simplified with the property (i) of the lemma. Then we use the naturality of the braiding, with $g = c_{V,W}$ and $f = \mathrm{id}_U$ and finally again the property (i). The calculation thus reads

$$\begin{aligned} (c_{V,W} \otimes \mathrm{id}_U) \circ (\mathrm{id}_V \otimes c_{U,W}) \circ (c_{U,V} \otimes \mathrm{id}_W) &= (c_{V,W} \otimes \mathrm{id}_U) \circ c_{U,V\otimes W} \\ &= c_{U,W\otimes V} \circ (\mathrm{id}_U \otimes c_{V,W}) \\ &= (\mathrm{id}_W \otimes c_{U,V}) \circ (c_{U,W} \otimes \mathrm{id}_V) \circ (\mathrm{id}_U \otimes c_{V,W}). \end{aligned}$$

□

Suppose that $\rho_V : A \to \mathrm{End}(V)$ is a representation of a braided bialgebra A. The vector space $V^{\otimes n}$ is equipped with the representation of A

$$\rho = (\rho_V \otimes \rho_V \otimes \cdots \otimes \rho_V) \circ \Delta^{(n)},$$

where $\Delta^{(n)}$ denotes the $n-1$-fold coproduct, defined (for example) as

$$\Delta^{(n)} = (\Delta \otimes \mathrm{id}_A \otimes \cdots \otimes \mathrm{id}_A) \circ \cdots \circ (\Delta \otimes \mathrm{id}_A) \circ \Delta,$$

although by coassociativity we are allowed to write it in other ways if we wish.

In Proposition 4.12 taking also $U = V$ and $W = V$, we get the Yang-Baxter equation. Combining with Proposition 4.10, we have proved the following.

Theorem 4.13
Let A be a braided bialgebra (or a braided Hopf algebra) with universal R-matrix $R \in A \otimes A$, and let $\rho_V : A \to \mathrm{End}(V)$ be a representation of A in a vector space V. Then the linear map $\check{R} : V \otimes V \to V \otimes V$ given by

$$\check{R} = c_{V,V} = S_{V,V} \circ \Big((\rho_V \otimes \rho_V)(R) \Big)$$

is a solution to the Yang-Baxter equation. Moreover, on the n-fold tensor product space $V^{\otimes n}$, the braid group action defined by $\check{R}$ as in Proposition 4.6 commutes with the action of A.

Braided Hopf algebras

Let $A = (A, \mu, \Delta, \eta, \epsilon, \gamma)$ be a Hopf algebra, and suppose that there exists a universal R-matrix $R \in A \otimes A$, i.e. that A can be made a braided Hopf algebra. We will now investigate some implications that this has on the structure of the Hopf algebra and on the universal R-matrix.

Exercise 37 (Behavior of universal R-matrix under the antipode)
Show that for a braided Hopf algebra A we have

$$(\gamma \otimes \mathrm{id}_A)(R) \;=\; R^{-1} \qquad \text{and} \qquad (\gamma \otimes \gamma)(R) \;=\; R.$$

Hint: *For the first statement, remember Proposition 4.9. For the second, Exercise 36 comes in handy.*

We can now prove a statement analogous to the property that in cocommutative Hopf algebras the square of the antipode is the identity map. Here we obtain that the square of the antipode of a braided Hopf algebra is an inner automorphism.

Theorem 4.14
Let A be a braided Hopf algebra with a universal R-matrix $R = \sum_i s_i \otimes t_i$. Then, for all $x \in A$ we have

$$\gamma(\gamma(x)) \;=\; u\, x\, u^{-1},$$

where $u \in A$ is

$$u \;=\; \mu \circ (\gamma \otimes \mathrm{id}_A) \circ S_{A,A}(R) \;=\; \sum_i \gamma(t_i) s_i.$$

We also have

$$\gamma^{-1}(x) \;=\; u^{-1}\, \gamma(x)\, u.$$

Proof. We will first prove an auxiliary formula, $\sum_{(x)} \gamma(x_{(2)})\, u\, x_{(1)} = \epsilon(x)\, u$ for all $x \in A$. To get this, calculate

$$\begin{aligned}
\sum_{(x)} \gamma(x_{(2)})\, u\, x_{(1)} &= \sum_{(x)} \sum_i \gamma(x_{(2)}) \gamma(t_i) s_i x_{(1)} \;=\; \sum_{(x)} \sum_i \gamma(t_i x_{(2)}) s_i x_{(1)} \\
&= \sum_{(x)} \sum_i \mu \circ (\gamma \otimes \mathrm{id}_A)\big(x_{(2)} t_i \otimes s_i x_{(1)}\big) \\
&= \mu \circ (\gamma \otimes \mathrm{id}_A) \circ S_{A,A}\big(R \Delta(x)\big) \\
&\overset{(R1)}{=} \mu \circ (\gamma \otimes \mathrm{id}_A) \circ S_{A,A}\big(\Delta^{\mathrm{op}}(x) R\big) \\
&= \sum_{(x)} \sum_i \gamma(x_{(1)} t_i) x_{(2)} s_i \;=\; \sum_{(x)} \sum_i \gamma(t_i) \gamma(x_{(1)}) x_{(2)} s_i \\
&\overset{(H3)}{=} \epsilon(x) \sum_i \gamma(t_i)\, 1_A\, s_i \;=\; \epsilon(x)\, u.
\end{aligned}$$

We will then show that $\gamma(\gamma(x))u = ux$. To do this, use the auxiliary formula for the first component

"$x_{(1)}$" of the coproduct of $x \in A$ in the third equality below

$$\begin{aligned}
\gamma(\gamma(x))\,u &\overset{(H2')}{=} \gamma(\gamma(\sum_{(x)} \epsilon(x_{(1)})\,x_{(2)}))\,u \\
&= \sum_{(x)} \gamma(\gamma(x_{(2)}))\,\epsilon(x_{(1)})\,u \\
&\overset{\text{auxiliary}}{=} \sum_{(x)} \gamma(\gamma(x_{(3)}))\,\gamma(x_{(2)})\,u\,x_{(1)} \qquad \text{(note that the sum represents a double coproduct)} \\
&= \sum_{(x)} \gamma(x_{(2)}\gamma(x_{(3)}))\,u\,x_{(1)} \qquad \text{(note that the sum represents a double coproduct)} \\
&\overset{(H3)}{=} \sum_{(x)} \epsilon(x_{(2)})\,\gamma(1_A)\,u\,x_{(1)} \\
&\overset{(H2')}{=} \gamma(1_A)\,u\,x \;=\; u\,x.
\end{aligned}$$

Now to prove the formula $\gamma(\gamma(x)) = uxu^{-1}$ it suffices to show that u is invertible, since then we can multiply the above equation from the right by u^{-1}. We claim that the inverse of u is

$$\tilde{u} \;=\; \mu \circ (\mathrm{id}_A \otimes \gamma^2) \circ S_{A,A}(R) \;=\; \sum_i t_i \gamma^2(s_i).$$

Let us calculate, using the property $\gamma^2(x)u = ux$,

$$\begin{aligned}
\tilde{u}\,u &= \sum_i t_i\,\gamma^2(s_i)\,u \;=\; \sum_i t_i\,u\,s_i \;=\; \sum_{i,j} t_i\,\gamma(t_j)\,s_j\,s_i \\
&\overset{\text{Ex.37}}{=} \sum_{i,j} \gamma(t_i)\,\gamma(t_j)\,s_j\,\gamma(s_i) \;=\; \sum_{i,j} \gamma(t_j t_i)\,s_j\,\gamma(s_i) \\
&= \mu^{\mathrm{op}} \circ (\mathrm{id}_A \otimes \gamma)\Big(\sum_{i,j} s_j \gamma(s_i) \otimes t_j t_i\Big) \\
&\overset{\text{Ex.37}}{=} \mu^{\mathrm{op}} \circ (\mathrm{id}_A \otimes \gamma)\Big(R\,R^{-1}\Big) \;=\; \gamma(1_A)1_A \;=\; 1_A.
\end{aligned}$$

Likewise,

$$u\,\tilde{u} \;=\; \sum_i u\,t_i\,\gamma^2(s_i) \;=\; \sum_i \gamma^2(t_i)\,u\,\gamma^2(s_i),$$

which by Exercise 37 equals $\sum_i t_i\,u\,s_i$, and this expression was already computed above to be 1_A. We leave it as an exercise to derive the last statement from the first. □

Exercise 38 (Linear maps whose square is an inner automorphism)
Suppose that A is an algebra, $u \in A$ is an invertible element, and $G : A \to A$ is a linear map such that

$$G(G(x)) \;=\; u\,x\,u^{-1} \qquad \textit{for all } x \in A.$$

(a) Show that G is bijective.

(b) Show that the inverse of G is given by the formula

$$G^{-1}(x) \;=\; u^{-1}\,G(x)\,u \qquad \textit{for all } x \in A.$$

(c) Finish the proof of Theorem 4.14 by showing that the second statement follows from the first.

In the following two exercises we explore some further properties of the element

$$u \;=\; \mu^{\mathrm{op}} \circ (\mathrm{id}_A \otimes \gamma)(R) \;=\; \sum_i \gamma(t_i) s_i \;\in A,$$

when the antipode γ is invertible.

Exercise 39 (A central element in braided Hopf algebras)
Let A be a braided Hopf algebra such that the antipode $\gamma : A \to A$ has an inverse $\gamma^{-1} : A \to A$. Show that $\gamma(u)u$ is in the center of A, i.e. $\gamma(u)ux = x\gamma(u)u$ for all $x \in A$, and that $\gamma(u)\,u = u\,\gamma(u)$.

In the following exercise it's good to recall also Exercise 34, and in part (b) one in fact needs almost all the properties of the universal R-matrices that we have seen so far. We use the notation

$$R_{21} \;=\; S_{A,A}(R) \;=\; \sum_i t_i \otimes s_i.$$

Exercise 40 (Properties of the element u in braided Hopf algebras)
Let A be a braided Hopf algebra such that the antipode $\gamma : A \to A$ has an inverse $\gamma^{-1} : A \to A$.

(a) Show that $\epsilon(u) = 1$.

(b) Show that $\Delta(u) \;=\; (R_{21}R)^{-1}\,(u \otimes u)$.

(c) Show that $u\,\gamma(u^{-1})$ is grouplike.

4.3 The Drinfeld double construction

There is a systematic way of creating braided Hopf algebras, the Drinfeld double construction.

Let us assume that $A = (A, \mu, \Delta, \eta, \epsilon, \gamma)$ is a Hopf algebra such that γ has an inverse γ^{-1}, and $B \subset A^\circ$ is a sub-Hopf algebra. We denote the unit of A simply by $1 = \eta(1)$, and the unit of A° (and thus also of B) by 1^*. By definition, then, for any $a \in A$ we have $\langle 1^*, a\rangle = \epsilon(a)$. For any $\varphi \in B$ we use the following notation for the coproduct

$$\mu^*(\varphi) \;=\; \sum_{(\varphi)} \varphi_{(1)} \otimes \varphi_{(2)}.$$

Theorem 4.15
Let A and $B \subset A^\circ$ be as above. Then the space $A \otimes B$ admits a unique Hopf algebra structure such that:

(i) The map $\iota_A : A \to A \otimes B$ given by $a \mapsto a \otimes 1^*$ is a homomorphism of Hopf algebras.

(ii) The map $\iota_B : B^{\mathrm{cop}} \to A \otimes B$ given by $\varphi \mapsto 1 \otimes \varphi$ is a homomorphism of Hopf algebras.

(iii) For all $a \in A$, $\varphi \in B$ we have

$$(a \otimes 1^*)\,(1 \otimes \varphi) \;=\; a \otimes \varphi.$$

(iv) For all $a \in A$, $\varphi \in B$ we have

$$(1 \otimes \varphi)\,(a \otimes 1^*) \;=\; \sum_{(a)} \sum_{(\varphi)} \langle \varphi_{(1)}, a_{(3)}\rangle\, \langle \varphi_{(3)}, \gamma^{-1}(a_{(1)})\rangle\, a_{(2)} \otimes \varphi_{(2)}.$$

This Hopf algebra is denoted by $\mathcal{D}(A, B)$ and it is called the Drinfeld double associated to A and B.

Example 4.16. When A is finite dimensional, $A^\circ = A^*$ is a Hopf algebra. It can also be shown that the antipode is always invertible in the finite dimensional case. The Drinfeld double associated to A and A^* is then denoted simply by $\mathcal{D}(A)$.

Example 4.17. When q is not a root of unity, we showed in Lemma 4.1 that the Hopf algebra H_q can be embedded to its restricted dual by a map such that $a \mapsto \tilde{a}$, $b \mapsto \tilde{b}$. In Section 4.4 we will consider in detail the Drinfeld double associated to the Hopf algebra H_q and the sub-Hopf algebra of H_q° which is isomorphic to H_q.

Proof of uniqueness in Theorem 4.15. When one claims that something exists and is uniquely determined by some given properties, it is often convenient to start with a proof of uniqueness, in the course of which one obtains explicit formulas that help proving existence. This is what we will do now. Denote the structural maps of $\mathcal{D}(A, B)$ by $\mu_\mathcal{D}$, $\Delta_\mathcal{D}$, $\eta_\mathcal{D}$, $\epsilon_\mathcal{D}$ and $\gamma_\mathcal{D}$, in order to avoid confusion with the structural maps of A (and of A°).

In order to prove that the product $\mu_\mathcal{D}$ is uniquely determined by the conditions, it suffices to compute its values on simple tensors. So let $a, b \in A$, $\varphi, \psi \in B$ and use the propertiy (iii) to write $(a \otimes \varphi) = (a \otimes 1^*)(1 \otimes \varphi)$ and $(b \otimes \psi) = (b \otimes 1^*)(1 \otimes \psi)$. Then calculate, assuming that $\mu_\mathcal{D}$ is an associative product,

$$\begin{aligned}
(a \otimes \varphi)\,(b \otimes \psi) \;&=\; (a \otimes 1^*)\,(1 \otimes \varphi)\,(b \otimes 1^*)\,(1 \otimes \psi) \\
&\overset{\text{(iv)}}{=} (a \otimes 1^*)\Big(\sum_{(\varphi),(b)} \langle \varphi_{(1)}, b_{(3)}\rangle\,\langle \varphi_{(3)}\;\gamma^{-1}(b_{(1)})\rangle\, b_{(2)} \otimes \varphi_{(2)}\Big)(1 \otimes \psi) \\
&\overset{\text{(iii)}}{=} (a \otimes 1^*)\Big(\sum_{(\varphi),(b)} \langle \varphi_{(1)}, b_{(3)}\rangle\,\langle \varphi_{(3)}, \gamma^{-1}(b_{(1)})\rangle\,(b_{(2)} \otimes 1^*)\,(1 \otimes \varphi_{(2)})\Big)(1 \otimes \psi) \\
&\overset{\text{(i) and (ii)}}{=} \sum_{(\varphi),(b)} \langle \varphi_{(1)}, b_{(3)}\rangle\,\langle \varphi_{(3)}, \gamma^{-1}(b_{(1)})\rangle\,(ab_{(2)} \otimes 1^*)\,(1 \otimes \varphi_{(2)}\psi).
\end{aligned}$$

By (iii) this simplifies to

$$(a \otimes \varphi)\,(b \otimes \psi) \;=\; \sum_{(\varphi),(b)} \langle \varphi_{(1)}, b_{(3)}\rangle\,\langle \varphi_{(3)}, \gamma^{-1}(b_{(1)})\rangle\; ab_{(2)} \otimes \varphi_{(2)}\psi, \tag{4.14}$$

and we see that the product $\mu_\mathcal{D}$ is indeed uniquely determined.

The unit in an associative algebra is always uniquely determined, and it is easy to check with the product formula (4.14) that the unit of the Drinfeld double is

$$1_\mathcal{D} \;=\; \eta_\mathcal{D}(1) \;=\; 1 \otimes 1^*. \tag{4.15}$$

The coproduct has to be a homomorphism of algebras. Thus using (iii): $(a \otimes \varphi) = (a \otimes 1^*)(1 \otimes \varphi) = \iota_A(a)\,\iota_B(\varphi)$, and (i): $\Delta_\mathcal{D}(\iota_A(a)) = \sum_{(a)} \iota_A(a_{(1)}) \otimes \iota_A(a_{(2)})$ and (ii): $\Delta_\mathcal{D}(\iota_B(\varphi)) = \sum_{(\varphi)} \iota_B(\varphi_{(2)}) \otimes \iota_B(\varphi_{(1)})$ we get

$$\Delta_\mathcal{D}(a \otimes \varphi) \;=\; \sum_{(a),(\varphi)} (a_{(1)} \otimes \varphi_{(2)}) \otimes (a_{(2)} \otimes \varphi_{(1)}). \tag{4.16}$$

The counit, too, has to be a homomorphism of algebras, so as above we easily get

$$\epsilon_\mathcal{D}(a \otimes \varphi) \;=\; \epsilon(a)\,\langle \varphi, 1\rangle. \tag{4.17}$$

Finally, the antipode has to be a homomorphism of algebras from $\mathcal{D}(A, B)$ to $\mathcal{D}(A, B)^{\text{op}}$, so again by (iii) we must have $\gamma_\mathcal{D}(a \otimes \varphi) = \gamma(\iota_B(\varphi))\gamma(\iota_A(a))$. From (i) we get the obvious $\gamma(\iota_A(a)) = \gamma(a) \otimes 1^*$. Recall that the antipode of the co-opposite Hopf algebra is the inverse of the ordinary, and that the antipode of the restricted dual is obtained by taking the transpose. Then (ii) gives

$\gamma_{\mathcal{D}}(\iota_B(\varphi)) = 1 \otimes (\gamma^*)^{-1}(\varphi)$. Now using (iv) and the homomorphism properties of antipodes, and properties of transpose, we get

$$\gamma_{\mathcal{D}}(a \otimes \varphi) \;=\; \sum_{(a),(\varphi)} \langle \varphi_{(1)}, \gamma^{-1}(a_{(3)}) \rangle \, \langle \varphi_{(3)}, a_{(1)} \rangle \; \gamma(a_{(2)}) \otimes (\gamma^*)^{-1}(\varphi_{(2)}). \tag{4.18}$$

□

Before we turn to verifying the existence part of the proof, let us already show how the Drinfeld double construction yields braided Hopf algebras. Assume here that A is a finite dimensional Hopf algebra with basis $(e_i)_{i=1}^d$, and let $(\delta^i)_{i=1}^d$ denote the dual basis for A^*, so that

$$\langle \delta^i, e_j \rangle \;=\; \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases} .$$

We have already met the evaluation map $A^* \otimes A \to \mathbb{C}$ given by $\varphi \otimes a \mapsto \langle \varphi, a \rangle$. Let us now introduce the coevaluation map $\mathrm{coev} : \mathbb{C} \to A \otimes A^*$, which under the identification $A \otimes A^* \cong \mathrm{Hom}(A, A)$ corresponds to $\lambda \mapsto \lambda\, \mathrm{id}_A$. We can write explicitly

$$\mathrm{coev}(\lambda) \;=\; \lambda \sum_{i=1}^d e_i \otimes \delta^i.$$

Below we will frequently use the formula

$$\sum_{i=1}^d \langle \delta^i, b \rangle \, e_i \;=\; b,$$

valid for any $b \in A$. The combination of counitality with the defining property of the antipode is repeatedly used abusing the notation for multiple coproducts, for example as

$$\sum_{(b)} \Big(\gamma(b_{(j)}) b_{(j+1)} \Big) \otimes b_{(1)} \otimes \cdots \otimes b_{(j-1)} \otimes b_{(j+2)} \otimes \cdots \otimes b_{(n)} \;=\; \sum_{(b)} \Big(1_A \Big) \otimes b_{(1)} \otimes \cdots \otimes b_{(n-2)},$$

and analoguously in other similar cases, also with γ^{-1} in the opposite or co-opposite cases.

Theorem 4.18
Let A be a finite dimensional Hopf algebra with invertible antipode, and let $(e_i)_{i=1}^d$ and $(\delta^i)_{i=1}^d$ be dual bases of A and A^*. Then the Drinfeld double $\mathcal{D}(A)$ is a braided Hopf algebra with a universal R-matrix

$$R \;=\; (\iota_A \otimes \iota_{A^*})(\mathrm{coev}(1)) \;=\; \sum_{i=1}^d (e_i \otimes 1^*) \otimes (1 \otimes \delta^i).$$

Proof. Let us start by showing (R0), i.e. that R is invertible. The inverse is given by

$$\bar{R} \;=\; \sum_i (\gamma(e_i) \otimes 1^*) \otimes (1 \otimes \delta^i),$$

as Exercise 37 requires. We compute

$$\begin{aligned} R\,\bar{R} \;&= \Big(\sum_i (e_i \otimes 1^*) \otimes (1 \otimes \delta^i) \Big) \Big(\sum_j (\gamma(e_j) \otimes 1^*) \otimes (1 \otimes \delta^j) \Big) \\ &= \sum_{i,j} (e_i \gamma(e_j) \otimes 1^*) \otimes (1 \otimes \delta^i \delta^j). \end{aligned}$$

We would like to show that this elements of $\mathcal{D}(A)\otimes\mathcal{D}(A) = A\otimes A^*\otimes A\otimes A^*$ is the unit $1_{\mathcal{D}}\otimes 1_{\mathcal{D}} = 1\otimes 1^*\otimes 1\otimes 1^*$. Consider evaluating the expressions in $A\otimes A^*\otimes A\otimes A^*$ in the second and fourth components at $b\in A$ and $c\in A$. By the above calculation we see that $R\,\bar{R}$ evaluates to

$$\sum_{i,j} e_i\gamma(e_j)\otimes 1\,\langle 1^*,b\rangle\,\langle\delta^i\delta^j,c\rangle = \epsilon(b)\sum_{i,j}\sum_{(c)} e_i\gamma(e_j)\otimes 1\,\langle\delta^i,c_{(1)}\rangle\,\langle\delta^j,c_{(2)}\rangle$$
$$= \epsilon(b)\sum_{(c)} c_{(1)}\gamma(c_{(2)})\otimes 1 = \epsilon(b)\epsilon(c)\,1\otimes 1.$$

But the unit $1\otimes 1^*\otimes 1\otimes 1^*$ would obviously have evaluated to the same value, so we conclude that $\bar{R}$ is a right inverse: $R\,\bar{R} = 1\otimes 1^*\otimes 1\otimes 1^*$. To show that $\bar{R}$ is a left inverse is similar.

To prove property (R1), note that the set of elements that verifies the property

$$S = \left\{x\in\mathcal{D}(A)\ :\ \Delta^{\mathrm{op}}_{\mathcal{D}}(x)\,R = R\,\Delta_{\mathcal{D}}(x)\right\}$$

is a subalgebra of $\mathcal{D}$: indeed the unit $1_{\mathcal{D}} = 1\otimes 1^*$ has coproduct $\Delta_{\mathcal{D}}(1_{\mathcal{D}}) = 1_{\mathcal{D}}\otimes 1_{\mathcal{D}} = \Delta^{\mathrm{op}}(1_{\mathcal{D}})$ so it is clear that $1_{\mathcal{D}}\in S$, and if $x,y\in S$, then

$$\Delta^{\mathrm{op}}_{\mathcal{D}}(xy)\,R = \Delta^{\mathrm{op}}_{\mathcal{D}}(x)\,\Delta^{\mathrm{op}}_{\mathcal{D}}(y)\,R = \Delta^{\mathrm{op}}_{\mathcal{D}}(x)\,R\,\Delta_{\mathcal{D}}(y) = R\,\Delta_{\mathcal{D}}(x)\,\Delta_{\mathcal{D}}(y) = R\,\Delta_{\mathcal{D}}(xy).$$

By the defining formulas for the products in a Drinfeld double, elements of the form $a\otimes 1^*$ and $1\otimes\varphi$ generate $\mathcal{D}(A)$ as an algebra, so it suffices to show that the property (R1) holds for elements of these two forms.

Consider an element of the form $a\otimes 1^*$. We only need the easy product formulas in the Drinfeld double to compute

$$\Delta^{\mathrm{op}}_{\mathcal{D}}(a\otimes 1^*)\,R = \sum_i\sum_{(a)}\Big((a_{(2)}\otimes 1^*)\,(e_i\otimes 1^*)\Big)\otimes\Big((a_{(1)}\otimes 1^*)\,(1\otimes\delta^i)\Big)$$
$$= \sum_i\sum_{(a)}\Big((a_{(2)}e_i\otimes 1^*)\Big)\otimes\Big((a_{(1)}\otimes\delta^i)\Big),$$

but for the other term we need the more general products

$$R\,\Delta_{\mathcal{D}}(a\otimes 1^*) = \sum_i\sum_{(a)}\Big((e_i\otimes 1^*)\,(a_{(1)}\otimes 1^*)\Big)\otimes\Big((1\otimes\delta^i)\,(a_{(2)}\otimes 1^*)\Big)$$
$$= \sum_i\sum_{(a)}\Big(\,e_ia_{(1)}\otimes 1^*\Big)\otimes\Big(\sum_{(\delta^i)}\Big\langle(\delta^i)_{(3)},\gamma^{-1}(a_{(2)})\Big\rangle\,\Big\langle(\delta^i)_{(1)},a_{(4)}\Big\rangle\,a_{(3)}\otimes(\delta^i)_{(2)}\Big)$$

To show the equality of these two expressions in $\mathcal{D}\otimes\mathcal{D}\cong A\otimes A^*\otimes A\otimes A^*$, evaluate in the second and fourth components on two elements b,c of A. The first expression evaluates to

$$\sum_i\sum_{(a)}\epsilon(b)\,\Big\langle\delta^i,c\Big\rangle\,a_{(2)}e_i\otimes a_{(1)} = \sum_{(a)}\epsilon(b)\,a_{(2)}c\otimes a_{(1)}$$

and the second to

$$\sum_i\sum_{(a)}\sum_{(\delta^i)}\epsilon(b)\,\Big\langle(\delta^i)_{(2)},c\Big\rangle\,\Big\langle(\delta^i)_{(3)},\gamma^{-1}(a_{(2)})\Big\rangle\,\Big\langle(\delta^i)_{(1)},a_{(4)}\Big\rangle\,e_ia_{(1)}\otimes a_{(3)}$$
$$= \epsilon(b)\sum_i\sum_{(a)}\Big\langle\delta^i,a_{(4)}\,c\,\gamma^{-1}(a_{(2)})\Big\rangle\ e_ia_{(1)}\otimes a_{(3)}$$
$$= \epsilon(b)\sum_{(a)} a_{(4)}\,c\,\gamma^{-1}(a_{(2)})\,a_{(1)}\otimes a_{(3)} \qquad \text{(now use (H3) and (H2′) for } A^{\mathrm{op}}\text{)}$$
$$= \epsilon(b)\sum_{(a)} a_{(2)}\,c\,\otimes a_{(1)},$$

which is the same as the first. We conclude that for all $a \in A$ the equality $\Delta^{\mathrm{op}}(a \otimes 1^*)R = R\Delta(a \otimes 1^*)$ holds.

Showing that elements of the form $1 \otimes \varphi$ satisfy the property is similar. We have then shown that the set of elements S for which $\Delta^{\mathrm{op}}(x)R = R\Delta(x)$ holds is a subalgebra containing a generating set of elements, so $S = \mathcal{D}(A)$. Since we have also shown that R is invertible, we now conclude property (R1).

Properties (R2) and (R3) of the R-matrix are similar and they can be verified in the same way. We leave this as an exercise. □

Exercise 41 (Properties (R2) and (R3) for the universal R-matrix of a Drinfeld double)
Finish the proof of Theorem 4.18 by verifying the properties (R2) and (R3) for R and $\mathcal{D}(A)$.

We should still verify that in the Drinfeld double construction the structural maps $\mu_{\mathcal{D}}$, $\Delta_{\mathcal{D}}$, $\eta_{\mathcal{D}}$, $\epsilon_{\mathcal{D}}$ and $\gamma_{\mathcal{D}}$, given by formulas (4.14 – 4.18), satisfy the axioms (H1 – H6). This is mostly routine and we will leave checking some of the axioms to the dedicated reader. In view of formulas (4.14 – 4.18) it is also clear that the embedding maps $\iota_A : A \to \mathcal{D}(A, B)$ and $\iota_B : B^{\mathrm{cop}} \to \mathcal{D}(A, B)$ are homomorphisms of Hopf algebras.

For checking the associativity property we still introduce a lemma. Note that the product (4.14) can be written as

$$\mu_{\mathcal{D}} \;=\; (\mu \otimes \Delta^*) \circ (\mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B) \;:\; A \otimes B \otimes A \otimes B \to A \otimes B, \qquad (4.19)$$

where $\tau : B \otimes A \to A \otimes B$ is given by

$$\tau(\varphi \otimes a) \;=\; \sum_{(a),(\varphi)} \langle \varphi_{(1)}, a_{(3)} \rangle \, \langle \varphi_{(3)}, \gamma^{-1}(a_{(1)}) \rangle \, a_{(2)} \otimes \varphi_{(2)}$$

Lemma 4.19
We have the following equalities of linear maps

$$\begin{aligned} \tau \circ (\mathrm{id}_B \otimes \mu) &= (\mu \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \tau) \circ (\tau \otimes \mathrm{id}_A) \;:\; B \otimes A \otimes A \to A \otimes B \\ \tau \circ (\Delta^* \otimes \mathrm{id}_A) &= (\mathrm{id}_A \otimes \Delta^*) \circ (\tau \otimes \mathrm{id}_B) \circ (\mathrm{id}_B \otimes \tau) \;:\; B \otimes B \otimes A \to A \otimes B \end{aligned}$$

Proof. Consider the first claimed equation. We take $\varphi \in B$ and $a, b \in A$, and show that the values of both maps on the simple tensor $\varphi \otimes a \otimes b$ are equal. Calculating the left hand side, we use the homomorphism property of coproduct

$$\begin{aligned} \tau(\varphi \otimes ab) \;&=\; \sum_{(\varphi),(ab)} \langle \varphi_{(1)}, (ab)_{(3)} \rangle \, \langle \varphi_{(3)}, \gamma^{-1}((ab)_{(1)}) \rangle \, (ab)_{(2)} \otimes \varphi_{(2)} \\ &=\; \sum_{(\varphi),(a),(b)} \langle \varphi_{(1)}, a_{(3)} b_{(3)} \rangle \, \langle \varphi_{(3)}, \gamma^{-1}(a_{(1)} b_{(1)}) \rangle \, a_{(2)} b_{(2)} \otimes \varphi_{(2)}. \end{aligned}$$

We then calculate the right hand side using in the second and third steps coassociativity and definition of the coproduct $\mu^*|_B$ in $B \subset A^\circ$, respectively,

$$\begin{aligned} &(\mu \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \tau) \circ (\tau \otimes \mathrm{id}_A)(\varphi \otimes a \otimes b) \\ =\; &(\mu \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \tau)\Big(\sum_{(\varphi),(a)} \langle \varphi_{(1)}, a_{(3)} \rangle \, \langle \varphi_{(3)}, \gamma^{-1}(a_{(1)}) \rangle \, a_{(2)} \otimes \varphi_{(2)} \otimes b \Big) \\ =\; &(\mu \otimes \mathrm{id}_B)\Big(\sum_{(\varphi),(a),(b)} \langle \varphi_{(1)}, a_{(3)} \rangle \, \langle \varphi_{(5)}, \gamma^{-1}(a_{(1)}) \rangle \, \langle \varphi_{(2)}, b_{(3)} \rangle \, \langle \varphi_{(4)}, \gamma^{-1}(b_{(1)}) \rangle \, a_{(2)} \otimes b_{(2)} \otimes \varphi_{(3)} \Big) \\ =\; &\sum_{(\varphi),(a),(b)} \langle \varphi_{(1)}, a_{(3)} b_{(3)} \rangle \, \langle \varphi_{(3)}, \gamma(b_{(1)}) \gamma^{-1}(a_{(1)}) \rangle \, a_{(2)} b_{(2)} \otimes \varphi_{(2)}. \end{aligned}$$

By the anti-homomorphism property of γ^{-1}, the expressions are equal, so we have proved the first equality. The proof of the second equality is similar. □

Sketch of a proof of the Hopf algebra axioms in Theorem 4.15. Let us check associativity (H1) of $\mathcal{D}(A, B)$. Using first Equation (4.19), then the second formula in Lemma 4.19, and finally changing the order of maps that operate in different components, we calculate

$$\begin{aligned}\mu_{\mathcal{D}} \circ (\mu_{\mathcal{D}} \otimes \mathrm{id}_{\mathcal{D}}) &= (\mu \otimes \Delta^*) \circ (\mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B) \circ (\mu \otimes \Delta^* \otimes \mathrm{id}_A \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B \otimes \mathrm{id}_A \otimes \mathrm{id}_B) \\ &= (\mu \otimes \Delta^*) \circ (\mathrm{id}_A \otimes \mathrm{id}_A \otimes \Delta^* \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \mathrm{id}_B \otimes \tau \otimes \mathrm{id}_B) \\ &\qquad \circ (\mu \otimes \mathrm{id}_B \otimes \mathrm{id}_B \otimes \mathrm{id}_A \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B \otimes \mathrm{id}_A \otimes \mathrm{id}_B) \\ &= (\mu \otimes \Delta^*) \circ ((\mu \otimes \mathrm{id}_A) \otimes (\Delta^* \otimes \mathrm{id}_B)) \circ (\mathrm{id}_A \otimes \mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \tau \otimes \tau \otimes \mathrm{id}_B).\end{aligned}$$

Likewise, with the first of the formulas in the lemma, we calculate

$$\begin{aligned}\mu_{\mathcal{D}} \circ (\mathrm{id}_{\mathcal{D}} \otimes \mu_{\mathcal{D}}) &= (\mu \otimes \Delta^*) \circ (\mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \mathrm{id}_B \mu \otimes \mu \otimes \Delta^*) \circ (\mathrm{id}_A \otimes \mathrm{id}_B \otimes \mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B) \\ &= (\mu \otimes \Delta^*) \circ (\mathrm{id}_A \otimes \mu \otimes \mathrm{id}_B \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \tau \otimes \mathrm{id}_A \otimes \mathrm{id}_B \otimes \mathrm{id}_B) \\ &\qquad \circ (\mathrm{id}_A \otimes \mathrm{id}_B \otimes \mathrm{id}_A \otimes \mathrm{id}_A \otimes \Delta^*) \circ (\mathrm{id}_A \otimes \mathrm{id}_B \otimes \mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B) \\ &= (\mu \otimes \Delta^*) \circ ((\mathrm{id}_A \otimes \mu) \otimes (\mathrm{id}_B \otimes \Delta^*)) \circ (\mathrm{id}_A \otimes \mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B \otimes \mathrm{id}_B) \circ (\mathrm{id}_A \otimes \tau \otimes \tau \otimes \mathrm{id}_B).\end{aligned}$$

Using associativity (H1) for both algebras (A, μ, η) and $(B, \Delta^*, \epsilon^*)$ we see that these two expressions match and associativity follows for the Drinfeld double $\mathcal{D}(A, B)$.

Some of the other axioms are very easy to check. Consider for example coassociativity (H1′) of $\mathcal{D}(A, B)$. In view of Equation (4.16), and coassociativity of both A and B, we have

$$\begin{aligned}(\Delta_{\mathcal{D}} \otimes \mathrm{id}_{\mathcal{D}}) \circ \Delta_{\mathcal{D}}(a \otimes \varphi) &= \sum_{(a)} \sum_{(\varphi)} \sum_{(a_{(1)})} \sum_{(\varphi_{(2)})} (a_{(1)})_{(1)} \otimes (\varphi_{(2)})_{(2)} \otimes (a_{(1)})_{(2)} \otimes (\varphi_{(2)})_{(1)} \otimes a_{(2)} \otimes \varphi_{(1)} \\ &= \sum_{(a)} \sum_{(\varphi)} \sum_{(a_{(2)})} \sum_{(\varphi_{(1)})} a_{(1)} \otimes \varphi_{(2)} \otimes (a_{(2)})_{(1)} \otimes (\varphi_{(1)})_{(2)} \otimes (a_{(2)})_{(2)} \otimes (\varphi_{(1)})_{(1)} \\ &= (\mathrm{id}_{\mathcal{D}} \otimes \Delta_{\mathcal{D}}) \circ \Delta_{\mathcal{D}}(a \otimes \varphi).\end{aligned}$$

□

Exercise 42 (The Drinfeld double of the Hopf algebra of a finite group)
Let G be a finite group, and $A = \mathbb{C}[G]$ the Hopf algebra of the group G. Let $(e_g)_{g \in G}$ be the natural basis of A, and let $(f_g)_{g \in G}$ be the dual basis of A^*.

(a) *Show that A^* is, as an algebra, isomorphic to the algebra of complex valued functions on G with pointwise multiplication: when $\phi, \psi : G \to \mathbb{C}$, the product $\phi\psi$ is the function defined by $(\phi\psi)(g) = \phi(g)\psi(g)$ for all $g \in G$.*

(b) *Find explicit formulas for the coproduct, counit and antipode of A^* in the basis $(f_g)_{g \in G}$.*

Let $\mathcal{D}(A)$ be the Drinfeld double of A.

(c) *Find explicit formulas for the coproduct, counit and unit of $\mathcal{D}(A)$ in the basis $(e_h \otimes f_g)_{g,h \in G}$.*

(d) *Show that the product $\mu_{\mathcal{D}}$ and antipode $\gamma_{\mathcal{D}}$ of $\mathcal{D}(A)$ are given by the following formulas*

$$\begin{aligned}\mu_{\mathcal{D}}\Big((e_{h'} \otimes f_{g'}) \otimes (e_h \otimes f_g)\Big) &= \delta_{g', hgh^{-1}} \; e_{h'h} \otimes f_g \\ \gamma_{\mathcal{D}}(e_h \otimes f_g) &= e_{h^{-1}} \otimes f_{hg^{-1}h^{-1}}.\end{aligned}$$

4.4 A Drinfeld double of H_q and the quantum group $\mathcal{U}_q(\mathfrak{sl}_2)$

A Drinfeld double of H_q for q not a root of unity

Let $q \in \mathbb{C} \setminus \{0\}$, and assume throughout that $q^N \neq 1$ for all $N \neq 0$. Recall that as an algebra, H_q is generated by elements a, a^{-1}, b subject to the relations

$$a\,a^{-1} = 1 \quad , \qquad a^{-1}\,a = 1 \quad , \qquad a\,b = q\,b\,a.$$

The Hopf algebra structure on H_q is then uniquely determined by the coproducts of a and b,

$$\Delta(a) = a \otimes a \quad , \qquad \Delta(b) = a \otimes b + b \otimes 1.$$

We have considered the elements $1^*, \tilde{a}, \tilde{a}^{-1}, \tilde{b} \in H_q^\circ$ given by

$$\langle 1^*, b^m a^n \rangle = \delta_{m,0} \quad , \qquad \langle \tilde{a}^{\pm 1}, b^m a^n \rangle = \delta_{m,0}\, q^{\pm n} \quad , \qquad \langle \tilde{b}, b^m a^n \rangle = \delta_{m,1}.$$

Let $H'_q \subset H_q^\circ$ be the Hopf subalgebra of H_q° generated by these elements. By Lemma 4.1, H'_q is isomorphic to H_q as a Hopf algebra by the isomorphism which sends $a \mapsto \tilde{a}$ and $b \mapsto \tilde{b}$. In particular, $(\tilde{b}^m\, \tilde{a}^n)_{m \in \mathbb{N}, n \in \mathbb{Z}}$ is a basis of H'_q.

For the Drinfeld double we need the inverse of the antipode. This is given in the following.

Exercise 43 (A formula for the inverse of the antipode in H_q)
Show that in the Hopf algebra H_q, the antipode γ is invertible and its inverse is given by

$$\gamma^{-1}(b^m a^n) = (-1)^m\, q^{-\frac{1}{2}m(m-1)-mn}\, b^m a^{-m-n}.$$

Therefore we can consider the associated Drinfeld double, $D_q = \mathcal{D}(H_q, H'_q)$. Both H_q and H'_q are embedded in D_q, so let us choose the following notation for the embedded generators

$$\alpha = \iota_{H_q}(a) = a \otimes 1^* \qquad \beta = \iota_{H_q}(b) = b \otimes 1^* \qquad \tilde{\alpha} = \iota_{H'_q}(\tilde{a}) = 1 \otimes \tilde{a} \qquad \tilde{\beta} = \iota_{H'_q}(\tilde{b}) = 1 \otimes \tilde{b}.$$

We have, by properties (i), (ii), (iii) of Drinfeld double

$$\beta^m\, \alpha^n\, \tilde{\beta}^{m'}\, \tilde{\alpha}^{n'} = b^m a^n \otimes \tilde{b}^{m'} \tilde{a}^{n'}$$

and these elements, for $m, m' \in \mathbb{N}$ and $n, n' \in \mathbb{Z}$ form a basis of D_q.

Let us start by calculating the products of the elements $\alpha, \beta, \tilde{\alpha}, \tilde{\beta} \in D_q$. Among the products of the generators of D_q, property (i) makes those involving only α and β trivial, and property (ii) makes those involving only $\tilde{\alpha}$ and $\tilde{\beta}$ trivial. Also by property (iii) there is nothing to calculate for the products $\alpha\,\tilde{\alpha}$, $\alpha\,\tilde{\beta}$, $\beta\,\tilde{\alpha}$, $\beta\,\tilde{\beta}$. For the rest, we need the double coproducts of a and b,

$$\begin{aligned}(\Delta \otimes \mathrm{id}_{H_q}) \circ \Delta(a) &= a \otimes a \otimes a \\ (\Delta \otimes \mathrm{id}_{H_q}) \circ \Delta(b) &= a \otimes a \otimes b + a \otimes b \otimes 1 + b \otimes 1 \otimes 1,\end{aligned}$$

and of $\tilde{a}$ and $\tilde{b}$ for which the formulas are the same. We also need particular cases of Exercise 43,

$$\gamma^{-1}(a) = a^{-1} \quad , \qquad \gamma^{-1}(b) = -b\, a^{-1}.$$

The products that require short calculations are

$$\tilde{\alpha}\,\alpha = \underbrace{\langle \tilde{a}, a \rangle}_{=q}\ \underbrace{\langle \tilde{a}, \gamma^{-1}(a) \rangle}_{=q^{-1}}\ a \otimes \tilde{a} = \alpha\,\tilde{\alpha}$$

and

$$\begin{aligned}\tilde{\alpha}\,\beta &= \underbrace{\langle \tilde{a}, b \rangle}_{=0}\ \underbrace{\langle \tilde{a}, \gamma^{-1}(a) \rangle}_{=q^{-1}}\ a \otimes \tilde{a} + \underbrace{\langle \tilde{a}, 1 \rangle}_{=1}\ \underbrace{\langle \tilde{a}, \gamma^{-1}(a) \rangle}_{=q^{-1}}\ b \otimes \tilde{a} + \underbrace{\langle \tilde{a}, 1 \rangle}_{=1}\ \underbrace{\langle \tilde{a}, \gamma^{-1}(b) \rangle}_{=0}\ 1 \otimes \tilde{a} \\ &= q^{-1}\, \beta\,\tilde{\alpha}\end{aligned}$$

and

$$\begin{aligned}\tilde{\beta}\,\alpha &= \underbrace{\langle \tilde{a}, a \rangle}_{=q}\ \underbrace{\langle \tilde{b}, \gamma^{-1}(a) \rangle}_{=0}\ a \otimes \tilde{a} + \underbrace{\langle \tilde{a}, a \rangle}_{=q}\ \underbrace{\langle 1^*, \gamma^{-1}(a) \rangle}_{=1}\ a \otimes \tilde{a} + \underbrace{\langle \tilde{b}, a \rangle}_{=0}\ \underbrace{\langle 1^*, \gamma^{-1}(a) \rangle}_{=1}\ a \otimes \tilde{a} \\ &= q\, \alpha\,\tilde{\beta}\end{aligned}$$

and

$$\begin{aligned}\tilde{\beta}\,\beta \;=\;\; & \langle\tilde{a},b\rangle\,\langle\tilde{b},\gamma^{-1}(a)\rangle\; a\otimes\tilde{a} + \langle\tilde{a},1\rangle\,\langle\tilde{b},\gamma^{-1}(a)\rangle\; b\otimes\tilde{a} + \langle\tilde{a},1\rangle\,\langle\tilde{b},\gamma^{-1}(b)\rangle\; 1\otimes\tilde{a} \\ & + \langle\tilde{a},b\rangle\,\langle 1^*,\gamma^{-1}(a)\rangle\; a\otimes\tilde{b} + \langle\tilde{a},1\rangle\,\langle 1^*,\gamma^{-1}(a)\rangle\; b\otimes\tilde{b} + \langle\tilde{a},1\rangle\,\langle 1^*,\gamma^{-1}(b)\rangle\; 1\otimes\tilde{b} \\ & + \langle\tilde{b},b\rangle\,\langle 1^*,\gamma^{-1}(a)\rangle\; a\otimes 1^* + \langle\tilde{b},1\rangle\,\langle 1^*,\gamma^{-1}(a)\rangle\; b\otimes 1^* + \langle\tilde{b},1\rangle\,\langle 1^*,\gamma^{-1}(b)\rangle\; 1\otimes 1^* \\ =\;\; & -\tilde{\alpha} + \beta\,\tilde{\beta} + \alpha.\end{aligned}$$

We get the following description of D_q.

Proposition 4.20
The Hopf algebra D_q is, as an algebra, generated by elements $\alpha, \alpha^{-1}, \beta, \tilde{\alpha}, \tilde{\alpha}^{-1}, \tilde{\beta}$ with relations

$$\begin{aligned} \alpha\alpha^{-1} &= 1 \;=\; \alpha^{-1}\alpha & \tilde{\alpha}\tilde{\alpha}^{-1} &= 1 \;=\; \tilde{\alpha}^{-1}\tilde{\alpha} \\ \alpha\beta &= q\,\beta\alpha & \tilde{\alpha}\tilde{\beta} &= q\,\tilde{\beta}\tilde{\alpha} \\ \alpha\tilde{\beta} &= q^{-1}\,\tilde{\beta}\alpha & \tilde{\alpha}\beta &= q^{-1}\,\beta\tilde{\alpha} \\ \alpha\tilde{\alpha} &= \tilde{\alpha}\alpha & \tilde{\beta}\beta - \beta\tilde{\beta} &= \alpha - \tilde{\alpha}. \end{aligned}$$

The Hopf algebra structure on D_q is the unique one such that

$$\Delta(\alpha) \;=\; \alpha\otimes\alpha \qquad \Delta(\tilde{\alpha}) \;=\; \tilde{\alpha}\otimes\tilde{\alpha} \qquad \Delta(\beta) \;=\; \alpha\otimes\beta + \beta\otimes 1 \qquad \Delta(\tilde{\beta}) \;=\; \tilde{\beta}\otimes\tilde{\alpha} + 1\otimes\tilde{\beta}.$$

Proof. It is clear that the elements generate D_q, and we have just shown that the above relations hold for the generators. Using the relations it is possible to express any element of D_q as a linear combination of the vectors $\beta^m\alpha^n\tilde{\beta}^{m'}\tilde{\alpha}^{n'}$. Since these are linearly independent in D_q, it follows that the algebra D_q has a presentation given by the generators and relations as stated. The coproduct formulas for α, $\tilde{\alpha}$, β, $\tilde{\beta}$ are obvious in view of requirements (i) and (ii) of Drinfeld double, and it is a standard calculation to show that the structural maps are determined by the given values. □

The quantum group $\mathcal{U}_q(\mathfrak{sl}_2)$ as a quotient of D_{q^2}

To take quotients of Hopf algebras we need the notion of Hopf ideals. A vector subspace J in a Hopf algebra H is a Hopf ideal if J is a two-sided ideal of H as an algebra (i.e. $\mu(J\otimes H)\subset J$ and $\mu(H\otimes J)\subset J$), and J is a coideal of H as a coalgebra (i.e. $\Delta(J)\subset J\otimes H + H\otimes J$ and $\epsilon|_J = 0$) and J is an invariant subspace for the antipode (i.e. $\gamma(J)\subset J$). These requirements are precisely what one needs for the structural maps to be well defined on the equivalence classes $x+J$ that form the quotient space H/J.

Lemma 4.21
The element $\kappa = \alpha\,\tilde{\alpha}$ is a grouplike central element in D_q, and the two-sided ideal J_q generated by $\kappa - 1$ is a Hopf ideal.

Proof. We have

$$\Delta(\kappa) = \Delta(\alpha\tilde{\alpha}) = \Delta(\alpha)\,\Delta(\tilde{\alpha}) = (\alpha\otimes\alpha)\,(\tilde{\alpha}\otimes\tilde{\alpha}) = (\alpha\tilde{\alpha}\otimes\alpha\tilde{\alpha}) = \kappa\otimes\kappa,$$

so κ is grouplike. To show that it is central, it suffices to show that it commutes with the generators, but this is easily seen from the relations in Proposition 4.20: for example

$$\begin{aligned} \alpha\kappa &= \alpha\alpha\tilde{\alpha} \;=\; \alpha\tilde{\alpha}\alpha \;=\; \kappa\alpha \\ \beta\kappa &= \beta\alpha\tilde{\alpha} \;=\; q^{-1}\,\alpha\beta\tilde{\alpha} \;=\; q^{-1}\,q\,\alpha\tilde{\alpha}\beta \;=\; \kappa\beta, \end{aligned}$$

and similarly for commutation with $\tilde{\alpha}$ and $\tilde{\beta}$. The two sided ideal generated by $\kappa - 1$ is spanned by elements of the form $x(\kappa-1)y$, where $x, y \in D_q$. To show that it is a coideal, we first compute

$$\Delta(\kappa - 1) \;=\; \kappa\otimes\kappa - 1\otimes 1 \;=\; (\kappa-1)\otimes\kappa + 1\otimes(\kappa-1) \;\in\; J_q\otimes D_q + D_q\otimes J_q.$$

Then, using $\Delta(x(\kappa-1)y) = \Delta(x)\,\Delta(\kappa-1)\,\Delta(y)$, the more general result $\Delta(J_q) \subset J_q \otimes D_q + D_q \otimes J_q$ follows. To show that J_q is stable under antipode, we first compute

$$\gamma(\kappa-1) \;=\; \tilde{\alpha}^{-1}\alpha^{-1} - 1 \;=\; \tilde{\alpha}^{-1}\alpha^{-1}(1-\alpha\tilde{\alpha}) \;=\; -\tilde{\alpha}^{-1}\alpha^{-1}(\kappa-1) \;\in\; J_q.$$

Then, using $\gamma(x(\kappa-1)y) = \gamma(y)\,\gamma(\kappa-1)\,\gamma(x)$, the more general result $\gamma(J_q) \subset J_q$ follows. To show that $\epsilon|_{J_q} = 0$ note that $\epsilon(\kappa-1) = \epsilon(\kappa) - \epsilon(1) = 1-1 = 0$ and thus also $\epsilon(x(\kappa-1)y) = \epsilon(x)\,\epsilon(\kappa-1)\,\epsilon(y) = 0$. □

We can now take the quotient Hopf algebra D_q/J_q. Let us summarize what we have done, then. We've taken two copies of the building block, or the "quantum Borel subalgebra" H_q and put them together by the Drinfeld double construction as $D_q = \mathcal{D}(H_q, H_q')$ — one of the copies has generators α and β, and the other has generators $\tilde{\alpha}$ and $\tilde{\beta}$. Then we have identified their "quantum Cartan subalgebras", generated respectively by α and $\tilde{\alpha}$, by requiring $\alpha = \tilde{\alpha}^{-1}$ (which is equivalent to $\kappa - 1 = 0$). This is a way to obtain essentially $\mathcal{U}_q(\mathfrak{sl}_2)$, although, to be consistent with common usage, we redefine the parameter q and use q^2 instead.

If we use the notations K, E and F for the equivalence classes in D_{q^2}/J_{q^2} of $\tilde{\alpha}$, $\frac{-1}{q-q^{-1}}\,\tilde{\beta}$ and β, respectively, then the relations in Proposition 4.20 become the ones in the following definition of $\mathcal{U}_q(\mathfrak{sl}_2)$.

Definition 4.22. Let $q \in \mathbb{C} \setminus \{0, +1, -1\}$. The algebra $\mathcal{U}_q(\mathfrak{sl}_2)$ is the algebra generated by elements E, F, K, K^{-1} with relations

$$\begin{aligned} K\,K^{-1} &= 1 = K^{-1}\,K & \qquad K\,E\,K^{-1} &= q^2\,E \\ E\,F - F\,E &= \frac{1}{q-q^{-1}}\left(K - K^{-1}\right) & \qquad K\,F\,K^{-1} &= q^{-2}\,F. \end{aligned}$$

We equip $\mathcal{U}_q(\mathfrak{sl}_2)$ with the unique Hopf algebra structure such that

$$\Delta(K) \;=\; K \otimes K \quad , \qquad \Delta(E) \;=\; E \otimes K + 1 \otimes E \quad , \qquad \Delta(F) \;=\; K^{-1} \otimes F + F \otimes 1.$$

An easy comparison of the above definition with Proposition 4.20 and Lemma 4.21 gives the following.

Proposition 4.23
When q is not a root of unity, then the Hopf algebras $\mathcal{U}_q(\mathfrak{sl}_2)$ and D_{q^2}/J_{q^2} are isomorphic.

A convenient Poincaré-Birkhoff-Witt type basis of $\mathcal{U}_q(\mathfrak{sl}_2)$ is

$$(F^m\,K^k\,E^n)_{m,n\in\mathbb{N},k\in\mathbb{Z}}.$$

For working with the above parametrization, with q^2 replacing what used to be q, it is convenient to use the following more symmetric q-integers and q-factorials, which we denote as

$$[n] \;=\; \frac{q^n - q^{-n}}{q - q^{-1}} \tag{4.20}$$

$$[n]! \;=\; [n]\,[n-1]\,\cdots\,[2]\,[1] \tag{4.21}$$

$$\begin{bmatrix} n \\ k \end{bmatrix} \;=\; \frac{[n]!}{[k]!\,[n-k]!} \tag{4.22}$$

when considered as rational functions of q, and as

$$[n]_q \quad , \qquad [n]_q! \quad , \qquad \begin{bmatrix} n \\ k \end{bmatrix}_q \quad ,$$

respectively, when evaluated at a value $q \in \mathbb{C} \setminus \{0\}$.

Exercise 44 (Some q-formulas)
Show the following properties of the q-integers, q-factorials and q-binomials

(a) $[n] = q^{n-1} + q^{n-3} + \cdots + q^{-n+3} + q^{-n+1}$ *and* $[n]_q = q^{1-n}\,[\![n]\!]_{q^2}$

(b) $[m+n] = q^n\,[m] + q^{-m}\,[n] = q^{-n}\,[m] + q^m\,[n]$

(c) $[l]\,[m-n] + [m]\,[n-l] + [n]\,[l-m] = 0$

(d) $[n] = [2]\,[n-1] - [n-2]$.

Exercise 45 (Commutator formulas in $\mathcal{U}_q(\mathfrak{sl}_2)$)
Let $q \in \mathbb{C} \setminus \{0, 1, -1\}$ and consider the algebra $\mathcal{U}_q(\mathfrak{sl}_2)$. Prove that for all $k \geq 1$ one has

$$\begin{aligned} E\,F^k - F^k\,E &= \frac{[k]_q}{q-q^{-1}}\,F^{k-1}\left(q^{1-k}\,K - q^{k-1}\,K^{-1}\right) \\ F\,E^k - E^k\,F &= \frac{[k]_q}{q-q^{-1}}\left(q^{k-1}\,K^{-1} - q^{1-k}\,K\right)E^{k-1}. \end{aligned}$$

4.5 Representations of D_{q^2} and $\mathcal{U}_q(\mathfrak{sl}_2)$

Let us now start analyzing representations of $\mathcal{U}_q(\mathfrak{sl}_2)$ and the closely related Hopf algebra D_{q^2}. The general story is very much parallel with the (more familiar) case of representations of $\mathfrak{sl}_2$. In particular, in a given $\mathcal{U}_q(\mathfrak{sl}_2)$-module V we will attempt to diagonalize K, and then notice that if v is an eigenvector of K with eigenvalue λ,

$$K.v = \lambda\,v,$$

then $E.v$ and $F.v$ also either vanish or are eigenvectors of eigenvalues $q^{\pm 2}\lambda$,

$$K.(E.v) = KE.v = q^2\,EK.v = q^2\lambda\,E.v \quad , \qquad K.(F.v) = KF.v = q^{-2}\,FK.v = q^{-2}\lambda\,F.v.$$

The situation is nicest if q^2 is not a root of unity, so that repeated application of E (or F) on an eigenvector produces other eigenvectors with distinct eigenvalues.

Another useful observation for studying representations is the following, very much analoguous to the quadratic Casimir element of ordinary $\mathfrak{sl}_2$.

Lemma 4.24
The elements $C \in \mathcal{U}_q(\mathfrak{sl}_2)$ and $\nu \in D_{q^2}$ given by

$$\begin{aligned} C &= E\,F + \frac{1}{(q-q^{-1})^2}\left(q^{-1}\,K + q\,K^{-1}\right) \\ &= F\,E + \frac{1}{(q-q^{-1})^2}\left(q\,K + q^{-1}\,K^{-1}\right) \end{aligned}$$

and

$$\begin{aligned} \nu &= \tilde{\beta}\,\beta + \frac{q}{q-q^{-1}}\,\alpha + \frac{q^{-1}}{q-q^{-1}}\,\tilde{\alpha} \\ &= \beta\,\tilde{\beta} + \frac{q^{-1}}{q-q^{-1}}\,\alpha + \frac{q}{q-q^{-1}}\,\tilde{\alpha} \end{aligned}$$

are central.

Proof. Let us first show that the two formulas for C are equal. Their difference is

$$EF - FE + \frac{1}{(q-q^{-1})^2}\Big((q^{-1}-q)K + (q-q^{-1})K^{-1}\Big).$$

After canceling one factor $q - q^{-1}$ from the numerator and denominator, this is seen to be zero by one of the defining relations of $\mathcal{U}_q(\mathfrak{sl}_2)$.

To show that C is central, it suffices to show that it commutes with the generators K, E and F. Commutation with K is evident, since $KEF = q^2\,EKF = EFK$ and the second term of C is a polynomial in K and K^{-1}. To show commutation with E, calculate CE using the first expression for C to get

$$CE \;=\; EFE + \frac{1}{(q-q^{-1})^2}\Big(q^{-1}\,KE + q\,K^{-1}\,E\Big)$$

and EC using the second expression for C to get

$$EC \;=\; EFE + \frac{1}{(q-q^{-1})^2}\Big(q\,EK + q^{-1}\,EK^{-1}\Big).$$

Then it suffices to recall the relations $KE = q^2\,EK$ and $K^{-1}E = q^{-2}\,EK^{-1}$ to see the equality $CE = EC$. The commutation of C with F is shown similarly.

The verification that ν is central in D_{q^2} is left as an exercise. For q not a root of unity, the first statement in fact follows from the second by passing to the quotient $\mathcal{U}_q(\mathfrak{sl}_2) \cong D_{q^2}/J_{q^2}$. □

On representations of D_{q^2}

We will start by analyzing representations of D_{q^2}, because every representation of $\mathcal{U}_q(\mathfrak{sl}_2)$ can be interpreted as a representation of D_{q^2}, where $\kappa = \alpha\tilde{\alpha}$ acts as identity. Note that we thus assume q is not a root of unity, so that D_{q^2} is defined and $\mathcal{U}_q(\mathfrak{sl}_2) \cong D_{q^2}/J_{q^2}$. The case when q is a root of unity is more complicated in terms of representation theory and has to be treated separately anyway.

We will first look for irreducible representations of D_{q^2}, i.e. simple D_{q^2}-modules. Note first of all the following general principle (essentially the same as Schur's lemma).

Lemma 4.25
If V is a finite dimensional irreducible representation of an algebra A, and if $c \in A$ is a central element, then there is a $\lambda \in \mathbb{C}$ such that c acts as $\lambda\,\mathrm{id}_V$ on V.

Proof. It is always possible to find one eigenvector of c, with eigenvalue that is a root of the characteristic polynomial. Call the eigenvalue λ and note that $c - \lambda\,\mathrm{id}_V$ is a D_{q^2}-module map $V \to V$ with a nontrivial kernel. The kernel is a subrepresentation, so by irreducibility it has to be the whole V. □

Because of the above principle, we will in what follows consider only representations of D_{q^2} where $\kappa = \alpha\tilde{\alpha}$ acts as $\lambda\,\mathrm{id}$. As a consequence $\tilde{\alpha}$ has the same action as $\lambda\,\alpha^{-1}$.

The following exercise illustrates an alternative concrete approach to the representation theory of D_{q^2}. It is instructive, but we shall not pursue this approach further.

Exercise 46 (A first step of a calculation for diagonalization of α in D_{q^2}-modules)
Let q be a non-zero complex number which is not a root of unity, and let D_{q^2} be the algebra generated by $\alpha, \alpha^{-1}, \beta, \tilde{\alpha}, \tilde{\alpha}^{-1}, \tilde{\beta}$ with relations

$$\begin{aligned}
\alpha\alpha^{-1} &= 1 = \alpha^{-1}\alpha & \tilde{\alpha}\tilde{\alpha}^{-1} &= 1 = \tilde{\alpha}^{-1}\tilde{\alpha} \\
\alpha\beta &= q^2\,\beta\alpha & \tilde{\alpha}\tilde{\beta} &= q^2\,\tilde{\beta}\tilde{\alpha} \\
\alpha\tilde{\beta} &= q^{-2}\,\tilde{\beta}\alpha & \tilde{\alpha}\beta &= q^{-2}\,\beta\tilde{\alpha} \\
\alpha\tilde{\alpha} &= \tilde{\alpha}\alpha & \tilde{\beta}\beta - \beta\tilde{\beta} &= \alpha - \tilde{\alpha}.
\end{aligned}$$

(a) *Suppose that V is a finite dimensional D_{q^2}-module, of dimension d. By considering generalized eigenspaces of α (or of $\tilde{\alpha}$), show that the elements β^k and $\tilde{\beta}^k$ must act as zero on V for any $k \geq d$.*

(b) *Find polynomials $P(\alpha,\tilde{\alpha})$, $Q(\alpha,\tilde{\alpha})$, $R(\alpha,\tilde{\alpha})$ of α and $\tilde{\alpha}$ such that the following equation holds*

$$P(\alpha,\tilde{\alpha})\,\beta^2\,\tilde{\beta}^2 + Q(\alpha,\tilde{\alpha})\,\beta\,\tilde{\beta}^2\,\beta + R(\alpha,\tilde{\alpha})\,\tilde{\beta}^2\,\beta^2 \;=\; (q\,\alpha - q^{-1}\,\tilde{\alpha})\,(\alpha-\tilde{\alpha})\,(q^{-1}\,\alpha - q\,\tilde{\alpha}).$$

(c) *Suppose that V is a D_{q^2}-module where the central element $\kappa = \alpha\tilde{\alpha}$ acts as $\lambda\,\mathrm{id}_V$ and where $\tilde{\beta}^2$ acts as zero. Show, using the result of (c), that α and $\tilde{\alpha}$ are diagonalizable on V and the eigenvalues of both are among*

$$\pm\sqrt{\lambda}\,q^{-1},\;\pm\sqrt{\lambda},\;\pm\sqrt{\lambda}\,q.$$

Conclude in particular that in any two-dimensional $\mathcal{U}_q(\mathfrak{sl}_2)$-module, K is diagonalizable and its possible eigenvalues are ± 1, $\pm q$, $\pm q^{-1}$.

The same idea can be used to diagonalize α in more general modules as follows.

Exercise 47 (Explicit diagonalization for D_{q^2} and $\mathcal{U}_q(\mathfrak{sl}_2)$)
Let q and D_{q^2} be as in the previous exercise. Define, for $t \in \mathbb{Z}$, the elements

$$\theta_t \;=\; q^t\,\alpha - q^{-t}\,\tilde{\alpha}.$$

(a) *Prove the following formula*

$$\tilde{\beta}^k\beta^m \;=\; \sum_{j=0}^{k} \frac{[m]_q!\;[k]_q!}{[m-j]_q!\;[k-j]_q!\;[j]_q!}\;\beta^{m-j}\,\Big(\prod_{s=1}^{j}\theta_{m+k-j-s}\Big)\,\tilde{\beta}^{k-j}.$$

Note that this contains the formulas of Exercise 45 as special cases.

(b) *By considering linear combinations of elements of the form*

$$P_m(\alpha,\tilde{\alpha})\;\beta^{k-m}\;\tilde{\beta}^k\;\beta^m,$$

where P_m are polynomials in two variables, show that the element

$$\prod_{t=-k+1}^{k-1}\theta_t$$

belongs to the two-sided ideal generated by $\tilde{\beta}^k$.

(c) *Suppose that V is a D_{q^2}-module where the central element $\kappa = \alpha\tilde{\alpha}$ acts as $\lambda\,\mathrm{id}_V$ and where $\tilde{\beta}^k$ acts as zero. Show that α and $\tilde{\alpha}$ are diagonalizable on V and that their eigenvalues are among*

$$\pm\sqrt{\lambda}\,q^{1-k},\;\pm\sqrt{\lambda}\,q^{2-k},\;\ldots,\;\pm\sqrt{\lambda}\,q^{k-2},\;\pm\sqrt{\lambda}\,q^{k-1}.$$

(d) *Conclude that on any finite dimensional $\mathcal{U}_q(\mathfrak{sl}_2)$ module of dimension d, the eigenvalues of K are among $\pm q^{d-1}, \pm q^{d-2}, \ldots, \pm q^{2-d}, \pm q^{1-d}$. What is the analoguous result about $\mathfrak{sl}_2$?*

Suppose now that V is an irreducible representation of D_{q^2}, and denote the (only) eigenvalue of κ by $\lambda \neq 0$. Take an eigenvector v of α, so $\alpha.v = \mu'\,v$ for some $\mu' \neq 0$. Now an easy computation shows that the vectors $\tilde{\beta}^j.v$ are either eigenvectors of α with eigenvalue $q^{-2j}\mu'$, or zero vectors. Since these eigenvalues are different and eigenvectors corresponding to different eigenvalues are linearly independent, we see that if V is finite dimensional, then there must be a $j > 0$ such that the vector $w_0 = \tilde{\beta}^{j-1}.v$ satisfies

$$\tilde{\beta}.w_0 \;=\; 0 \qquad \text{and} \qquad \alpha.w_0 \;=\; \mu\, w_0,$$

where $\mu = q^{2(1-j)}\mu'$. Denote $w_j = \beta^j.w_0$. Again, w_j are eigenvectors of α with eigenvalues $q^{2j}\mu$, so for some $d \in \mathbb{N}$ we have

$$w_{d-1} \;=\; \beta^{d-1}.w_0 \;\neq\; 0 \qquad \text{but} \qquad w_d \;=\; \beta.w_{d-1} \;=\; \beta^d.w_0 \;=\; 0.$$

We claim that the linear span $W \subset V$ of $\{w_0, w_1, w_2, \ldots, w_{d-1}\}$ is a subrepresentation, and thus by irreducibility $W = V$. We have

$$\alpha.w_j \;=\; q^{2j}\mu\, w_j \qquad \text{and} \qquad \tilde{\alpha}.w_j \;=\; q^{-2j}\frac{\lambda}{\mu}\, w_j,$$

so W is stable under the action of $\alpha, \tilde{\alpha}$ and β. We must only verify that $\tilde{\beta}$ preserves W. Calculate the action of $\tilde{\beta}$ on w_j commuting $\tilde{\beta}$ to the right of all β, and finally recalling that $\tilde{\beta}.w_0 = 0$,

$$\begin{aligned}
\tilde{\beta}.w_j \;&= \tilde{\beta}\beta^j.w_0 \;=\; (\beta\tilde{\beta} + \alpha - \tilde{\alpha})\beta^{j-1}.w_0 \\
&= \beta\tilde{\beta}\beta^{j-1}.w_0 + (q^{2(j-1)}\mu - q^{-2(j-1)}\frac{\lambda}{\mu})\; \beta^{j-1}.w_0 \\
&= \beta(\beta\tilde{\beta} + \alpha - \tilde{\alpha})\beta^{j-2}.w_0 + \Big(q^{2(j-1)}\mu - q^{-2(j-1)}\frac{\lambda}{\mu}\Big)\; \beta^{j-1}.w_0 \\
&= \beta^2\tilde{\beta}\beta^{j-2}.w_0 + \Big((q^{2(j-1)} + q^{2(j-2)})\mu - (q^{-2(j-1)} + q^{-2(j-2)})\frac{\lambda}{\mu}\Big)\; \beta^{j-1}.w_0 \\
&= \cdots \\
&= \beta^j\tilde{\beta}.w_0 + \Big((q^{2(j-1)} + q^{2(j-2)} + \cdots + q^2 + 1)\mu - (q^{-2(j-1)} + q^{-2(j-2)} + \cdots + q^{-2} + 1)\frac{\lambda}{\mu}\Big)\; \beta^{j-1}.w_0 \\
&= [j]_q \,\Big(q^{j-1}\mu - q^{1-j}\frac{\lambda}{\mu}\Big)\; w_{j-1}.
\end{aligned}$$

This finishes the proof that W is a subrepresentation. We will finally obtain a relation between the values of μ, λ and d. For this, note that $\beta^d.w_0 = w_d = 0$. Thus also $\tilde{\beta}\beta^d.w_0 = 0$. But the above calculation is still valid and it says that $\tilde{\beta}\beta^d.w_0$ is a constant multiple of w_{d-1}, with the constant $[d]_q\,(q^{d-1}\mu - q^{1-d}\lambda/\mu)$. This constant must therefore vanish, ans since the q-integers are non-zero, we get the following relation between the parameters λ, μ and d

$$\mu^2 \;=\; q^{2(1-d)}\lambda. \tag{4.23}$$

Given $\lambda \in \mathbb{C} \setminus \{0\}$ and $d \in \mathbb{N}$, the two solutions for μ are

$$\mu \;=\; \pm q^{1-d}\,\sqrt{\lambda}.$$

In particular, the eigenvalues of α on W are of the form $q^{2j}\mu$ and those of $\tilde{\alpha}$ are $q^{-2j}\lambda/\mu$, so the spectra of both consist of

$$\pm\sqrt{\lambda}q^{1-d},\; \pm\sqrt{\lambda}q^{3-d},\; \ldots,\; \pm\sqrt{\lambda}q^{d-3},\; \pm\sqrt{\lambda}q^{d-1}.$$

Note also that the action of $\tilde{\beta}$ simplifies a bit,

$$\tilde{\beta}.w_j \;=\; \pm\sqrt{\lambda}\,(q^{-1} - q)\,[j]_q\,[d-j]_q\; w_{j-1}.$$

We have in fact found all the irreducible finite dimensional representations of D_{q^2}.

Theorem 4.26
For any nonzero complex number λ and a choice of square root $\sqrt{\lambda}$, and d a positive integer, there exists a d-dimensional irreducible representation $W_d^{(\sqrt{\lambda})}$ of D_{q^2} with basis $\{w_0, w_1, w_2, \ldots, w_{d-1}\}$ such that

$$\alpha.w_j = \sqrt{\lambda}\, q^{1-d+2j}\, w_j \qquad \tilde{\alpha}.w_j = \sqrt{\lambda}\, q^{d-1-2j}\, w_j$$
$$\beta.w_j = w_{j+1} \qquad \tilde{\beta}.w_j = \sqrt{\lambda}\, [j]_q\, [d-j]_q\, (q^{-1}-q)\, w_{j-1}.$$

Any finite dimensional D_{q^2}-module contains a submodule isomorphic to some $W_d^{(\sqrt{\lambda})}$, and in particular there are no other finite dimensional irreducible D_{q^2} modules.

Proof. To verify that the formulas indeed define a representation is straightforward and the calculations are essentially the same as above. To verify irreducibility of $W_d^{(\sqrt{\lambda})}$, note that if $W' \subset W_d^{(\sqrt{\lambda})}$ is a non-zero submodule, then it contains some eigenvector of α, which must be proportional to some w_j. Then by the repeated action of $\tilde{\beta}$ and β we see that W' contains all w_j, $j = 0, 1, 2, \ldots, d-1$ (note that the coefficient $\sqrt{\lambda}\, [j]_q\, [d-j]_q\, (q^{-1}-q)$ is never zero for $j = 1, 2, \ldots, d-1$). Above we already showed that any finite dimensional D_{q^2} module V must contain a submodule isomorphic to $W_d^{(\pm\sqrt{\lambda})}$, so it follows indeed that these are all the possible irreducible D_{q^2}-modules. □

Since any representation of $\mathcal{U}_q(\mathfrak{sl}_2)$ is a representation of D_{q^2} such that $\lambda = 1$, we have also found all irreducible representations of $\mathcal{U}_q(\mathfrak{sl}_2)$. To get the explicit formulas, recall that the generators K, E, F correspond to the equivalence classes of $\tilde{\alpha}$, $\frac{-1}{q-q^{-1}}\tilde{\beta}$ and β modulo the Hopf ideal J_{q^2} generated by the element $\kappa - 1$.

Theorem 4.27
Let q be a non-zero complex number which is not a root of unity. For any positive integer d and for $\varepsilon \in \{+1, -1\}$, there exists a d-dimensional irreducible representation W_d^{ε} of $\mathcal{U}_q(\mathfrak{sl}_2)$ with basis $\{w_0, w_1, w_2, \ldots, w_{d-1}\}$ such that

$$K.w_j = \varepsilon\, q^{d-1-2j}\, w_j$$
$$F.w_j = w_{j+1}$$
$$E.w_j = \varepsilon\, [j]_q\, [d-j]_q\, w_{j-1}.$$

There are no other finite dimensional irreducible $\mathcal{U}_q(\mathfrak{sl}_2)$-modules.

Proof. Follows directly from Theorem 4.26. □

Using the formulas in Lemma 4.24 one computes that on W_d^{ε}

$$\text{the central element } C \text{ acts as } \varepsilon\, \frac{q^d + q^{-d}}{(q-q^{-1})^2}\, \mathrm{id}_{W_d^{\varepsilon}}. \tag{4.24}$$

Since the numbers $\pm(q^d + q^{-d})$ are distinct, we see first of all that none of the W_d^{ε} are isomorphic with each other (of course for different dimension d they couldn't be isomorphic anyway). Thus the value of C distinguishes the different irreducible representations.

Having found all irreducible representations of $\mathcal{U}_q(\mathfrak{sl}_2)$, we will next prove complete reducibility of all representations of it. Let us check that when q is not a root of unity, $\mathcal{U}_q(\mathfrak{sl}_2)$ satisfies the semisimplicity criterion of Proposition 3.53.

Lemma 4.28
Let $q \in \mathbb{C} \setminus \{0\}$ not a root of unity. If V is a finite dimensional $\mathcal{U}_q(\mathfrak{sl}_2)$-module and $W \subset V$ is an irreducible submodule such that V/W is a trivial one dimensional module, then there is a trivial one dimensional submodule $W' \subset V$ such that $V = W \oplus W'$.

Proof. Theorem 4.27 lists all possible irreducible $\mathcal{U}_q(\mathfrak{sl}_2)$-modules, they are W_d^ε for d a positive integer and $\varepsilon \in \{\pm 1\}$. So we have $W \cong W_d^\varepsilon$ for some d and ε. We first suppose that $d \neq 1$ or $\varepsilon \neq +1$ — the case when W also is trivial (i.e. $W \cong W_1^{+1}$) is treated separately. By Equation (4.24), the central element C acts as multiplication by the constant $c_{d,\varepsilon} = \varepsilon(q^d + q^{-d})/(q - q^{-1})^2$ on W. On the quotient V/W it acts as $c_{1,1} = (q + q^{-1})/(q - q^{-1})^2$. Therefore

$$\frac{1}{c_{d,\varepsilon} - c_{1,1}}\Big(C - c_{1,1}\,\mathrm{id}_V\Big)$$

is a projection to W which is also an $\mathcal{U}_q(\mathfrak{sl}_2)$-module map. This implies that W has a complementary submodule $\mathrm{Ker}\,(C - c_{1,1}\,\mathrm{id})$.

The case when both W and V/W are trivial has to be treated separately, but it is very easy to show that in this case V is a trivial 2-dimensional representation and any complementary subspace to W is a complementary submodule. □

Corollary 4.29
For q not a root of unity, the algebra $\mathcal{U}_q(\mathfrak{sl}_2)$ is semisimple.

Proof. Use Proposition 3.53, Remark 3.54 and Lemma 4.28. □

Exercise 48 (Some tensor products of $\mathcal{U}_q(\mathfrak{sl}_2)$-modules)
Assume that $q \in \mathbb{C}$ is not a root of unity.

(a) *Show that $W_d^\varepsilon \cong W_d^{+1} \otimes W_1^\varepsilon$.*

(b) *Let $d_1 \geq d_2 > 0$ and denote by $w_0^{(1)}, w_1^{(1)}, \ldots, w_{d_1-1}^{(1)}$ and $w_0^{(2)}, w_1^{(2)}, \ldots, w_{d_2-1}^{(2)}$ the bases of $W_{d_1}^{+1}$ and $W_{d_2}^{+1}$, respectively, chosen as in Theorem 4.27. Consider the module $W_{d_1}^{+1} \otimes W_{d_2}^{+1}$. Show that for any $l \in \{0, 1, 2, \ldots, d_2 - 1\}$ the vector*

$$v \;=\; \sum_{s=0}^{l} \frac{(-1)^s}{[s]_q!}\,\frac{[l]_q!}{[l-s]_q!}\,\frac{[d_1-1-s]_q!}{[d_1-1]_q!}\,\frac{[d_2-l-1+s]_q!}{[d_2-l-1]_q!}\;q^{s(2l-d_2-s)}\;w_s^{(1)} \otimes w_{l-s}^{(2)}$$

is an eigenvector of K and that it satisfies

$$E.v \;=\; 0.$$

(c) *Using the result of (b), conclude that we have the following isomorphism of $\mathcal{U}_q(\mathfrak{sl}_2)$-modules*

$$W_{d_1}^{+1} \otimes W_{d_2}^{+1} \;\cong\; W_{d_1+d_2-1}^{+1} \oplus W_{d_1+d_2-3}^{+1} \oplus W_{d_1+d_2-5}^{+1} \oplus \cdots \oplus W_{d_1-d_2+3}^{+1} \oplus W_{d_1-d_2+1}^{+1}.$$

4.6 Solutions to YBE from infinite dimensional Drinfeld doubles

Let us pause for a moment to see where we are in finding solutions to the Yang-Baxter equation, Equation (YBE). The overall story goes smoothly — by Theorem 4.13 any representation of any braided Hopf algebra gives us a solution of YBE, and by Theorem 4.18 the Drinfeld double construction produces braided Hopf algebras. We have even concretely described an interesting Drinfeld double D_{q^2} and a quotient $\mathcal{U}_q(\mathfrak{sl}_2)$ of it, and we have found all their irreducible representations in Theorems 4.26 and 4.27.

There is just one issue — to obtain the universal R-matrix which makes the Drinfeld double a braided Hopf algebra, we had to assume finite dimensionality of the Hopf algebra whose Drinfeld double we take. Unfortunately, the Hopf algebra D_{q^2} is a Drinfeld double of the infinite dimensional building block Hopf algebra H_{q^2}, so we seem to have a small problem.

Although we can't properly make D_{q^2} and $\mathcal{U}_q(\mathfrak{sl}_2)$ braided Hopf algebras, in that we will not really find a universal R-matrix in the second tensor power of these algebras, we can nevertheless find solutions of the Yang-Baxter equation by more or less the same old receipe. Let us first describe the heuristics, and then prove the main result.

Heuristics and formula for the R-matrices

Assume that A is a Hopf algebra with invertible antipode, and $\mathcal{D} = \mathcal{D}(A, A^\circ)$ is the Drinfeld double. Recall that $\mathcal{D} = A \otimes A^\circ$ as a vector space, and the Hopf algebras A and $(A^\circ)^{\mathrm{cop}}$ are embedded to $\mathcal{D}$ by the maps

$$\iota_A : A \to \mathcal{D} \qquad \iota_{A^\circ} : A^\circ \to \mathcal{D}$$
$$a \mapsto a \otimes 1^* \qquad \varphi \mapsto 1 \otimes \varphi.$$

We would like to set, as in Theorem 4.18,

$$R \stackrel{?}{=} \sum_\alpha \iota_A(e_\alpha) \otimes \iota_{A^\circ}(\delta^\alpha), \tag{4.25}$$

where (e_α) is a basis of A, and (δ^α) is a "dual basis" of A°. This is of course problematic in the infinite dimensional case.

Let us first fix some notation. Since A embeds to $\mathcal{D}$ as a Hopf algebra, we can consider restrictions on A of elements $\phi \in \mathcal{D}^\circ$ of the restricted dual of the Drinfeld double: define $\phi|_A \in A^\circ$ by

$$\langle \phi|_A, a \rangle = \langle \phi, \iota_A(a) \rangle \qquad \text{for all } a \in A.$$

Furthermore, since A° embeds to $\mathcal{D}$, we can interpret the above as an element of $\mathcal{D}$. We define

$$\phi' = \iota_{A^\circ}(\phi|_A) \in \mathcal{D} \qquad \text{for any } \phi \in \mathcal{D}^\circ. \tag{4.26}$$

If the bases (e_α) and (δ^α) were to be dual to each other, we would expect a formula of the type

$$\sum_\alpha \langle \varphi, e_\alpha \rangle \, \delta^\alpha \stackrel{?}{=} \varphi$$

to hold for any $\varphi \in A^\circ$. So in particular when $\varphi = \phi|_A$, we expect

$$\sum_\alpha \langle \phi|_A, e_\alpha \rangle \, \iota_B(\delta^\alpha) \stackrel{?}{=} \iota_B(\phi|_A) = \phi'.$$

Returning to the heuristic formula (4.25) for the universal R-matrix of $\mathcal{D}$, let us consider how it would act on representations. If V is a $\mathcal{D}$-module with basis $(v_j)_{j=1}^d$ and representative forms $\lambda_{i,j} \in \mathcal{D}^\circ$ such that

$$x.v_j = \sum_{i=1}^d \langle \lambda_{i,j}, x \rangle \, v_i \qquad \text{for any } x \in \mathcal{D}$$

we would like to make the R-matrix act on $V \otimes V$ by

$$\begin{aligned} R(v_i \otimes v_j) &\stackrel{?}{=} \sum_\alpha \iota_A(e_\alpha).v_i \otimes \iota_{A^\circ}(\delta^\alpha).v_j \\ &\stackrel{?}{=} \sum_\alpha \sum_{l,k=1}^d \underbrace{\langle \lambda_{l,i}, \iota_A(e_\alpha) \rangle}_{=\langle \lambda_{l,i}|_A, e_\alpha \rangle} \langle \lambda_{k,j}, \iota_{A^\circ}(\delta^\alpha) \rangle \, v_l \otimes v_k \\ &\stackrel{?}{=} \sum_{l,k=1}^d \langle \lambda_{k,j}, (\lambda_{l,i})' \rangle \, v_l \otimes v_k. \end{aligned}$$

We have found a formula that is expressed only in terms of the representative forms, and therefore it is meaningful also when A is infinite dimensional. We are mostly using $\check{R} = S_{V,V} \circ R$, so the appropriate definitions are

$$\check{R} : V \otimes V \to V \otimes V \qquad \check{R}(v_i \otimes v_j) = \sum_{k,l=1}^d r_{i,j}^{k,l} \, v_k \otimes v_l$$
$$r_{i,j}^{k,l} = \langle \lambda_{k,j}, (\lambda_{l,i})' \rangle. \tag{4.27}$$

Proving that the formula gives solutions to YBE

We now check that Equation (4.27) indeed works. We record a small lemma, which is needed along the way.

Lemma 4.30
For any $\phi \in \mathcal{D}^\circ$ and $x \in \mathcal{D}$, the following equality holds in $\mathcal{D}$

$$\sum_{(\phi)} \sum_{(x)} \langle \phi_{(1)}, x_{(2)} \rangle \, x_{(1)} (\phi_{(2)})' \; = \; \sum_{(\phi)} \sum_{(x)} \langle \phi_{(2)}, x_{(1)} \rangle \, (\phi_{(1)})' x_{(2)}.$$

When $x = \psi'$ with $\psi \in \mathcal{D}^\circ$ we have

$$\sum_{(\phi),(psi)} \langle \phi_{(1)}, (\psi_{(1)})' \rangle \, (\psi_{(2)})' \, (\phi_{(2)})' \; = \; \sum_{(\phi),(\psi)} \langle \phi_{(2)}, (\psi_{(2)})' \rangle \, (\phi_{(1)})' (\psi_{(1)})'.$$

Proof. The proof of the first statement is left as an exercise. The second statement follows as a particular case of the first, when we observe that for $x = \psi'$ the coproduct of x can be written in terms of the coproduct of ψ as

$$\sum_{(x)} x_{(1)} \otimes x_{(2)} \; = \Delta_{\mathcal{D}}(x) \; = \; \Delta_{\mathcal{D}}(\iota_{A^\circ}(\psi|_A)) \; = \; (\iota_{A^\circ} \otimes \iota_{A^\circ})((\mu^*)^{\mathrm{cop}}(\psi|_A)) \; = \; \sum_{(\psi)} (\psi_{(2)})' \otimes (\psi_{(1)})'.$$

□

Theorem 4.31
Let A be a Hopf algebra with invertible antipode and $B \subset A^\circ$ a Hopf subalgebra of the restricted dual, and let $\mathcal{D} = \mathcal{D}(A, B)$ be the Drinfeld double associated to A and B. Let V be a $\mathcal{D}$-module with basis $(v_j)_{j=1}^d$, and assume that the representative forms $\lambda_{i,j} \in \mathcal{D}^\circ$ satisfy $\lambda_{i,j}|_A \in B$. Then the linear map $\check{R} : V \otimes V \to V \otimes V$ defined by Equation (4.27) satisfies the Yang-Baxter equation (YBE). Furthermore, the associated braid group representation on $V^{\otimes n}$ commutes with the action of $\mathcal{D}$.

Proof. The proof is a direct calculation — besides the definitions, the key properties to keep in mind are the coproduct formula of representative forms $\mu^*(\lambda_{i,j}) = \sum_k \lambda_{i,k} \otimes \lambda_{k,j}$ and the formulas of Lemma 4.30. Let us take an elementary tensor $v_s \otimes v_t \otimes v_u \in V \otimes V \otimes V$. Applying the left hand side of the YBE on this, we get

$$\begin{aligned}
& \check{R}_{12} \circ \check{R}_{23} \circ \check{R}_{12}(v_s \otimes v_t \otimes v_u) \\
= & \sum_{i,j,k,l,m,n} r^{l,m}_{i,k} \, r^{k,n}_{j,u} \, r^{i,j}_{s,t} \, v_l \otimes v_m \otimes v_n \\
= & \sum_{i,j,k,l,m,n} \langle \lambda_{l,k}, (\lambda_{m,i})' \rangle \, \langle \lambda_{k,u}, (\lambda_{n,j})' \rangle \, \langle \lambda_{i,t}, (\lambda_{j,s})' \rangle \, v_l \otimes v_m \otimes v_n \\
= & \sum_{i,j,l,m,n} \langle \lambda_{l,u}, (\lambda_{m,i})'(\lambda_{n,j})' \rangle \, \langle \lambda_{i,t}, (\lambda_{j,s})' \rangle \, v_l \otimes v_m \otimes v_n \\
= & \sum_{l,m,n} \sum_{(\lambda_{m,t}),(\lambda_{n,s})} \langle \lambda_{l,u}, ((\lambda_{m,t})_{(1)})'((\lambda_{n,s})_{(1)})' \rangle \, \langle (\lambda_{m,t})_{(2)}, ((\lambda_{n,s})_{(2)})' \rangle \, v_l \otimes v_m \otimes v_n,
\end{aligned}$$

where in the last two steps we used the coproduct formula for representative forms. Similarly, the right hand side of the YBE takes the value

$$
\begin{aligned}
& \check{R}_{23} \circ \check{R}_{12} \circ \check{R}_{23}(v_s \otimes v_t \otimes v_u) \\
= & \sum_{i,j,k,l,m,n} r^{m,n}_{k,j}\, r^{l,k}_{s,i}\, r^{i,j}_{t,u}\; v_l \otimes v_m \otimes v_n \\
= & \sum_{i,j,k,l,m,n} \langle \lambda_{m,j}, (\lambda_{n,k})' \rangle\, \langle \lambda_{l,i}, (\lambda_{k,s})' \rangle\, \langle \lambda_{i,u}, (\lambda_{j,t})' \rangle\; v_l \otimes v_m \otimes v_n \\
= & \sum_{j,k,l,m,n} \langle \lambda_{m,j}, (\lambda_{n,k})' \rangle\, \langle \lambda_{l,u}, (\lambda_{k,s})'(\lambda_{j,t})' \rangle\; v_l \otimes v_m \otimes v_n \\
= & \sum_{l,m,n} \sum_{(\lambda_{m,t}),(\lambda_{n,s})} \langle (\lambda_{m,t})_{(1)}, ((\lambda_{n,s})_{(1)})' \rangle\, \langle \lambda_{l,u}, ((\lambda_{n,s})_{(2)})'((\lambda_{m,t})_{(2)})' \rangle\; v_l \otimes v_m \otimes v_n .
\end{aligned}
$$

The equality of the two sides of the Yang-Baxter equation then follows from the second formula of Lemma 4.30 above.

To prove that the associated braid group representation commutes with the action of $\mathcal{D}$, it is enough to show that on $V \otimes V$ the matrix $\check{R}$ commutes with the action of $\mathcal{D}$. Let $x \in \mathcal{D}$, and calculate on elementary tensors

$$
\begin{aligned}
x.\big(\check{R}(v_i \otimes v_j)\big) &= x.\Big(\sum_{k,l} \langle \lambda_{k,j}, (\lambda_{l,i})' \rangle\, v_k \otimes v_l\Big) \\
&= \sum_{(x)} \sum_{k,l} \langle \lambda_{k,j}, (\lambda_{l,i})' \rangle\, \big(x_{(1)}.v_k \otimes x_{(2)}.v_l\big) \\
&= \sum_{(x)} \sum_{k,l,m,n} \langle \lambda_{k,j}, (\lambda_{l,i})' \rangle\, \langle \lambda_{m,k}, x_{(1)} \rangle\, \langle \lambda_{n,l}, x_{(2)} \rangle\, v_m \otimes v_n \\
&= \sum_{(x)} \sum_{l,m,n} \langle \lambda_{m,j}, x_{(1)}\, (\lambda_{l,i})' \rangle\, \langle \lambda_{n,l}, x_{(2)} \rangle\, v_m \otimes v_n \\
&= \sum_{(x)} \sum_{(\lambda_{n,i})} \sum_{m,n} \langle \lambda_{m,j}, x_{(1)}\, ((\lambda_{n,i})_{(2)})' \rangle\, \langle (\lambda_{n,i})_{(1)}, x_{(2)} \rangle\, v_m \otimes v_n .
\end{aligned}
$$

This is to be compared with

$$
\begin{aligned}
\check{R}\big(x.(v_i \otimes v_j)\big) &= \sum_{(x)} \check{R}\big(x_{(1)}.v_i \otimes x_{(2)}.v_j\big) \\
&= \sum_{(x)} \sum_{k,l} \langle \lambda_{k,i}, x_{(1)} \rangle\, \langle \lambda_{l,j}, x_{(2)} \rangle\, \check{R}(v_k \otimes v_l) \\
&= \sum_{(x)} \sum_{k,l,m,n} \langle \lambda_{k,i}, x_{(1)} \rangle\, \langle \lambda_{l,j}, x_{(2)} \rangle\, \langle \lambda_{m,l}, (\lambda_{n,k})' \rangle\, v_m \otimes v_n \\
&= \sum_{(x)} \sum_{k,m,n} \langle \lambda_{k,i}, x_{(1)} \rangle\, \langle \lambda_{m,j}, (\lambda_{n,k})'\, x_{(2)} \rangle\, v_m \otimes v_n \\
&= \sum_{(x)} \sum_{(\lambda_{n,i})} \sum_{m,n} \langle (\lambda_{n,i})_{(2)}, x_{(1)} \rangle\, \langle \lambda_{m,j}, ((\lambda_{n,i})_{(1)})'\, x_{(2)} \rangle\, v_m \otimes v_n .
\end{aligned}
$$

The two expressions agree by virtue of Lemma 4.30. □

4.7 On the quantum group $\mathcal{U}_q(\mathfrak{sl}_2)$ at roots of unity

Throughout this section, let $q \notin \{+1, -1\}$ be a root of unity and denote by e the smallest positive integer such that $q^e \in \{+1, -1\}$.

A finite dimensional quotient when q is a root of unity

Exercise 49 (A finite dimensional quotient of $\mathcal{U}_q(\mathfrak{sl}_2)$ when q is a root of unity)

(a) Show that the elements E^e, K^e, F^e are central in $\mathcal{U}_q(\mathfrak{sl}_2)$.

(b) Let J be two sided ideal in the algebra $\mathcal{U}_q(\mathfrak{sl}_2)$ generated by the central elements E^e, F^e and $K^e - 1$. Show that J is a Hopf ideal in the Hopf algebra $\mathcal{U}_q(\mathfrak{sl}_2)$. Show that the quotient Hopf algebra $\widetilde{\mathcal{U}}_q(\mathfrak{sl}_2) = \mathcal{U}_q(\mathfrak{sl}_2) \,/\, J$ is finite dimensional.

Hint: *The formulas of Exercise 45 are useful.*

Exercise 50 (The center of $\widetilde{\mathcal{U}}_q(\mathfrak{sl}_2)$)
Assume that e is odd and satisfies $q^e = +1$. Let $A = \widetilde{\mathcal{U}}_q(\mathfrak{sl}_2)$ be the quotient of $\mathcal{U}_q(\mathfrak{sl}_2)$ by the relations $E^e = 0$, $F^e = 0$, $K^e = 1$ (see Exercise 49). A basis of A is

$$E^a\, F^b\, K^c \qquad \text{with} \qquad a, b, c \in \{0, 1, 2, \ldots, e-1\}\,.$$

(a) Show that the center of A is e-dimensional and a basis of the center is $1, C, C^2, C^3, \ldots, C^{e-1}$, where C is the quadratic Casimir

$$C \;=\; E\,F + \frac{1}{(q-q^{-1})^2}\Big(q^{-1}\,K + q\,K^{-1}\Big).$$

Hint: *This can be done in different ways, but one possible strategy is the following:*

- *Describe the subspace of elements commuting with K.*
- *Write down the condition for elements to commute with both K and F and from this argue that the dimension of the center is at most e.*
- *Argue that the powers of C are linearly independent central elements.*

(b) Show that the unit is the only grouplike central element in $\widetilde{\mathcal{U}}_q(\mathfrak{sl}_2)$.

Definition 4.32. Let A be a braided Hopf algebra with universal R-matrix $R \in A \otimes A$, and denote $R_{21} = S_{A,A}(R)$. Assume that there exists a central element $\theta \in A$ such that

$$\Delta(\theta) \;=\; (R_{21}\,R)^{-1}\,(\theta\otimes\theta) \qquad , \qquad \epsilon(\theta) \;=\; 1 \qquad \text{and} \qquad \gamma(\theta) \;=\; \theta.$$

Then A is said to be <u>ribbon Hopf algebra</u> and θ is called <u>ribbon element</u>.

Exercise 51 (Twists in modules over ribbon Hopf algebras)
Assume that A is a ribbon Hopf algebra and denote the braiding of A-modules V and W by $c_{V,W}$.

(a) Show that the ribbon element θ is invertible.

(b) For any A-module V define a linear map $\Theta_V : V \to V$ by $\Theta_V(v) = \theta^{-1}.v$ for all $v \in V$. Prove the following:

- *When $f : V \to W$ is an A-module map, we have $\Theta_W \circ f = f \circ \Theta_V$.*
- *When V is an A-module, and V^* is the dual A-module we have $\Theta_{V^*} = (\Theta_V)^*$ (the right hand side is the transpose of Θ_V).*
- *When V and W are A-modules, we have $\Theta_{V\otimes W} = (\Theta_V \otimes \Theta_W) \circ c_{W,V} \circ c_{V,W}$.*

Exercise 52 (The Hopf algebra $\widetilde{\mathcal{U}}_q(\mathfrak{sl}_2)$ is ribbon)
Let q be a root of unity, and assume that the smallest positive integer e such that $q^e \in \{\pm 1\}$ is odd and satisfies $q^e = +1$. Then

$$R \;=\; \frac{1}{e}\sum_{i,j,k=0}^{e-1} \frac{(q-q^{-1})^k}{[k]_q!}\, q^{k(k-1)/2+2k(i-j)-2ij}\; E^k K^i \otimes F^k K^j$$

is a universal R-matrix for $A = \widetilde{\mathcal{U}}_q(\mathfrak{sl}_2)$ *(see also Exercise 56).*

(a) *Show that* K *commutes with* $u = (\mu \circ (\gamma \otimes \mathrm{id}_A))(R_{21})$.

(b) *Show that* $\gamma(\gamma(x)) = K\,x\,K^{-1}$ *for all* $x \in A$*. Recalling a similar property of* u*, show that* $K^{-1}\,u$ *is a central element.*

(c) *Show that* $K^{-2}\,u\,\gamma(u^{-1})$ *is a grouplike central element. Conclude that* $\gamma(K^{-1}u) = K^{-1}u$.

(d) *Show that* $\theta = K^{-1}\,u$ *is a ribbon element.*

Representations at roots of unity

Recall that $q \in \mathbb{C}$ is assumed to be a root of unity and we denote by e the smallest positive integer such that $q^e \in \{+1, -1\}$.

Exercise 53 (Irreducible $\mathcal{U}_q(\mathfrak{sl}_2)$-modules of low dimension when q is a root of unity)
Consider the Hopf algebra $\mathcal{U}_q(\mathfrak{sl}_2)$.

(a) *For* $d < e$ *a positive integer and* $\varepsilon \in \{\pm 1\}$*, show that the formulas*

$$\begin{aligned} K.w_j &= \varepsilon\, q^{d-1-2j}\, w_j \\ F.w_j &= w_{j+1} \\ E.w_j &= \varepsilon\, [j]_q\, [d-j]_q\, w_{j-1} \end{aligned}$$

still define an irreducible $\mathcal{U}_q(\mathfrak{sl}_2)$*-module* W_d^{ε} *with basis* $w_0, w_1, w_2, \ldots, w_{d-1}$.

(b) *Show that any irreducible* $\mathcal{U}_q(\mathfrak{sl}_2)$*-module of dimension less than* e *is isomorphic to a module of the above type.*

Exercise 54 (No irreducible $\mathcal{U}_q(\mathfrak{sl}_2)$-modules of high dimension when q is a root of unity)
The goal of this exercise is to show that there are no irreducible $\mathcal{U}_q(\mathfrak{sl}_2)$*-modules of dimension greater than* e*. It is convenient to use a proof by contradiction. Therefore, in parts (a) and (b), suppose that* V *is an irreducible* $\mathcal{U}_q(\mathfrak{sl}_2)$*-module* V *with* $\dim V > e$.

(a) *If there exists a non-zero eigenvector* $v \in V$ *of* K *such that* $F.v = 0$*, then show that the linear span of* $v, E.v, E^2.v, \ldots, E^{e-1}.v$ *is a submodule of* V*. Conclude that this is not possible if* V *is irreducible and* $\dim V > e$.

(b) *If there doesn't exist any non-zero eigenvector* $v \in V$ *of* K *such that* $F.v = 0$*, then considering any non-zero eigenvector* $v \in V$ *of* K*, show that the linear span of* $v, F.v, F^2.v, \ldots, F^{e-1}.v$ *is a submodule of* V*. Conclude that this, too, is impossible if* V *is irreducible and* $\dim V > e$.

(c) *Conclude that there are no irreducible* $\mathcal{U}_q(\mathfrak{sl}_2)$*-modules of dimension greater than* e.

Hint for all parts of the exercise: *Recall that* K^e, E^e, F^e *are central by Exercise 49, and remember also the central element* $C = EF + \frac{1}{(q-q^{-1})^2}(q^{-1}K + qK^{-1})$.

Exercise 55 (A family of indecomposable $\mathcal{U}_q(\mathfrak{sl}_2)$-modules of dimension e when q is a root of unity)
Consider the Hopf algebra $\mathcal{U}_q(\mathfrak{sl}_2)$.

(a) *Let* $\mu, a, b \in \mathbb{C}$ *with* $\mu \neq 0$*. Show that the following formulas define an* e*-dimensional*

$\mathcal{U}_q(\mathfrak{sl}_2)$-module with basis $w_0, w_1, w_2, \ldots, w_{e-1}$:

$$\begin{aligned} K.w_j &= \mu\, q^{-2j}\, w_j && \text{for } 0 \le j \le e-1 \\ F.w_j &= w_{j+1} && \text{for } 0 \le j \le e-2 \\ F.w_{e-1} &= b\, w_0 \\ E.w_j &= \Big(ab + \frac{[j]_q}{q-q^{-1}}(\mu q^{1-j} - \mu^{-1} q^{j-1})\Big)\, w_{j-1} && \text{for } 1 \le j \le e-1 \\ E.w_0 &= a\, w_{e-1} \end{aligned}$$

Denote this module by $W_e(\mu; a, b)$.

(b) *Show that $W_e(\mu; a, b)$ is indecomposable, that is, it can not be written as a direct sum of two non-zero submodules.*

(c) *Show that $W_e(\mu; a, b)$ is irreducible unless $b = 0$ and $\mu \in \{\pm 1, \pm q, \pm q^2, \ldots, \pm q^{e-2}\}$.*

(d) *Consider the Hopf algebra $\widetilde{\mathcal{U}}_q(\mathfrak{sl}_2)$ which is the quotient of $\mathcal{U}_q(\mathfrak{sl}_2)$ by the ideal generated by E^e, F^e and $K^e - 1$ (cf. Exercise 49). A $\widetilde{\mathcal{U}}_q(\mathfrak{sl}_2)$-module can be thought of as a $\mathcal{U}_q(\mathfrak{sl}_2)$-module, where E^e, F^e and $K^e - 1$ act as zero. Show that a $\widetilde{\mathcal{U}}_q(\mathfrak{sl}_2)$-module V is irreducible if and only if it is irreducible as a $\mathcal{U}_q(\mathfrak{sl}_2)$-module.*

(e) *Consider the modules W_d^ε of Exercise 53, for $d < e$, and the modules $W_e(\mu; a, b)$. Find all values of d and ε, and of μ, a, b for which these are irreducible $\widetilde{\mathcal{U}}_q(\mathfrak{sl}_2)$-modules in each of the following cases:*

- *when e is odd and $q^e = +1$*
  (Answer: *d anything, $\varepsilon = +1$; $a = 0$, $b = 0$, $\mu = q^{-1}$; in fact $W_e(q^{-1}; 0, 0) \cong W_e^{+1}$*)
- *when e is odd and $q^e = -1$*
  (Answer: *d anything, $\varepsilon = (-1)^{d-1}$; $a = 0$, $b = 0$, $\mu = -q^{-1}$; in fact $W_e(-q^{-1}; 0, 0) \cong W_e^{+1}$*)
- *when e is even*
  (Answer: *d odd, ε anything; no possible values of μ, a, b*)

Exercise 56 (A solution of Yang-Baxter equation from two-dimensional $\widetilde{\mathcal{U}}_q(\mathfrak{sl}_2)$-modules)
Assume that $e > 1$, that e is odd and that $q^e = +1$. The finite dimensional algebra $\widetilde{\mathcal{U}}_q(\mathfrak{sl}_2)$ is generated by E, F, K with relations

$$\begin{aligned} KE &= q^2\, EK & KF &= q^{-2}\, FK & EF - FE &= \frac{1}{q-q^{-1}}\Big(K - K^{-1}\Big) \\ E^e &= 0 & F^e &= 0 & K^e &= 1. \end{aligned}$$

It can be shown that the Hopf algebra $\widetilde{\mathcal{U}}_q(\mathfrak{sl}_2)$ is braided with the universal R-matrix

$$R = \frac{1}{e} \sum_{i,j,k=0}^{e-1} \frac{(q-q^{-1})^k}{[k]_q!} q^{k(k-1)/2 + 2k(i-j) - 2ij}\, E^k K^i \otimes F^k K^j.$$

Let V be the two dimensional $\widetilde{\mathcal{U}}_q(\mathfrak{sl}_2)$-module W_2^{+1} with basis w_0, w_1 and calculate the matrix of

$$\check{R} = S_{V,V} \circ (\rho_V \otimes \rho_V)(R)$$

in the basis $w_0 \otimes w_0$, $w_0 \otimes w_1$, $w_1 \otimes w_0$, $w_1 \otimes w_1$.

Hint: *In the calculations one encounters expressions of type $\sum_{t=0}^{e-1} q^{ts}$, for $s \in \mathbb{Z}$, which can be simplified significantly when q is a root of unity of order e.*