from certain solutions of the Yang-Baxter equation. To this end, we introduce various classes of tensor categories that are responsible for the close relationship between quantum groups and knot theory. Part IV presents more advanced material: it is an account of Drinfeld's elegant treatment of the monodromy of the Knizhnik-Zamolodchikov equations. Our aim is to highlight Drinfeld's deep result expressing the braided tensor category of modules over a quantum enveloping algebra in terms of the corresponding semisimple Lie algebra. We conclude the book with the construction of a "universal knot invariant". This is a nice, far-reaching application of the algebraic techniques developed in the preceding chapters.

I wish to acknowledge the inspiration I drew during the composition of this text from [Dri87] [Dri89a] [Dri89b] [Dri90] by Drinfeld, [JS93] by Joyal and Street, [Tur89] [RT90] by Reshetikhin and Turaev. After having become acquainted with quantum groups, the reader is encouraged to return to these original sources. Further references are given in the notes at the end of each chapter. Lusztig's and Turaev's monographs [Lus93] [Tur94] may complement our exposition advantageously.

This book grew out of two graduate courses I taught at the Department of Mathematics of the Université Louis Pasteur in Strasbourg during the years 1990–92. Part I is the expanded English translation of [Kas92]. It is a pleasure to express my thanks to C. Bennis, R. Berger, C. Mitschi, P. Nuss, C. Reutenauer, M. Rosso, V. Turaev, M. Wambst for valuable discussions and comments, and to Raymond Séroul who coded the figures. I owe special thanks to Patrick Ion for his marvellous job in preparing the book for printing, with his attention to mathematical, English, typographical, and computer details.

Christian Kassel
March 1994, Strasbourg

Notation. — Throughout the text, k is a field and the words "vector space", "linear map" mean respectively "k-vector space" and "k-linear map". The boldface letters $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ stand successively for the nonnegative integers, all integers, the field of rational, real, and complex numbers. The Kronecker symbol δ_{ij} is defined by $\delta_{ij} = 1$ if $i = j$ and is zero otherwise. We denote the symmetric group on n letters by S_n. The sign of a permutation σ is indicated by $\varepsilon(\sigma)$.

The symbol $\square$ indicates the end of a proof. Roman figures refer to the numbering of the chapters.

Contents

Chapter I
Preliminaries

The goal of this first chapter is the construction of polynomial algebras $GL(2)$ and $SL(2)$ modelling the 2×2-matrices with invertible determinant [resp. with determinant equal to 1]. The multiplication of matrices induces an additional structure on these algebras. This structure is one of the basic ingredients of what will be called a Hopf algebra in Chapter III. We complete the chapter with various concepts of ring theory to be used in the sequel. The ground field is denoted by k.

I.1 Algebras and Modules

We recall some facts on algebras and modules.

An *algebra* is a ring A together with a ring map $\eta_A : k \to A$ whose image is contained in the centre of A. The map $(\lambda, a) \mapsto \eta_A(\lambda)a$ from $k \times A$ to A equips A with a vector space structure over k and the multiplication map $\mu_A : A \times A \to A$ is bilinear.

A *morphism of algebras* or an *algebra morphism* is a ring map $f : A \to B$ such that

$$f \circ \eta_A = \eta_B. \tag{1.1}$$

As a consequence of (1.1), f preserves the units, i.e., we have $f(1) = 1$. The linear map $\eta_A : k \to A$ is a morphism of algebras. If $i : A \to B$ is an injective algebra morphism, we say that A is a *subalgebra* of the algebra B.

Let us denote by $\mathrm{Hom}_{Alg}(A, B)$ the set of algebra morphisms from A to B. In general, this set has no further structure. Nevertheless, we shall soon see how to put a group structure on $\mathrm{Hom}_{Alg}(A, B)$ when A and B satisfy some additional hypotheses.

We give a few examples of algebras that will be used frequently in this book.

1. Given an algebra A, we define the *opposite algebra* A^{op} as the algebra with the same underlying vector space as A, but with multiplication defined by

$$\mu_{A^{\mathrm{op}}} = \mu_A \circ \tau_{A,A} \tag{1.2}$$

where $\tau_{A,A}$ is the *flip* switching the two factors of $A \times A$. In other words,

$$\mu_{A^{\mathrm{op}}}(a, a') = a'a. \tag{1.3}$$

An algebra A is *commutative* if and only if

$$\mu_{A^{\mathrm{op}}} = \mu_A. \tag{1.4}$$

2. The *centre* $Z(A)$ of an algebra A is the subalgebra

$$\{a \in A \mid aa' = a'a \text{ for all } a' \in A\}.$$

We have $Z(A) = Z(A^{\mathrm{op}})$.

3. If I is a two-sided ideal of an algebra A, i.e., a subspace of A such that

$$\mu_A(I \times A) \subset I \supset \mu_A(A \times I),$$

then there exists a unique algebra structure on the quotient vector space A/I such that the canonical projection from A onto A/I is a morphism of algebras.

4. We endow the product set $A = \prod_{i \in I} A_i$ of a family $(A_i)_{i \in I}$ of algebras with the unique algebra structure such that the canonical projection from A to A_i is an algebra morphism for all $i \in I$. The algebra A is called the *product algebra* of the family $(A_i)_{i \in I}$.

5. Given an algebra A we can form the algebra $A[x]$ of all polynomials $\sum_{i=0}^{n} a_i x^i$ where n is any non-negative integer and the algebra $A[x, x^{-1}]$ of all Laurent polynomials $\sum_{i=m}^{n} a_i x^i$ where $m, n \in \mathbf{Z}$.

6. For any positive integer n we denote by $M_n(A)$ the algebra of all $n \times n$-matrices with entries in A.

7. The space $\mathrm{End}(V)$ of linear endomorphisms of a vector space V is an algebra with product given by the composition and unit by the identity map id_V of V.

Given an algebra A, a *left A-module* or, simply, an *A-module* is a vector space V together with a bilinear map $(a, v) \mapsto av$ from $A \times V$ to V such that

$$a(a'v) = (aa')v \quad \text{and} \quad 1v = v \tag{1.5}$$

for all $a, a' \in A$ and $v \in V$. One similarly defines a right A-module using a bilinear map from $V \times A$ to V. A right A-module is nothing else than a left module over the opposite algebra A^{op}. Therefore we need only consider left modules which shall for simplicity be called modules in the sequel.

If V and V' are A-modules, a linear map $f : V \to V'$ is said to be *A-linear* or a *morphism of A-modules* if

$$f(av) = af(v) \tag{1.6}$$

for all $a \in A$ and $v \in V$.

An *A-submodule* V' of an A-module V is a subspace of V with an A-module structure such that the inclusion of V' into V is A-linear.

The action of A on an A-module V defines an algebra morphism ρ from A to $\mathrm{End}(V)$ by

$$\rho(a)(v) = av. \tag{1.7}$$

The map ρ is called a *representation* of A on V.

Given A-modules $V_1, \dots, V_n$, the direct sum $V_1 \oplus \cdots \oplus V_n$ has an A-module structure given by

$$a(v_1, \dots, v_n) = (av_1, \dots, av_n) \tag{1.8}$$

where $a \in A$, $v_1 \in V_1, \dots, v_n \in V_n$. These definitions lead us to the following ones.

Definition I.1.1. *An A-module V is simple if it has no other submodules than $\{0\}$ and V. It is semisimple if it is isomorphic to a direct sum of simple A-modules. It is indecomposable if it is not isomorphic to the direct sum of two non-zero submodules.*

In the language of representations, a simple module [resp. a semisimple module] is an *irreducible* representation [resp. a *completely reducible* representation]. The following well-known proposition will be used in Chapters V–VII.

Proposition I.1.2. *The following statements are equivalent.*

(i) *For any pair $V' \subset V$ of finite-dimensional A-modules, there exists an A-module V'' such that $V \cong V' \oplus V''$.*

(ii) *For any pair $V' \subset V$ of finite-dimensional A-modules where V' is simple, there exists an A-module V'' such that $V \cong V' \oplus V''$.*

(iii) *For any pair $V' \subset V$ of finite-dimensional A-modules, there exists an A-linear map $p : V \to V'$ with $p^2 = p$.*

(iv) *For any pair $V' \subset V$ of finite-dimensional A-modules where V' is simple, there exists an A-linear map $p : V \to V'$ with $p^2 = p$.*

(v) *Any finite-dimensional A-module is semisimple.*

PROOF. Clearly, (i) $\Rightarrow$ (ii) and (iii) $\Rightarrow$ (iv). We also have (i) $\Rightarrow$ (iii): it suffices to define p as the canonical projection from $V' \oplus V''$ onto V'. Similarly, (ii) $\Rightarrow$ (iv).

Assertion (iii) $\Rightarrow$ Assertion (i). Let $V'' = \mathrm{Ker}\,(p)$; it is a submodule of V. The relations $v = p(v) + (v - p(v))$ and $p^2 = p$ prove that V is the direct sum V' and V''. Similarly, (iv) $\Rightarrow$ (ii).

Assertion (ii) $\Rightarrow$ Assertion (v). Assuming (ii), we have to prove that any finite-dimensional A-module V is semisimple. We may also assume that $\dim(V) > 0$. Consider a non-zero submodule V_1 of V of minimal dimension; it has to be simple. By (ii) there exists a submodule V^1 such that $V \cong V_1 \oplus V^1$ and $\dim(V^1) < \dim(V)$. Iterating this procedure, we build a sequence $(V_n)_{n>0}$ of simple submodules and a sequence $(V^n)_{n>0}$ of submodules such that

$$V^n \cong V_{n+1} \oplus V^{n+1} \quad \text{and} \quad \dim(V^{n+1}) < \dim(V^n).$$

Since the dimension of V^n is strictly decreasing, there exists an integer p such that $V^p = \{0\}$. The module V is a direct sum of simple modules: $V \cong V_1 \oplus \cdots \oplus V_p$.

It remains to be shown that Assertion (v) implies Assertion (i). Let $V' \subset V$ be a pair of finite-dimensional A-modules. By (v)

$$V = \bigoplus_{i \in I} V_i$$

is a direct sum over a finite index set I of simple submodules V_i. Let J be a maximal subset of I such that

$$V' \cap (\bigoplus_{j \in J} V_j) = \{0\}. \tag{1.9}$$

If $i \notin J$, then

$$V' \cap (V_i \oplus \bigoplus_{j \in J} V_j) \neq \{0\},$$

hence

$$V_i \cap (V' + \bigoplus_{j \in J} V_j) \neq \{0\}.$$

Since V_i is simple, this implies that

$$V_i \subset V' + \bigoplus_{j \in J} V_j$$

for all $i \notin J$. This holds also for all $i \in J$. Consequently, for the sum V of all V_i we must have

$$V = V' + \bigoplus_{j \in J} V_j. \tag{1.10}$$

As a consequence of (1.9–1.10), we get $V = V' \oplus V''$ where V'' is the submodule $\oplus_{j \in J} V_j$. □

I.2 Free Algebras

Let X be a set. Consider the vector space $k\{X\}$ with basis the set of all words $x_{i_1} \ldots x_{i_p}$ in the alphabet X, including the empty word $\emptyset$. A word will be called a monomial. Define the degree of the monomial $x_{i_1} \ldots x_{i_p}$ as its length p. *Concatenation* of words defines a multiplication on $k\{X\}$ by

$$(x_{i_1} \ldots x_{i_p})(x_{i_{p+1}} \ldots x_{i_n}) = x_{i_1} \ldots x_{i_p} x_{i_{p+1}} \ldots x_{i_n}. \tag{2.1}$$

Formula (2.1) equips $k\{X\}$ with an algebra structure, called the *free algebra* on the set X. The unit is the empty word: $1 = \emptyset$. In the sequel we shall mainly consider free algebras on finite sets. If $X = \{x_1, \ldots, x_n\}$ we also denote $k\{X\}$ by $k\{x_1, \ldots, x_n\}$.

Free algebras have the following universal property.

Proposition I.2.1. *Let X be a set. Given an algebra A and a set-theoretic map f from X to A, there exists a unique algebra morphism $\bar{f} : k\{X\} \to A$ such that $\bar{f}(x) = f(x)$ for all $x \in X$.*

PROOF. It is enough to define $\bar{f}$ on any word of X. For the empty word we set $\bar{f}(\emptyset) = 1$. Otherwise, if $x_{i_1}, \ldots, x_{i_p}$ are elements of X, we define

$$\bar{f}(x_{i_1} \ldots x_{i_p}) = f(x_{i_1}) \ldots f(x_{i_p}).$$

The rest of the proof follows easily. □

An equivalent formulation of Proposition 2.1 is: There exists a natural bijection

$$\mathrm{Hom}_{Alg}(k\{X\}, A) \cong \mathrm{Hom}_{Set}(X, A) \tag{2.2}$$

where $\mathrm{Hom}_{Set}(X, A)$ is the set of all set-theoretic maps from X to A. In particular, if X is the finite set $\{x_1, \ldots, x_n\}$, then $f \mapsto (f(x_1), \ldots, f(x_n))$ induces a bijection

$$\mathrm{Hom}_{Alg}(k\{x_1, \ldots, x_n\}, A) \cong A^n. \tag{2.3}$$

Any algebra A is the quotient of a free algebra $k\{X\}$. It suffices to take any generating set X for the algebra A (for instance $X = A$). Consequently, $A = k\{X\}/I$ where I is a two-sided ideal of $k\{X\}$. In this case, for any algebra A' we have the natural bijection

$$\mathrm{Hom}_{Alg}(k\{X\}/I, A') \cong \{f \in \mathrm{Hom}_{Set}(X, A') \mid \bar{f}(I) = 0\}. \tag{2.4}$$

Example 1. Let I be the two-sided ideal of $k\{x_1, \ldots, x_n\}$ generated by all elements of the form $x_i x_j - x_j x_i$ where i, j run over all integers from 1 to n. The quotient-algebra $k\{x_1, \ldots, x_n\}/I$ is isomorphic to the polynomial algebra $k[x_1, \dots, x_n]$ in n variables with coefficients in the ground field k. As a corollary of (2.4) we have

$$\mathrm{Hom}_{Alg}(k[x_1, \dots, x_n], A) \cong \{(a_1, \dots, a_n) \in A^n \mid a_i a_j = a_j a_i \text{ for all } (i,j)\} \tag{2.5}$$

for any algebra A.

In the next sections we shall see more examples where families of elements subject to "universal" algebraic relations are represented by quotients of free algebras.

I.3 The Affine Line and Plane

Let us restrict to commutative algebras. As a consequence of (2.5) we have the following proposition.

Proposition I.3.1. *Let A be a commutative algebra and f be a set-theoretic map from the finite set $\{x_1, \dots, x_n\}$ to A. There exists a unique morphism of algebras $\bar{f}$ from $k[x_1, \dots, x_n]$ to A such that $\bar{f}(x_i) = f(x_i)$ for all i.*

In other words, giving an algebra morphism from the polynomial algebra $k[x_1, \dots, x_n]$ to a *commutative* algebra A is equivalent to giving an n-tuple $(a_1, \dots, a_n)$ of elements of A:

$$\mathrm{Hom}_{Alg}(k[x_1, \dots, x_n], A) \cong A^n. \tag{3.1}$$

Let us consider the special case $n = 1$ of (3.1). For any commutative algebra A the underlying set A is in bijection with the set $\mathrm{Hom}_{Alg}(k[x], A)$:

$$\mathrm{Hom}_{Alg}(k[x], A) \cong A. \tag{3.2}$$

The algebra $k[x]$ is called the *affine line* and the set $\mathrm{Hom}_{Alg}(k[x], A)$ is called the set of A-points of the affine line. Now A has an abelian group structure. We wish to express it in a universal way using the affine line $k[x]$. The abelian group structure of A consists of three maps, namely the addition $+ : A^2 \to A$, the unit $0 : \{0\} \to A$, and the inverse $- : A \to A$, satisfying the well-known axioms which express the fact that the addition is associative and commutative, that it has 0 as a left and right unit and that

$$(-a) + a = a + (-a) = 0$$

for all $a \in A$. These laws do not depend on the particular commutative algebra A. It will therefore be possible to express them universally.

To this end, let us introduce the *affine plane* $k[x', x'']$ with the bijection

$$\mathrm{Hom}_{Alg}(k[x', x''], A) \cong A^2 \tag{3.3}$$

obtained from (3.1) for $n = 2$. An element of $\mathrm{Hom}_{Alg}(k[x', x''], A)$ is called an A-point of the affine plane. The set $\mathrm{Hom}_{Alg}(k, A)$, reduced to the single point η_A, will be denoted by $\{0\}$.

Proposition I.3.2. *Let $\Delta : k[x] \to k[x', x'']$, $\varepsilon : k[x] \to k$, $S : k[x] \to k[x]$ be the algebra morphisms defined by*

$$\Delta(x) = x' + x'', \quad \varepsilon(x) = 0, \quad S(x) = -x.$$

Under the identifications (3.2–3.3), the morphisms Δ, ε and S correspond to the maps $+$, 0 and $-$ respectively.

PROOF. Left to the reader. □

The morphisms Δ, ε and S are subject to further relations which express the associativity, the commutativity, the unit and the inverse axioms of an abelian group. They equip the affine line $k[x]$ with what will be called a cocommutative Hopf algebra structure in Chapter III.

In order to illustrate better the phenomenon we have just observed, we give another example. For any algebra A denote by $A^\times$ the group of invertible elements of A. We represent the set $A^\times$ by an algebra as above. Consider the ideal I of $k[x, y]$ generated by $xy - 1$. For any commutative algebra A we have

$$\mathrm{Hom}_{Alg}(k[x, y]/I, A) \cong A^\times. \tag{3.4}$$

The set $\{x^k\}_{k \in \mathbf{Z}}$ is a basis of the vector space $k[x, y]/I$. We denote this algebra by $k[x, x^{-1}]$; it is the algebra of Laurent polynomials in one variable. One defines similarly the algebra

$$k[x', x'', x'^{-1}, x''^{-1}] = k[x', y', x'', y'']/(x'y' - 1, x''y'' - 1)$$

of Laurent polynomials in two variables. We have a bijection

$$\mathrm{Hom}_{Alg}(k[x', x'^{-1}, x'', x''^{-1}], A) \cong A^\times \times A^\times. \tag{3.5}$$

Define algebra morphisms

$$\Delta : k[x, x^{-1}] \to k[x', x'^{-1}, x'', x''^{-1}], \quad \varepsilon : k[x, x^{-1}] \to k,$$

$$S : k[x, x^{-1}] \to k[x, x^{-1}]$$

by

$$\Delta(x) = x'x'', \quad \varepsilon(x) = 1, \quad S(x) = x^{-1}. \tag{3.6}$$

Then the morphisms Δ, ε and S correspond respectively to the multiplication in $A^\times$, to the unit 1 and to the inverse under the identifications (3.4–3.5). Here again, the morphisms Δ, ε, S equip $k[x, x^{-1}]$ with a cocommutative Hopf algebra structure.

I.4 Matrix Multiplication

For any algebra A we denote by $M_2(A)$ the algebra of 2×2-matrices with entries in A. As a set, $M_2(A)$ is in bijection with the set A^4 of 4-tuples of A. By (3.1) we have a natural bijection

$$\mathrm{Hom}_{Alg}(M(2), A) \cong M_2(A) \tag{4.1}$$

for any commutative algebra A where $M(2)$ is defined as the polynomial algebra $k[a,b,c,d]$. This bijection maps an algebra morphism $f : M(2) \to A$ to the matrix

$$\begin{pmatrix} f(a) & f(b) \\ f(c) & f(d) \end{pmatrix}.$$

The multiplication of matrices is a map $M_2(A) \times M_2(A) \to M_2(A)$ we wish to represent universally on $M(2)$, in the spirit of Section 3. The set $M_2(A) \times M_2(A)$ being in bijection with A^8, we introduce the polynomial algebra

$$M(2)^{\otimes 2} = k[a', a'', b', b'', c', c'', d', d''] . \tag{4.2}$$

Proposition I.4.1. *Let $\Delta : M(2) \to M(2)^{\otimes 2}$ be the algebra morphism defined by*

$$\begin{array}{ll} \Delta(a) = a'a'' + b'c'', & \Delta(b) = a'b'' + b'd'', \\ \Delta(c) = c'a'' + d'c'', & \Delta(d) = c'b'' + d'd''. \end{array}$$

Then for any commutative algebra A, the morphism Δ corresponds to the matrix multiplication in $M_2(A)$ under the identifications (4.1–4.2).

The proof is easy and left to the reader. It is convenient to rewrite the formulas for Δ in Proposition 4.1 in the compact matrix form

$$\Delta \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \Delta(a) & \Delta(b) \\ \Delta(c) & \Delta(d) \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}. \tag{4.3}$$

I.5 Determinants and Invertible Matrices

We keep the notations of the previous section. We now consider the group $GL_2(A)$ of invertible matrices of the matrix algebra $M_2(A)$. When A is commutative, we know that a matrix is invertible if and only if its determinant is invertible in A:

$$GL_2(A) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(A) \text{ such that } \alpha\delta - \beta\gamma \in A^\times \right\}.$$

Define $SL_2(A)$ as the subgroup of $GL_2(A)$ of matrices with determinant $\alpha\delta - \beta\gamma = 1$.

Proposition I.5.1. *Define the commutative algebras*

$$GL(2) = M(2)[t]/((ad - bc)t - 1)$$

and

$$SL(2) = GL(2)/(t - 1) = M(2)/(ad - bc - 1).$$

For any commutative algebra A there are bijections

$$\mathrm{Hom}_{Alg}(GL(2), A) \cong GL_2(A) \quad \text{and} \quad \mathrm{Hom}_{Alg}(SL(2), A) \cong SL_2(A) \tag{5.1}$$

sending an algebra morphism f to the matrix

$$\begin{pmatrix} f(a) & f(b) \\ f(c) & f(d) \end{pmatrix}.$$

Proof. We give it only for $GL(2)$. Similar arguments work for $SL(2)$. Let $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ be a matrix in $GL_2(A)$. Since A is commutative, there exists a unique algebra morphism $f : M(2)[t] \to A$ such that

$$f(a) = \alpha, \quad f(b) = \beta, \quad f(c) = \gamma, \quad f(d) = \delta \quad \text{and} \quad f(t) = (\alpha\delta - \beta\gamma)^{-1}.$$

Now,

$$\begin{aligned} f\big((ad - bc)t - 1\big) &= \big(f(a)f(d) - f(b)f(c)\big)f(t) - f(1) \\ &= (\alpha\delta - \beta\gamma)(\alpha\delta - \beta\gamma)^{-1} - 1 \\ &= 0. \end{aligned}$$

This implies that the morphism f factors through the quotient algebra $GL(2)$. The rest of the proof is easy. □

The next lemma follows from a straightforward computation using the morphism Δ of Proposition 4.1.

Lemma I.5.2. *We have* $\Delta(ad - bc) = (a'd' - b'c')(a''d'' - b''c'')$.

We now lift the group structures of $GL_2(A)$ and of $SL_2(A)$ to the algebras $GL(2)$ and $SL(2)$. Consider the commutative algebras

$$GL(2)^{\otimes 2} = M(2)^{\otimes 2}[t', t'']/((a'd' - b'c')t' - 1, (a''d'' - b''c'')t'' - 1)$$

and

$$SL(2)^{\otimes 2} = GL(2)^{\otimes 2}/(t' - 1, t'' - 1) = M(2)^{\otimes 2}/(a'd' - b'c' - 1, a''d'' - b''c'' - 1).$$

Proposition I.5.3. *The formulas of Proposition 4.1 define algebra morphisms*

$$\Delta : GL(2) \to GL(2)^{\otimes 2} \quad \text{and} \quad \Delta : SL(2) \to SL(2)^{\otimes 2}.$$

PROOF. The formulas of Proposition 4.1 define an algebra morphism Δ from $M(2)[t]$ to $GL(2)^{\otimes 2}$ provided we set $\Delta(t) = t't''$. In order to show that Δ factors through $GL(2)$ we have to check that $\Delta((ad-bc)t-1)$ vanishes. Now, by Lemma 5.2 and by definition of $GL(2)^{\otimes 2}$, we have

$$\begin{aligned}\Delta((ad-bc)t-1) &= (a'd'-b'c')(a''d''-b''c'')t't''-1\\ &= 1.1-1=0.\end{aligned}$$

The proof for $SL(2)$ is similar. □

In Section 4 we checked that the map Δ corresponded to matrix multiplication under the above identifications. Let us exhibit the algebra maps

$$\varepsilon : GL(2) \to k \quad \text{and} \quad \varepsilon : SL(2) \to k$$

corresponding to the units of the groups $GL_2(A)$ and $SL_2(A)$ and the algebra morphisms

$$S : GL(2) \to GL(2) \quad \text{and} \quad S : SL(2) \to SL(2)$$

corresponding to the inversions in the same groups. They are defined by the formulas

$$\varepsilon(a) = \varepsilon(d) = \varepsilon(t) = 1, \qquad \varepsilon(b) = \varepsilon(c) = 0,$$

$$S(a) = (ad-bc)^{-1}\,d, \qquad S(b) = -(ad-bc)^{-1}\,b,$$

$$S(c) = -(ad-bc)^{-1}\,c, \qquad S(d) = (ad-bc)^{-1}\,a,$$

and $S(t) = t^{-1} = ad - bc$. We rewrite them in the more compact and illuminating form

$$\varepsilon\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } S\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ad-bc)^{-1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}. \tag{5.2}$$

I.6 Graded and Filtered Algebras

The remaining sections of this chapter are devoted to some concepts of ring theory.

Definition I.6.1. *An algebra A is graded if there exist subspaces $(A_i)_{i\in\mathbf{N}}$ such that*

$$A = \bigoplus_{i\in\mathbf{N}} A_i \qquad \textit{and} \qquad A_i \cdot A_j \subset A_{i+j}$$

for all $i, j \in \mathbf{N}$. The elements of A_i are said to be homogeneous of degree i.

We always assume that the unit 1 of a graded algebra belongs to A_0.

Example 1. Free algebras are graded by the length of words, i.e., the subspace A_i of $A = k\{X\}$ is defined as the subspace linearly generated by all monomials of degree i. The elements of X are of degree 1.

Proposition I.6.2. *Let $A = \bigoplus_{i\geq 0} A_i$ be a graded algebra and I be a two-sided ideal generated by homogeneous elements. Then*

$$I = \bigoplus_{i\geq 0} I \cap A_i$$

and the quotient algebra A/I is graded with $(A/I)_i = A_i/(I\cap A_i)$ for all i.

PROOF. It suffices to show that $I = \bigoplus_{i\geq 0} I\cap A_i$. First observe that the sum has to be direct since the subspaces A_i form a direct sum. Therefore, it remains to be checked that $I = \sum_{i\geq 0} I \cap A_i$. The ideal I is generated by homogeneous elements x_i of degree d_i. Consequently, if $x \in I$ then

$$x = \sum_i a_i x_i b_i$$

for some $a_i, b_i \in A$. Now, $a_i = \sum_j a_i^j$ and $b_i = \sum_j b_i^j$, where a_i^j and b_i^j are homogeneous elements of degree j. It follows that

$$x = \sum_{i,j,k} a_i^j x_i b_i^k$$

is a sum of homogeneous elements of degree $d_i + j + k$ in I. This implies that I is a subspace of $\sum_{i\geq 0} I \cap A_i$. The converse inclusion is clear. □

Example 2. The polynomial algebra $k[x_1, \ldots, x_n]$ is graded as the quotient of the free algebra $A = k\{x_1, \ldots, x_n\}$ (graded as in Example 1) by the ideal I generated by the degree-2 homogeneous elements $x_i x_j - x_j x_i$ where i and j run over all integers between 1 and n. The generators $x_1, \ldots, x_n$ are of degree one.

The algebras $M(2)$ and $M(2)^{\otimes 2}$ of Section 4 are graded as polynomial algebras. On the contrary, the ideals defining the algebras $GL(2)$ and $SL(2)$ are not generated by homogeneous elements. Though not graded, $GL(2)$ and $SL(2)$ are filtered algebras in the sense of the following definition.

Definition I.6.3. *An algebra A is filtered if there exists an increasing sequence $\{0\} \subset F_0(A) \subset \ldots \subset F_i(A) \subset \ldots \subset A$ of subspaces of A such that*

$$A = \bigcup_{i\geq 0} F_i(A) \quad \textit{and} \quad F_i(A)\cdot F_j(A) \subset F_{i+j}(A).$$

The elements of $F_i(A)$ are said to be of degree $\leq i$.

For any filtered algebra A there exists a graded algebra $S = \mathrm{gr}(A)$ defined by

$$S_i = F_i(A)/F_{i-1}(A).$$

We give a few examples of filtered algebras.

Example 3. Any algebra A has a trivial filtration given by $F_i(A) = A$ for all i.

Example 4. We filter any graded algebra $A = \bigoplus_{i\geq 0} A_i$ by

$$F_i(A) = \bigoplus_{0\leq j\leq i} A_j$$

for all $i \in \mathbf{N}$. We have $\mathrm{gr}(A) = A$.

Example 5. Let $A \supset \ldots \supset F_1(A) \supset F_0(A)$ be a filtered algebra and I be a two-sided ideal of A. The quotient-algebra A/I is filtered with

$$F_i(A/I) = F_i(A)/F_i(A) \cap I.$$

In this case we have

$$\mathrm{gr}(A/I) = \bigoplus_{i\geq 0} F_i(A)/(F_{i-1}(A) + F_i(A) \cap I).$$

As a special case, consider the algebra $SL(2)$. It is filtered as the quotient of the graded algebra $M(2)$. We have

$$\mathrm{gr}(SL(2)) \cong k[a, b, c, d,]/(ad - bc).$$

I.7 Ore Extensions

Let R be an algebra and $R[t]$ be the free (left) R-module consisting of all polynomials of the form

$$P = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0 t^0$$

with coefficients in R. If $a_n \neq 0$, we say that the degree $\deg(P)$ of P is equal to n; by convention, we set $\deg(0) = -\infty$. The aim of this section is to find all algebra structures on $R[t]$ compatible with the algebra structure on R and with the degree. We need the following definition.

Let α be an algebra endomorphism of R. An *α-derivation* of R is a linear endomorphism δ of R such that

$$\delta(ab) = \alpha(a)\delta(b) + \delta(a)b \tag{7.1}$$

for all $a, b \in R$. Observe that (7.1) implies $\delta(1) = 0$.

Theorem I.7.1. (a) *Assume that $R[t]$ has an algebra structure such that the natural inclusion of R into $R[t]$ is a morphism of algebras, and we have $\deg(PQ) = \deg(P) + \deg(Q)$ for any pair (P, Q) of elements of $R[t]$. Then R has no zero-divisors and there exist a unique injective algebra endomorphism α of R and a unique α-derivation δ of R such that*

$$ta = \alpha(a)t + \delta(a) \tag{7.2}$$

for all $a \in R$.

(b) *Conversely, let R be an algebra without zero-divisors. Given an injective algebra endomorphism α of R and an α-derivation δ of R, there exists a unique algebra structure on $R[t]$ such that the inclusion of R into $R[t]$ is an algebra morphism and Relation (7.2) holds for all a in R.*

The algebra defined by Theorem 7.1 (b), denoted $R[t, \alpha, \delta]$, is called the *Ore extension* attached to the data (R, α, δ).

Proof. (a) Let a, b be non-zero elements of R, hence of degree 0 in $R[t]$. We have $\deg(ab) = \deg(a) + \deg(b) = 0$, which implies that $ab \neq 0$. Consequently, R has no zero-divisors.

Let us now prove the existence and the uniqueness of the endomorphisms α and δ. Take any non-zero element a of R and consider the product ta. We have $\deg(ta) = \deg(t) + \deg(a) = 1$. By definition of $R[t]$ there exist uniquely determined elements $\alpha(a) \neq 0$ and $\delta(a)$ of R such that

$$ta = \alpha(a)t + \delta(a). \tag{7.2}$$

This defines maps α and δ in a unique fashion. The left multiplication by t being linear, so are α and δ. Furthermore, α has to be injective. Let us expand both sides of the equality $(ta)b = t(ab)$ in $R[t]$ using (7.2). Here a and b are elements of R. We get

$$\alpha(a)\alpha(b)t + \alpha(a)\delta(b) + \delta(a)b = \alpha(ab)t + \delta(ab). \tag{7.3}$$

Relation (7.3) implies that

$$\alpha(ab) = \alpha(a)\alpha(b) \quad \text{and} \quad \delta(ab) = \alpha(a)\delta(b) + \delta(a)b. \tag{7.4}$$

Applying (7.2) to $t1 = t$ yields $\alpha(1) = 1$ and $\delta(1) = 0$. It follows that α is an injective algebra endomorphism and δ is an α-derivation.

(b) It clearly suffices to know the product ta for any $a \in R$ in order to determine the product on $R[t]$ completely. Thus, (7.2) defines the algebra structure on $R[t]$ uniquely.

Let us now prove the existence of the algebra structure. To this end, we shall embed $R[t]$ into the associative algebra $\mathcal{M}$ consisting of all infinite matrices $(f_{ij})_{i,j\geq 1}$ with entries in the algebra $\mathrm{End}(R)$ of linear endomorphisms of R such that each row, as well as each column, has only finitely many non-zero entries. The unit of $\mathcal{M}$ is the infinite diagonal matrix I with identities on the diagonal. Given an element a of R, we denote by $\widehat{a} \in \mathrm{End}(R)$ the left multiplication by a. The hypotheses made on α and δ translate into the relations

$$\alpha\widehat{a} = \widehat{\alpha(a)}\alpha \quad \text{and} \quad \delta\widehat{a} = \widehat{\alpha(a)}\delta + \widehat{\delta(a)} \tag{7.5}$$

in $\mathrm{End}(R)$. Now, consider the infinite matrix

$$T = \begin{pmatrix} \delta & 0 & 0 & 0 & \cdots \\ \alpha & \delta & 0 & 0 & \cdots \\ 0 & \alpha & \delta & 0 & \cdots \\ 0 & 0 & \alpha & \delta & \cdots \\ 0 & 0 & 0 & \alpha & \ddots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

in $\mathcal{M}$. It allows one to define a linear map $\Phi : R[t] \to \mathcal{M}$ by

$$\Phi\Big(\sum_{i=0}^{n} a_i t^i\Big) = \sum_{i=0}^{n} (\widehat{a}_i I) T^i. \tag{7.6}$$

Lemma I.7.2. *The map Φ is injective.*

PROOF. For any integer $i \geq 1$, let e_i be the infinite column vector whose entries are all zero, except for the i-th one which is equal to the unit 1 of R. We may apply the matrix T of endomorphisms to e_i. Since $\delta(1) = 0$ and $\alpha(1) = 1$ we get

$$T(e_i) = e_{i+1} \tag{7.7}$$

for all $i \geq 1$. Now, let $P = \sum_{i=0}^{n} a_i t^i$ be an element of $R[t]$ such that $\Phi(P) = 0$. We wish to show that all elements $a_0, \ldots, a_n$ are zero. Apply $\Phi(P)$ to the vector column e_1. By (7.7) we get

$$0 = \Phi(P)(e_1) = \sum_{i=0}^{n} (\widehat{a}_i I) T^i(e_1) = \sum_{i=0}^{n} \widehat{a}_i e_{i+1}.$$

The set $\{e_i\}_{i \geq 1}$ being free, we have $\widehat{a}_i = 0$ for all i. Since R has a unit, we get $a_i = 0$ for all i. Hence, $P = 0$. □

Relations (7.5) imply the following relation in $\mathcal{M}$ for all $a \in R$.

Lemma I.7.3. *We have $T(\widehat{a}I) = (\widehat{\alpha(a)}I)T + (\widehat{\delta(a)}I)$.*

We now complete the proof of Theorem 7.1 (b). Let S be the subalgebra of $\mathcal{M}$ generated by the elements T and $\widehat{a}I$ where a runs over R. By Lemma 7.3 it is clear that S is the image of $R[t]$ under the map Φ. Since the latter is injective, it induces a linear isomorphism from $R[t]$ to the algebra S. This allows one to lift the algebra structure of S to $R[t]$. Relation (7.2) holds in $R[t]$ in view of Lemma 7.3. □

We draw a few consequences. First, we wish to give a general formula for the product in $R[t, \alpha, \delta]$. Consider $P = \sum_{i=0}^{n} a_i t^i$ and $Q = \sum_{i=0}^{m} b_i t^i$. Set $PQ = \sum_{i=0}^{n+m} c_i t^i$. Let $S_{n,k}$ be the linear endomorphism of R defined as the sum of all $\binom{n}{k}$ possible compositions of k copies of δ and of $n-k$ copies of α.

Corollary I.7.4. *Under the hypotheses of Theorem 7.1 (b), the following holds.*

(a) *For all i with $0 \leq i \leq m+n$ we have*

$$c_i = \sum_{p=0}^{i} a_p \sum_{k=0}^{p} S_{p,k}(b_{i-p+k}) \tag{7.8}$$

and for all $a \in R$ and $n \in \mathbf{N}$ we have in $R[t, \alpha, \delta]$

$$t^n a = \sum_{k=0}^{n} S_{n,k}(a)\, t^{n-k}. \tag{7.9}$$

(b) *The algebra $R[t, \alpha, \delta]$ has no zero-divisors. As a left R-module, it is free with basis $\{t^i\}_{i \in \mathbf{N}}$.*

(c) *If α is an automorphism, then $R[t, \alpha, \delta]$ is also a right free R-module with the same basis $\{t^i\}_{i \in \mathbf{N}}$.*

PROOF. (a) Relation (7.9) follows from (7.2) by induction on n. It implies (7.8).

(b) This is a consequence of the existence of the degree and of the definition of $R[t]$.

(c) Let us first prove that the set $\{t^i\}_{i \geq 0}$ generates $R[t, \alpha, \delta]$ as a right R-module. This means that any element P of $R[t, \alpha, \delta]$ can also be written under the form $P = \sum_{i=0}^{n} t^i a^i$ where $a_0, \ldots, a_n \in R$. Let us prove this by induction on the degree n of P. For $n = 0$, it is clear. For higher n we use the relation

$$at^n = t^n \alpha^{-n}(a) + \text{lower-degree terms} \tag{7.10}$$

which makes sense once α is assumed to be invertible. It remains to be proved that the set $\{t^i\}_{i \geq 0}$ is free. Suppose it is not. Then there exists a relation of the form

$$t^n a_n + t^{n-1} a_{n-1} + \cdots + t a_1 + a_0 = 0$$

with $a_n \neq 0$. Using (7.10) once again, we get another relation of the form

$$\alpha^n(a_n) t^n + \text{lower-degree terms} = 0,$$

which, by Part (b), implies that $\alpha^n(a_n) = 0$. The map α being an isomorphism, we get $a_n = 0$, hence a contradiction. □

Example 1. Consider the special case $\alpha = \mathrm{id}_R$. If $\delta = 0$, then the Ore extension $R[t, \mathrm{id}_R, 0]$ is clearly isomorphic to the polynomial algebra $R[t]$. In case of a general derivation δ, the algebra $R[t, \mathrm{id}_R, \delta]$ is an algebra of polynomial differential operators (see Exercise 8). When $R = k[x]$ and δ is the usual derivation d/dx of polynomials, then $R[t, \mathrm{id}_R, \delta]$ is the Weyl algebra which is generated by two variables x and δ subject to the well-known Heisenberg relation $\delta x - x\delta = 1$.

I.8 Noetherian Rings

Proposition I.8.1. *Let A be a ring. The following two statements are equivalent.*

(i) *Any left ideal I of A is finitely generated, i.e., there exist $a_1, \dots, a_n$ in I such that $I = Aa_1 + \dots + Aa_n$.*

(ii) *Any ascending sequence $I_1 \subset I_2 \subset I_3 \subset \dots \subset A$ of left ideals of A is finite, i.e., there exists an integer r such that $I_{r+i} = I_r$ for all $i \geq 0$.*

PROOF. Let us first show that (i) implies (ii). Consider an ascending sequence $I_1 \subset I_2 \subset I_3 \subset \dots$ of left ideals of A. The union of these ideals is a left ideal I which, by (i), is generated by a finite number $a_1, \dots, a_n$ of elements of A. By definition of the union there exists an integer r such that $a_1, \dots, a_n$ all belong to the ideal I_r. It follows that $I \subset I_r \subset I_{r+i} \subset I$ for all $i \geq 0$.

We now establish the converse. Let I be a left ideal that is not finitely generated and a_1 be an element of I. The left ideal $I_1 = Aa_1$ is contained in I and $I_1 \neq I$. Therefore, we can find an element $a_2 \in I \setminus Aa_1$. We have $I_1 \subset I_2 = Aa_1 + Aa_2 \subset I$ and $I_1 \neq I_2 \neq I$. Proceeding inductively, we find an infinite strictly ascending sequence $I_1 \subset \cdots I_n \subset I_{n+1} \subset \cdots I$ of left ideals. □

Any ring A satisfying the equivalent conditions of Proposition 8.1 is said to be *left Noetherian*. The ring A is *right Noetherian* if the opposite ring A^{op} is left Noetherian. It is *Noetherian* if it is both left and right Noetherian.

Example 1. Any (skew-)field K is Noetherian, the only ideals being $\{0\}$ and K.

The property of being Noetherian is preserved by quotients and Ore extensions, as will be seen next.

Proposition I.8.2. *Let $\varphi : A \to B$ be a surjective morphism of rings. If A is left Noetherian, then so is B.*

PROOF. Let J be a left ideal of B. The left ideal $I = \varphi_{-1}(J)$ of A is generated by elements $a_1, \dots, a_n$. Therefore, $J = \varphi(\varphi_{-1}(J))$ is generated by $\varphi(a_1), \dots, \varphi(a_n)$. □

The following theorem is a non-commutative version of Hilbert's basis theorem.

Theorem I.8.3. *Let R be an algebra, α be an algebra automorphism and δ be an α-derivation of R. If R is left Noetherian, then so is the Ore extension $R[t, \alpha, \delta]$.*

As a consequence of Proposition 8.2 and Theorem 8.3 applied to the case $\alpha = \mathrm{id}$ and $\delta = 0$, we have

Corollary I.8.4. *If R is left Noetherian, then so is $R[X_1, \dots, X_n]/I$ for any ideal I.*

Proof of Theorem 8.3. Let I be a left ideal of the Ore extension $R[t, \alpha, \delta]$. We have to prove that I is finitely generated. Given an integer $d \geq 0$, define I_d as the union of $\{0\}$ and of all elements of R which appear as leading coefficients of degree d elements of I. One checks easily that I_d is a left ideal of R.

On the other hand, if a is the leading coefficient of some polynomial P, then $\alpha(a)$ is the leading coefficient of tP. Consequently, $\alpha(I_d)$ is included in I_{d+1}. We therefore have the ascending sequence

$$I_0 \subset \alpha^{-1}(I_1) \subset \alpha^{-2}(I_2) \subset \dots \subset \alpha^{-n}(I_n) \subset \alpha^{-(n+1)}(I_{n+1}) \subset \dots$$

of left ideals in R. Since R is left Noetherian, there exists an integer n such that $I_{n+i} = \alpha^i(I_n)$ for all $i \geq 0$.

For any d with $0 \leq d \leq n$ choose generators $a_{d,1}, \dots, a_{d,p}$ of I_d. Let $P_{d,i}$ be a degree d element of I whose leading coefficient is $a_{d,i}$. The set $\{P_{d,i}\}_{0 \leq d \leq n, 1 \leq i \leq p}$ is finite. Let us prove by induction on the degree that any polynomial P in I belongs to the ideal $I' = \sum_{d,i} R[t, \alpha, \delta] \, P_{d,i}$. This will imply that $I = I'$ is finitely generated, hence establish the theorem.

The induction hypothesis clearly holds in degree 0. Suppose we have proved that any element of degree $< d$ in I is in I'. Let P be a degree d element of I.

(a) If $d \leq n$, the leading coefficient a of P is of the form $a = \sum_{0 \leq i \leq p} r_i a_{d,i}$ where $r_0, \dots, r_p$ are elements of R. Consequently, $Q = P - \sum_{0 \leq i \leq p} r_i P_{d,i}$ is an element of I of degree $< d$. By induction, Q, hence P, belong to I'.

(b) If $d > n$, the leading coefficient a of P belongs to $I_d = \alpha^{d-n}(I_n)$. It can be written $a = \sum_{0 \leq i \leq p} r_i \alpha^{d-n}(a_{d,i})$ for some $r_0, \dots, r_p$ in R. Consider the polynomial

$$Q = P - \sum_{0 \leq i \leq p} r_i t^{d-n} P_{d,i}.$$

The coefficient of t^d in Q is

$$a - \sum_{0 \le i \le p} r_i \alpha^{d-n}(a_{d,i}) = 0,$$

which shows that the degree of Q is $< d$. We can therefore apply the induction hypothesis and conclude as above. □

I.9 Exercises

1. (*Schur's lemma*) Prove that any A-linear map between simple A-modules is either zero or an isomorphism. Deduce that the A-linear endomorphisms of a simple A-module form a skew-field.

2. Let $p = p^2$ be an A-linear idempotent endomorphism of an indecomposable A-module V. Show that $p = 0$ or $p = \mathrm{id}_V$.

3. Let A_1, A_2 be algebras. Let V_1 be an A_1-module and V_2 be an A_2-module. Establish that $(a_1, a_2)(v_1, v_2) = (a_1 v_1, a_2 v_2)$ (where $a_1 \in A_1$, $a_2 \in A_2$, $v_1 \in V_1$, $v_2 \in V_2$) defines an $A_1 \times A_2$-module structure on $V_1 \times V_2$. Prove also that any $A_1 \times A_2$-module is of this form.

4. Let A be a filtered algebra and $\mathrm{gr}(A)$ the associated graded algebra. Prove that if $\mathrm{gr}(A)$ is Noetherian without zero-divisors, then so is A.

5. (*Rees algebra*) Let $A \supset \ldots \supset F_1 \supset F_0$ be a filtered algebra. Define the Rees algebra $R(A)$ as the subalgebra

$$R(A) = \sum_{n \ge 0} F_n t^n$$

of the polynomial algebra $A[t]$. Prove that

(i) there are algebra isomorphisms

$$R(A)/(t-1) \cong A, \quad R(A)/(t) \cong \mathrm{gr}(A), \quad R(A)[t^{-1}] \cong A[t, t^{-1}],$$

(ii) if the algebra $\mathrm{gr}(A)$ is generated by homogeneous elements $\bar{a}_1, \ldots, \bar{a}_n$ of respective degrees $d_1, \ldots, d_n$, then $R(A)$ is generated by the elements t, $a_1 t^{d_1}, \ldots, a_n t^{d_n}$ where a_i is a lift of $\bar{a}_i$ in F_i for all i.

6. (*Poincaré series of a graded algebra*) Let $A = \bigoplus_{i \ge 0} A_i$ be a graded algebra such that the vector spaces A_i are all finite-dimensional. Define the Poincaré series of A as the formal series

$$P(A) = \sum_{i \ge 0} \dim(A_i)\, t^i.$$

Prove that

$$P(k\{x_1, \ldots, x_n\}) = \frac{1}{1 - nt} \quad \text{and} \quad P(k[x_1, \ldots, x_n]) = \frac{1}{(1-t)^n}.$$

7. Compute the Poincaré series of the graded algebra associated to the filtered algebra $SL(2)$.

8. (*Leibniz formula*) Let δ be an α-derivation of an algebra R. Prove that if $a_1, \ldots, a_n$ are elements of R, then

$$\begin{aligned}\delta(a_1 \ldots a_n) &= \delta(a_1) a_2 \ldots a_n \\ &+ \textstyle\sum_{i=2}^{n-1} \alpha(a_1 \ldots a_{i-1}) \delta(a_i) a_{i+1} \ldots a_n + \alpha(a_1 \ldots a_{n-1}) \delta(a_n)\end{aligned}$$

and

$$\delta^n(a_1 a_2) = \sum_{k=0}^{n} S_{n,k}(a_1)\, \delta^{n-k}(a_2).$$

for $n \ge 1$. The endomorphisms $S_{n,k}$ were defined in Section 7.

9. Let R be an algebra with an algebra automorphism α and an α-derivation δ. Establish that $\delta\alpha^{-1}$ is an α^{-1}-derivation of the opposite algebra R^{op} and that we have an algebra isomorphism

$$R[t, \alpha, \delta]^{\mathrm{op}} \cong R^{\mathrm{op}}[t, \alpha^{-1}, -\delta\alpha^{-1}].$$

Deduce that $R[t, \alpha, \delta]$ is right Noetherian if R is.

10. (*Algebra of differential operators*) Let R be an algebra over a field of characteristic zero and let δ be a derivation of R. The algebra of differential operators associated to δ is the Ore extension $R[t, \mathrm{id}_R, \delta]$, which we simply denote by $R[t, \delta]$.

(a) Prove that for any integer $n > 0$ and any element a of R we have

$$t^n a = \sum_{k=0}^{n} \binom{n}{k} \delta^k(a)\, t^{n-k}.$$

(b) Show that any trace on $R[t, \delta]$, i.e., any linear map τ on $R[t, \delta]$ such that $\tau(xy) = \tau(yx)$ for any pair (x, y) of elements of $R[t, \delta]$, is zero.

11. (*Algebra of pseudo-differential operators*) Keep the hypotheses and the notations of the previous exercise. Show that the formula

$$\Big(\sum_i a_i t^i\Big)\Big(\sum_i b_i t^i\Big) = \sum_i c_i t^i$$

where

$$c_i = \sum_{k\in\mathbf{N},\, p\in\mathbf{Z}} \frac{p(p-1)\dots(p-k+1)}{k!}\, a_p\, \delta^k(b_{i-p+k}),$$

defines an algebra structure on the vector space $R[t,\delta][[t^{-1}]]$ of formal series of the form $\sum_{i=-\infty}^{n} a_i t^i$. Check that $R[t,\delta]$ is a subalgebra. Define the *non-commutative residue* as the linear map from $R[t,\delta][[t^{-1}]]$ to $R/([R,R]+\delta(R))$, sending the formal series $\sum_{i=-\infty}^{n} a_i t^i$ to the class of the coefficient a_{-1}. Prove that the non-commutative residue is a trace on the algebra $R[t,\delta][[t^{-1}]]$ of pseudo-differential operators.

I.10 Notes

Ore extensions were introduced by Ore in [Ore33]. They are also called *"skew polynomial rings"* in [Coh71] [MR87] (see also [Cur52]). One of Ore's motivations was to find a large class of non-commutative algebras that are embeddable into a skew-field. As is well-known, this is possible for any commutative integral domain, but not for a general non-commutative algebra. Ore proved that any algebra obtained from a skew-field by iterated Ore extensions can itself be embedded into some skew-field (see Proposition 0.8.4 in [Coh71]). For more details on Noetherian rings, we refer the reader to [Lan65] and [MR87]. The examples given in [MR87], 2.11 show that the non-commutative version of Hilbert's basis theorem is no longer true if the endomorphism α is not assumed to be bijective.

Chapter II

Tensor Products

This chapter is devoted to a few facts on tensor products of vector spaces and of algebras that will be needed in the sequel. We fix a field k once and for all.

II.1 Tensor Products of Vector Spaces

Given vector spaces U and V, we denote by $\mathrm{Hom}(U,V)$ the space of linear maps from U to V. In particular, define $\mathrm{End}(V) = \mathrm{Hom}(V,V)$, the space of linear endomorphisms of V. If W is a third vector space, we denote by $\mathrm{Hom}^{(2)}(U,V;W)$ the space of bilinear maps from $U\times V$ to W.

The tensor product $U\otimes V$ of two vector spaces can be characterized as follows.

Theorem II.1.1. *Given vector spaces U and V there exist a vector space $U\otimes V$ and a bilinear map $\varphi_0 : U\times V \to U\otimes V$ such that, for all vector spaces W, the linear map*

$$\mathrm{Hom}(U\otimes V, W) \to \mathrm{Hom}^{(2)}(U,V;W)$$

given by $f\mapsto f\circ\varphi_0$ is a linear isomorphism. The vector space $U\otimes V$ is called the tensor product of U and V. It is unique up to isomorphism.

For any $u\in U$ and $v\in V$, set $u\otimes v = \varphi_0(u,v)$. Since φ_0 is bilinear, the following relations hold in $U\otimes V$:

$$(u+u')\otimes v = u\otimes v + u'\otimes v, \tag{1.1}$$

$$u \otimes (v + v') = u \otimes v + u \otimes v', \tag{1.2}$$

$$\lambda(u \otimes v) = (\lambda u) \otimes v = u \otimes (\lambda v) \tag{1.3}$$

where $u, u' \in U$, $v, v' \in V$ and $\lambda \in k$. Moreover, as we shall see in the subsequent proof, any element of $U \otimes V$ is a finite sum of the form

$$\sum_{i=1}^{p} u_i \otimes v_i \tag{1.4}$$

where $u_1, \ldots, u_p$ belong to U and $v_1, \ldots, v_p$ belong to V.

Proof. We indicate the proof. Consider the vector space $k[U \times V]$ whose basis is the set $U \times V$. We define $U \otimes V$ as the quotient of $k[U \times V]$ by the subspace generated by the elements

$$(u + u', v) - (u, v) - (u', v), \quad (u, v + v') - (u, v) - (u, v'),$$

$$(\lambda u, v) - \lambda(u, v), \quad (u, \lambda v) - \lambda(u, v)$$

where $u, u' \in U$, $v, v' \in V$ and $\lambda \in k$. The class of $(u, v) \in U \times V$ in $U \otimes V$ is denoted $\varphi_0(u, v) = u \otimes v$. By construction, the canonical map φ_0 from $U \times V$ to $U \otimes V$ is bilinear. The rest of the proof follows easily. For details, see [Bou70], Chap. 2 and [Lan65]. $\square$

Corollary II.1.2. *For any triple (U, V, W) of vector spaces there is a natural isomorphism*

$$\mathrm{Hom}(U \otimes V, W) \cong \mathrm{Hom}(U, \mathrm{Hom}(V, W)).$$

Proof. If φ is a bilinear map from $U \times V$ to W and u is any vector of U, then $\varphi(u, -)$ is a linear map from V to W. This sets up the desired isomorphism. $\square$

The proof of the following easy proposition is left to the reader.

Proposition II.1.3. *Let U, V, W be vector spaces. There are isomorphisms*

$$(U \otimes V) \otimes W \cong U \otimes (V \otimes W)$$

determined by $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$,

$$k \otimes V \cong V \cong V \otimes k$$

determined by $\lambda \otimes v \mapsto \lambda v$ and $v \mapsto v \otimes 1$, and

$$V \otimes W \cong W \otimes V$$

given by the flip $\tau_{V,W}$ defined by $\tau_{V,W}(v \otimes w) = w \otimes v$.

The tensor product also commutes with the direct sum of spaces. Let $(U_i)_{i \in I}$ be a family of vector spaces indexed by a set I. Recall that there exists a vector space $\bigoplus_{i \in I} U_i$, called the *direct sum* of the family (U_i), and linear maps $q_i : U_i \to \bigoplus_{i \in I} U_i$ such that for any vector space V, the linear map

$$\mathrm{Hom}(\bigoplus_{i \in I} U_i, V) \to \prod_{i \in I} \mathrm{Hom}(U_i, V) \tag{1.5}$$

given by $f \mapsto (f \circ q_i)_i$ is an isomorphism.

Proposition II.1.4. *We have*

$$(\bigoplus_{i \in I} U_i) \otimes V \cong \bigoplus_{i \in I} (U_i \otimes V). \tag{1.6}$$

Proof. By Corollary 1.2 and (1.5) we have the chain of isomorphisms

$$\begin{aligned} \mathrm{Hom}((\bigoplus_{i \in I} U_i) \otimes V, W) &\cong \mathrm{Hom}(\bigoplus_{i \in I} U_i, \mathrm{Hom}(V, W)) \\ &\cong \prod_{i \in I} \mathrm{Hom}(U_i, \mathrm{Hom}(V, W)) \\ &\cong \prod_{i \in I} \mathrm{Hom}(U_i \otimes V, W) \\ &\cong \mathrm{Hom}(\bigoplus_{i \in I} (U_i \otimes V), W). \end{aligned}$$

These hold for any vector space W. A classical argument given in full detail in the second proof of Proposition 5.1 (c) allows one to conclude. $\square$

Recall also the notion of a direct product of vector spaces. Let $(V_i)_{i \in I}$ be a family of vector spaces indexed by a set I. There exists a vector space $\prod_{i \in I} V_i$, called the *direct product* of the family $(V_i)_{i \in I}$, and linear maps $p_i : \prod_{i \in I} V_i \to V_i$ such that for all vector spaces U, the map

$$\mathrm{Hom}(U, \prod_{i \in I} V_i) \to \prod_{i \in I} \mathrm{Hom}(U, V_i) \tag{1.7}$$

given by $f \mapsto (p_i \circ f)_i$ is an isomorphism. As a set, $\prod_{i \in I} V_i$ may be realized as the vector space of all families $(v_i)_{i \in I}$ such that $v_i \in V_i$ for all i. The direct sum $\bigoplus_{i \in I} V_i$ is then the subspace of $\prod_{i \in I} V_i$ consisting of the families $(v_i)_{i \in I}$ where all but finitely many v_i are zero. When the indexing set I is finite, the direct product coincides with the direct sum. Otherwise, the direct sum is a proper subspace of the direct product.

Corollary II.1.5. *Let $\{u_i\}_{i \in I}$ be a basis of the vector space U and $\{v_j\}_{j \in J}$ be a basis of V. Then the set $\{u_i \otimes v_j\}_{(i,j) \in I \times J}$ is a basis of the tensor product $U \otimes V$. Consequently, we have $\dim(U \otimes V) = \dim(U) \dim(V)$.*

PROOF. By definition of the direct sum, we have

$$U \cong \bigoplus_{i\in I} ku_i \quad \text{and} \quad V \cong \bigoplus_{j\in J} kv_j. \tag{1.8}$$

Applying Propositions 1.3–1.4 and using $k \otimes k \cong k$, we get

$$U \otimes V \cong \bigoplus_{(i,j)\in I\times J} k\,(u_i \otimes v_j).$$

□

Let us define the notion of a *free module* over an algebra A using the tensor product. It is a module of the form $A \otimes V$ where V is a vector space and A acts on $A \otimes V$ by

$$a(a' \otimes v) = aa' \otimes v$$

for $a, a' \in A$ and $v \in V$. A *basis* of an A-module M is a subset $\{x_i\}_{i\in I}$ of M such that the map

$$(a_i)_{i\in I} \mapsto \sum_{i\in I} a_i x_i$$

from the direct sum $\bigoplus_{i\in I} A$ to M is an isomorphism. By Propositions 1.3–1.4,

$$\bigoplus_{i\in I} A \cong \bigoplus_{i\in I} (A \otimes k) \cong A \otimes V$$

where $V = \bigoplus_{i\in I} k$. It follows that an A-module has a basis if and only if it is free.

II.2 Tensor Products of Linear Maps

Let $f : U \to U'$ and $g : V \to V'$ be linear maps. We define their tensor product $f \otimes g : U \otimes V \to U' \otimes V'$ by

$$(f \otimes g)(u \otimes v) = f(u) \otimes g(v) \tag{2.1}$$

for all u in U and v in V. This gives rise to a linear map

$$\lambda : \mathrm{Hom}(U, U') \otimes \mathrm{Hom}(V, V') \to \mathrm{Hom}(V \otimes U, U' \otimes V') \tag{2.2}$$

defined by

$$\Big(\lambda(f \otimes g)\Big)(v \otimes u) = f(u) \otimes g(v). \tag{2.3}$$

The reasons for the switch of U and V in (2.2) will become apparent in III.5.2 and in Chapter XIV. The main result of this section is the following.

Theorem II.2.1. *The map λ is an isomorphism provided at least one of the pairs (U, U'), (V, V') or (U, V) consists of finite-dimensional vector spaces.*

PROOF. Assume that U and U' are finite-dimensional. We wish to show that the map λ of (2.2) is an isomorphism. We shall do this by reducing λ to simpler maps. We can write $U = \bigoplus_{i\in I} ku_i$ where $\{u_i\}_{i\in I}$ is a finite basis of U. As a consequence of the isomorphism (1.5–1.6), the map λ turns into a map from $(\prod_i \mathrm{Hom}(ku_i, U')) \otimes \mathrm{Hom}(V, V')$ to $\prod_i \mathrm{Hom}(V \otimes ku_i, U' \otimes V')$. The set I being finite, we may replace $\prod_i$ by $\bigoplus_i$. Applying (1.6) again, it remains to prove that the map

$$\lambda : \mathrm{Hom}(ku_i, U') \otimes \mathrm{Hom}(V, V') \to \mathrm{Hom}(V \otimes ku_i, U' \otimes V')$$

is an isomorphism in the special case $U = ku_i$.

Since ku_i is one-dimensional, this amounts to checking that the map

$$\lambda' : U' \otimes \mathrm{Hom}(V, V') \to \mathrm{Hom}(V, U' \otimes V') \tag{2.4}$$

defined by

$$\lambda'(u' \otimes f)(v) = u' \otimes f(v)$$

is an isomorphism. By assumption, we also have $U' = \bigoplus_{i\in I'} ku'_i$ for some finite basis $\{u_i\}_{i\in I'}$. We again use (1.6–1.7) and the fact that the direct product over the finite set I' is the same as the direct sum. We get

$$U' \otimes \mathrm{Hom}(V, V') \cong \bigoplus_{i\in I'} ku'_i \otimes \mathrm{Hom}(V, V')$$

and

$$\mathrm{Hom}(V, U' \otimes V') \cong \prod_{i\in I'} \mathrm{Hom}(V, ku'_i \otimes V').$$

This allows us to break λ' into the direct product of the maps

$$\lambda' : ku'_i \otimes \mathrm{Hom}(V, V') \to \mathrm{Hom}(V, ku'_i \otimes V').$$

In this special case, λ' is given by $\lambda'(u'_i \otimes f)(v) = u'_i \otimes f(v)$, which is clearly an isomorphism. Hence, so is the map λ' of (2.4), which concludes the proof.

There are similar arguments in the remaining two cases. □

We deduce two corollaries involving the dual vector space $V^* = \mathrm{Hom}(V, k)$ of a vector space V. For the first one, we specialize Theorem 2.1 by taking $U' = V' = k$.

Corollary II.2.2. *The map $\lambda : U^* \otimes V^* \to (V \otimes U)^*$ is an isomorphism provided U or V are finite-dimensional.*

For the second corollary, we take $U = V' = k$ in Theorem 2.1.

Corollary II.2.3. *The map $\lambda_{U,V} : V \otimes U^* \to \mathrm{Hom}(U,V)$ given for $u \in U$, $v \in V$ and $\alpha \in U^*$ by*

$$\lambda_{U,V}(v \otimes \alpha)(u) = \alpha(u)\, v \tag{2.5}$$

is an isomorphism if U or V are finite-dimensional. In particular, if V is a finite-dimensional vector space, the map $\lambda_{V,V}$ is an isomorphism

$$V \otimes V^* \cong \mathrm{End}(V).$$

We now wish to express the general map λ of (2.2) in terms of the special maps λ defined in Corollaries 2.2–2.3 and of the flip. This is done in the following lemma which will be useful later. Note that the map $\lambda_{U,U'} \otimes \lambda_{V,V'}$ is invertible when either U or U', and either V or V' are finite-dimensional.

Lemma II.2.4. *The following diagram commutes:*

$$\begin{tikzcd}
U' \otimes U^* \otimes V' \otimes V^* \arrow[r, "\lambda_{U,U'} \otimes \lambda_{V,V'}"] \arrow[d, "\mathrm{id} \otimes \tau_{U^*,V'} \otimes \mathrm{id}"] & \mathrm{Hom}(U,U') \otimes \mathrm{Hom}(V,V') \arrow[dd, "\lambda"] \\
U' \otimes V' \otimes U^* \otimes V^* \arrow[d, "\mathrm{id} \otimes \mathrm{id} \otimes \lambda"] & \\
U' \otimes V' \otimes (V \otimes U)^* \arrow[r, "\lambda_{V \otimes U, U' \otimes V'}"] & \mathrm{Hom}(V \otimes U, U' \otimes V')
\end{tikzcd}$$

PROOF. Easy. □

There is another important operation on linear homomorphisms that we have not yet discussed. It is the *composition* $(g,f) \mapsto g \circ f$ of two linear maps. This operation is bilinear and leads, for any triple (U,V,W) of vector spaces, to the map

$$\mathrm{Hom}(V,W) \otimes \mathrm{Hom}(U,V) \xrightarrow{\circ} \mathrm{Hom}(U,W).$$

Under some finite-dimensionality conditions, we can express the composition in simpler terms again involving the special maps λ of Corollary 2.3 as well as the *evaluation map*

$$\mathrm{ev}_V : V^* \otimes V \to k$$

which is defined as usual, namely by

$$\mathrm{ev}_V(\alpha \otimes v) = <\alpha, v> = \alpha(v) \tag{2.6}$$

for any linear form α and any vector v of V.

Lemma II.2.5. *The square*

$$\begin{tikzcd}
W \otimes V^* \otimes V \otimes U^* \arrow[r, "\mathrm{id} \otimes \mathrm{ev}_V \otimes \mathrm{id}"] \arrow[d, "\lambda_{V,W} \otimes \lambda_{U,V}"] & W \otimes U^* \arrow[d, "\lambda_{U,W}"] \\
\mathrm{Hom}(V,W) \otimes \mathrm{Hom}(U,V) \arrow[r, "\circ"] & \mathrm{Hom}(U,W)
\end{tikzcd}$$

commutes.

PROOF. Easy. □

II.3 Duality and Traces

All vector spaces considered in this section are assumed to be finite-dimensional. If V is such a vector space, we denote a basis of V by $\{v_i\}_i$ using the corresponding lower-case letter for vectors. The dual basis in the dual vector space V^* is denoted $\{v^i\}_i$. Using these bases, the evaluation map can be redefined by

$$\mathrm{ev}_V(v^i \otimes v_j) = <v^i, v_j> = \delta_{ij}. \tag{3.1}$$

Let us express the isomorphism $\lambda_{U,V} : V \otimes U^* \cong \mathrm{Hom}(U,V)$ of Corollary 2.3 in terms of bases. Let $f : U \to V$ be a linear map. Using bases for U and V, we have

$$f(u_j) = \sum_i f_j^i v_i \tag{3.2}$$

for some family $(f_j^i)_{ij}$ of scalars. It is easily checked that

$$f = \lambda_{U,V}\Big(\sum_{ij} f_j^i\, v_i \otimes u^j\Big). \tag{3.3}$$

In particular, taking for f the identity of V, we get

$$\mathrm{id}_V = \lambda_{V,V}\Big(\sum_i v_i \otimes v^i\Big). \tag{3.4}$$

This allows us to define the *coevaluation map* of any finite-dimensional vector space V as the linear map $\delta_V : k \to V \otimes V^*$ defined by

$$\delta_V(1) = \lambda_{V,V}^{-1}(\mathrm{id}_V) = \sum_i v_i \otimes v^i. \tag{3.5}$$

By its very definition, the map δ_V is independent of the choice of a basis. We now record some relations between the evaluation and coevaluation maps. These relations will turn out to be fundamental when we define duality in categories in Chapter XIV.

Proposition II.3.1. *The composition of the maps*

$$V \xrightarrow{\delta_V \otimes \mathrm{id}_V} V \otimes V^* \otimes V \xrightarrow{\mathrm{id}_V \otimes \mathrm{ev}_V} V$$

is equal to the identity of V. Similarly, the composition of the maps

$$V^* \xrightarrow{\mathrm{id}_{V^*} \otimes \delta_V} V^* \otimes V \otimes V^* \xrightarrow{\mathrm{ev}_V \otimes \mathrm{id}_{V^*}} V^*$$

is equal to the identity of V^*.

PROOF. Immediate. □

Let us recall the operation of *transposition*. For a linear map $f : U \to V$, define its *transpose* $f^* : V^* \to U^*$ as the linear map defined for all $\alpha \in V^*$ and all $u \in U$ by

$$< f^*(\alpha), u > = < \alpha, f(u) > . \tag{3.6}$$

In other words, f^* is the unique linear map such that the square

$$\begin{array}{ccc} V^* \otimes U & \xrightarrow{f^* \otimes \mathrm{id}_U} & U^* \otimes U \\ \downarrow{\scriptstyle \mathrm{id}_{V^*} \otimes f} & & \downarrow{\scriptstyle \mathrm{ev}_U} \\ V^* \otimes V & \xrightarrow{\mathrm{ev}_V} & k \end{array} \tag{3.7}$$

commutes. The transposition may be recovered from the evaluation and coevaluation maps as shown in the following result whose proof is left to the reader.

Proposition II.3.2. *Let $f : U \to V$ be a linear map. Then the transpose f^* is equal to the composition of the maps*

$$V^* \xrightarrow{\mathrm{id}_{V^*} \otimes \delta_U} V^* \otimes U \otimes U^* \xrightarrow{\mathrm{id}_{V^*} \otimes f \otimes \mathrm{id}_{U^*}} V^* \otimes V \otimes U^* \xrightarrow{\mathrm{ev}_V \otimes \mathrm{id}_{U^*}} U^*.$$

Observe that if (3.2) holds, then

$$f^*(v^j) = \sum_i f_i^j u^i. \tag{3.8}$$

We thus see that transposition amounts to exchanging upper and lower indices. We generalize this as follows. Let f be a linear map from $V \otimes W$ to $X \otimes Y$. Using bases on these spaces, we define the *partial transposes*

$$f^+ : X^* \otimes W \to V^* \otimes Y \quad \text{and} \quad f^\times : V \otimes Y^* \to X \otimes W^*$$

by

$$f^+(x^i \otimes w_j) = \sum_{k,\ell} f_{kj}^{i\ell}\, v^k \otimes y_\ell \tag{3.9}$$

and

$$f^\times(v_i \otimes y^j) = \sum_{k,\ell} f_{i\ell}^{kj}\, x_k \otimes w^\ell \tag{3.10}$$

if

$$f(v_i \otimes w_j) = \sum_{k,\ell} f_{ij}^{k\ell}\, x_k \otimes y_\ell. \tag{3.11}$$

Lemma II.3.3. *The definitions of f^+ and $f^\times$ are independent of the choice of bases. We also have*

$$(f^+)^\times = (f^\times)^+ = f^*.$$

PROOF. Left to the reader. □

The isomorphism $\lambda_{V,V}$ of Corollary 2.3 allows one to define the *trace of an endomorphism* in a finite-dimensional vector space V. The trace $\mathrm{tr} : \mathrm{End}(V) \to k$ is defined as the composition

$$\mathrm{End}(V) \xrightarrow{\lambda_{V,V}^{-1}} V \otimes V^* \xrightarrow{\tau_{V,V^*}} V^* \otimes V \xrightarrow{\mathrm{ev}_V} k. \tag{3.12}$$

Proposition II.3.4. *Let f and g be endomorphisms of a finite-dimensional vector space V.*

(a) *The trace satisfies the relation*

$$\mathrm{tr}(f \circ g) = \mathrm{tr}(g \circ f). \tag{3.13}$$

(b) *If $(f_j^i)_{ij}$ is the matrix of f in a basis of V, then*

$$\mathrm{tr}(f) = \sum_i f_i^i. \tag{3.14}$$

(c) *We also have*

$$\mathrm{tr}(f^*) = \mathrm{tr}(f). \tag{3.15}$$

PROOF. (a) By linearity, it suffices to prove (3.13) for

$$f = \lambda_{V,V}(v \otimes \alpha) \quad \text{and} \quad g = \lambda_{V,V}(w \otimes \beta)$$

where $v, w \in V$ and $\alpha, \beta \in V^*$. We have $f \circ g = \lambda_{V,V}(\alpha(w)\, v \otimes \beta)$ by Lemma 2.5. Consequently, $\mathrm{tr}(f \circ g) = \alpha(w)\,\beta(v)$, which clearly equals $\mathrm{tr}(g \circ f)$.

(b) From Relations (3.2–3.3) we derive

$$\mathrm{tr}(f) = \sum_{ij} f_j^i < v^j, v_i > = \sum_i f_i^i.$$

(c) Relation (3.15) follows from (3.8) and (3.14). □

The next result expresses the trace in terms of the evaluation and coevaluation maps and of the flip.

Proposition II.3.5. *The trace of $f : V \to V$ is equal to the composition of the maps*

$$k \xrightarrow{\delta_V} V \otimes V^* \xrightarrow{f \otimes \mathrm{id}_{V^*}} V \otimes V^* \xrightarrow{\tau_{V,V^*}} V^* \otimes V \xrightarrow{\mathrm{ev}_V} k.$$

We close these generalities with the *partial traces* of an endomorphism f of $U \otimes V$. By Theorem 2.1 the map $f \otimes g \mapsto \lambda(f \otimes g) \circ \tau_{U,V}$ is an isomorphism $\overline{\lambda}$ from $\mathrm{End}(U) \otimes \mathrm{End}(V)$ onto $\mathrm{End}(U \otimes V)$. We define tr_1 and tr_2 by the following commutative diagram.

$$\begin{array}{ccccc} \mathrm{End}(V) & \xleftarrow{\mathrm{tr}_1} & \mathrm{End}(U \otimes V) & \xrightarrow{\mathrm{tr}_2} & \mathrm{End}(U) \\ \uparrow{\scriptstyle \cong} & & \uparrow{\scriptstyle \overline{\lambda}} & & \uparrow{\scriptstyle \cong} \\ k \otimes \mathrm{End}(V) & \xleftarrow{\mathrm{tr} \otimes \mathrm{id}} & \mathrm{End}(U) \otimes \mathrm{End}(V) & \xrightarrow{\mathrm{id} \otimes \mathrm{tr}} & \mathrm{End}(U) \otimes k \end{array} \tag{3.16}$$

Lemma II.3.6. *If $f(u_i \otimes v_j) = \sum_{k,\ell} f_{ij}^{k\ell}\, u_k \otimes v_\ell$ on some bases of U and V, then*

$$\mathrm{tr}_1(f)(v_j) = \sum_{i,\ell} f_{ij}^{i\ell}\, v_\ell \quad \textit{and} \quad \mathrm{tr}_2(f)(u_i) = \sum_{j,k} f_{ij}^{kj}\, u_k. \tag{3.17}$$

We also have $\mathrm{tr}_1(\mathrm{tr}_2(f)) = \mathrm{tr}_2(\mathrm{tr}_1(f)) = \mathrm{tr}(f)$.

PROOF. Left to the reader. □

II.4 Tensor Products of Algebras

Given algebras A and B, we put an algebra structure on the tensor product $A \otimes B$ by

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb' \tag{4.1}$$

where $a, a' \in A$ and $b, b' \in B$. We call $A \otimes B$ the *tensor product of the algebras A and B*. Its unit is $1 \otimes 1$. Defining $i_A(a) = a \otimes 1$ and $i_B(b) = 1 \otimes b$, we get algebra morphisms $i_A : A \to A \otimes B$ and $i_B : B \to A \otimes B$. The following relation holds in view of (4.1):

$$i_A(a) i_B(b) = i_B(b) i_A(a) = a \otimes b \tag{4.2}$$

for all $a \in A$ and $b \in B$. The tensor product of algebras enjoys the following universal property.

Proposition II.4.1. *Let $f : A \to C$ and $g : B \to C$ be algebra morphisms such that, for any pair $(a, b) \in A \times B$, the relation $f(a)g(b) = g(b)f(a)$ holds in C. Then there exists a unique morphism of algebras $f \otimes g : A \otimes B \to C$ such that $(f \otimes g) \circ i_A = f$ and $(f \otimes g) \circ i_B = g$.*

We can rephrase Proposition 4.1 by saying that $\mathrm{Hom}_{Alg}(A \otimes B, C)$ is the subset of $\mathrm{Hom}_{Alg}(A, C) \times \mathrm{Hom}_{Alg}(B, C)$ consisting of all pairs (f, g) of morphisms whose images commute in C. In particular, if C is *commutative* we have

$$\mathrm{Hom}_{Alg}(A \otimes B, C) \cong \mathrm{Hom}_{Alg}(A, C) \times \mathrm{Hom}_{Alg}(B, C). \tag{4.3}$$

PROOF. Any element of $A \otimes B$ is a finite sum of elements of the form $a \otimes b$. Therefore, by (4.2), $f \otimes g$ (if it exists) has to be of the form

$$(f \otimes g)(a \otimes b) = (f \otimes g)(i_A(a))(f \otimes g)(i_B(b)) = f(a)g(b).$$

This proves the uniqueness assertion. As for the existence of the map $f \otimes g$, one checks that the previous formula defines an algebra morphism. This

uses the commutativity assumption as follows:

$$\begin{aligned}(f \otimes g)(a \otimes b)(f \otimes g)(a' \otimes b') &= f(a)g(b)f(a')g(b') \\ &= f(a)f(a')g(b)g(b') \\ &= f(aa')g(bb') \\ &= (f \otimes g)(aa' \otimes bb').\end{aligned}$$

□

We apply Proposition 4.1 to a situation encountered in Chapter I.

Proposition II.4.2. *Let $A = k\{X\}/I$ be a quotient of the free algebra on a set X. Take two copies X' and X'' of X. Let I' and I'' be the corresponding ideals in $k\{X'\}$ and $k\{X''\}$. Then the tensor product algebra $A \otimes A$ is isomorphic to the algebra*

$$A^{\otimes 2} = k\{X' \sqcup X''\}/(I', I'', X'X'' - X''X')$$

where $X' \sqcup X''$ denotes the disjoint union of the two copies and where $X'X'' - X''X'$ is the two-sided ideal generated by all elements of the form $x'x'' - x''x'$ with $x' \in X'$ and $x'' \in X''$.

PROOF. For any $x \in X$ we denote the corresponding copy in X' [resp. in X''] by x' [resp. by x'']. Setting $\varphi'(x) = x'$ and $\varphi''(x) = x''$ defines algebra morphisms $\varphi', \varphi'' : A \to A^{\otimes 2}$. Since $x'y'' = y''x'$ by definition of $A^{\otimes 2}$, we have $\varphi'(x)\varphi''(y) = \varphi''(y)\varphi'(x)$ for any pair (x, y) of elements of X. By Proposition 4.1 there exists an algebra morphism $\varphi : A \otimes A \to A^{\otimes 2}$ such that $\varphi(x \otimes y) = x'y''$.

Conversely, we get an algebra morphism ψ from $A^{\otimes 2}$ to $A \otimes A$ by setting $\psi(x') = x \otimes 1$ and $\psi(x'') = 1 \otimes x$ where $x' \in X'$ and $x'' \in X''$. One easily checks that φ and ψ are inverse of each other. □

We retain from the previous statement that one passes from $A^{\otimes 2}$ to $A \otimes A$ by replacing the copy x' of x by $x \otimes 1$ and the copy x'' by $1 \otimes x$ and vice versa. Let us apply this recipe to the constructions of I.4–5. Denoting $M(2)$, $GL(2)$ or $SL(2)$ by G, we see that in all three cases the algebra $G^{\otimes 2}$ defined in I.4–5 is isomorphic to the tensor product algebra $G \otimes G$. We can thus rewrite the map Δ of Proposition I.4.1 as the algebra morphism from G to $G \otimes G$ determined by

$$\Delta(a) = a \otimes a + b \otimes c, \qquad \Delta(b) = a \otimes b + b \otimes d,$$

$$\Delta(c) = c \otimes a + d \otimes c, \qquad \Delta(d) = c \otimes b + d \otimes d.$$

We rewrite these four relations in the compact matrix form

$$\Delta\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \Delta(a) & \Delta(b) \\ \Delta(c) & \Delta(d) \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{4.4}$$

Lemma I.5.2 implies that

$$\Delta(ad-bc) = (ad-bc)\otimes(ad-bc). \tag{4.5}$$

II.5 Tensor and Symmetric Algebras

Let V be a vector space. Define $T^0(V) = k$, $T^1(V) = V$ and $T^n(V) = V^{\otimes n}$ (the tensor product of n copies of V) if $n > 1$. The canonical isomorphisms

$$T^n(V) \otimes T^m(V) \cong T^{n+m}(V)$$

induce an associative product on the vector space $T(V) = \oplus_{n\geq 0} T^n(V)$. Equipped with this algebra structure, $T(V)$ is called the *tensor algebra* of V. The product in $T(V)$ is explicitly given by

$$(x_1 \otimes \ldots \otimes x_n)(x_{n+1} \otimes \ldots \otimes x_{n+m}) = x_1 \otimes \ldots \otimes x_n \otimes x_{n+1} \otimes \ldots \otimes x_{n+m} \tag{5.1}$$

where $x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m}$ are elements of V. The unit for this product is the image of the unit element 1 in $k = T^0(V)$. Let i_V be the canonical embedding of $V = T^1(V)$ into $T(V)$. By (5.1) we have

$$x_1 \otimes \ldots \otimes x_n = i_V(x_1) \ldots i_V(x_n), \tag{5.2}$$

which allows us to set

$$x_1 \ldots x_n = x_1 \otimes \ldots \otimes x_n \tag{5.3}$$

whenever $x_1, \ldots, x_n$ are elements of V.

Proposition II.5.1. (a) *The algebra $T(V)$ is graded such that $T^n(V)$ is the subspace of degree n homogeneous elements.*

(b) *For any algebra A and any linear map $f : V \to A$, there exists a unique algebra morphism $\bar{f} : T(V) \to A$ such that $\bar{f} \circ i_V = f$. Consequently, the map $\bar{f} \mapsto \bar{f} \circ i_V$ is a bijection*

$$\mathrm{Hom}_{Alg}(T(V), A) \cong \mathrm{Hom}(V, A). \tag{5.4}$$

(c) *Let I be an indexing set for a basis of the vector space V. Then the tensor algebra $T(V)$ is isomorphic to the free algebra $k\{I\}$.*

Proof. Part (a) is clear. Let us prove Part (b). If $\bar{f}$ exists, it has to be of the form

$$\bar{f}(x_1 \ldots x_n) = f(x_1) \ldots f(x_n)$$

in view of (5.3). This proves the uniqueness of $\bar{f}$. As for its existence, one checks immediately that the previous formula defines an algebra morphism from $T(V)$ into A.

(c) By Corollary 1.5, if $\{e_i\}_{i\in I}$ is a basis of V, then $\{e_{i_1} \ldots e_{i_n}\}_{i_1,\ldots,i_n \in I}$ is a basis of the vector space $T^n(V)$. When n runs over the set of non-negative integers we get a basis of $T(V)$ which is clearly in bijection with a basis of $k\{I\}$. This bijection induces an isomorphism between both vector spaces. The product on $T(V)$ corresponds to the concatenation in $k\{I\}$ under this isomorphism.

Let us give another, less pedestrian, proof of Part (c). By (1.5), (1.8), (5.4) and (I.2.2) we have the following chain of natural bijections:

$$\begin{aligned}
\mathrm{Hom}_{Alg}(T(V), A) &\cong \mathrm{Hom}(V, A) \\
&\cong \mathrm{Hom}\Big(\bigoplus_{i\in I} ke_i, A\Big) \\
&\cong \prod_{i\in I} \mathrm{Hom}(ke_i, A) \\
&\cong \mathrm{Hom}_{Set}(I, A) \\
&\cong \mathrm{Hom}_{Alg}(k\{I\}, A).
\end{aligned}$$

Let α be the composition of these bijections. First, take $A = T(V)$ and define $\varphi = \alpha(\mathrm{id}_{T(V)})$; this is an algebra morphism from $k\{I\}$ to $T(V)$. Now take $A = k\{I\}$ and define $\psi = \alpha^{-1}(\mathrm{id}_{k\{I\}})$; this is an algebra morphism from $T(V)$ to $k\{I\}$. We claim that φ and ψ are isomorphisms between $T(V)$ and $k\{I\}$. First, observe that the bijection α is natural, which means that for any algebra morphism $f : A \to A'$ we have

$$f \circ \alpha(\omega) = \alpha(f \circ \omega)$$

for any $\omega \in \mathrm{Hom}_{Alg}(T(V), A)$. Let us now compose φ and ψ. On the one hand, we get

$$\psi \circ \varphi = \psi \circ \alpha(\mathrm{id}_{T(V)}) = \alpha(\psi \circ \mathrm{id}_{T(V)}) = \alpha(\psi) = \mathrm{id}_{k\{I\}},$$

whereas on the other hand, we have

$$\alpha(\varphi \circ \psi) = \varphi \circ \alpha(\psi) = \varphi \circ \mathrm{id}_{k\{I\}} = \varphi,$$

whence $\varphi \circ \psi = \alpha^{-1}(\varphi) = \mathrm{id}_{T(V)}$. □

Let us define symmetric algebras. If V is a vector space, the *symmetric algebra* $S(V)$ is the quotient $S(V) = T(V)/I(V)$ of the tensor algebra $T(V)$ by the two-sided ideal $I(V)$ generated by all elements $xy - yx$ where x and y run over V. If $x_1, \ldots, x_n$ are elements of V, we again denote by $x_1 \ldots x_n$ the class of $x_1 \ldots x_n$ in $S(V)$. The image of $T^n(V)$ under the projection of $T(V)$ onto $S(V)$ is denoted $S^n(V)$. Let i_V be the canonical map from $V = T^1(V)$ to $S(V)$.

Proposition II.5.2. (a) *The algebra $S(V)$ is commutative, and is graded such that $S^n(V)$ is the subspace of degree n homogeneous elements.*

(b) *For any algebra A and any linear map $f : V \to A$ such that*

$$f(x)f(y) = f(y)f(x)$$

for any pair (x, y) of elements of V, there exists a unique algebra morphism $\bar{f} : S(V) \to A$ such that $\bar{f} \circ i_V = f$.

(c) *If I is an indexing set for a basis of V, then the symmetric algebra $S(V)$ is isomorphic to the polynomial algebra $k[I]$ on the set I.*

(d) *If V' is another vector space, we have an algebra isomorphism*

$$S(V \oplus V') \cong S(V) \otimes S(V'). \tag{5.5}$$

Part (b) implies that the map $\bar{f} \mapsto \bar{f} \circ i_V$ is a bijection

$$\mathrm{Hom}_{Alg}(S(V), A) \cong \mathrm{Hom}(V, A) \tag{5.6}$$

when the algebra A is *commutative.*

PROOF. We leave (a)–(c) as an exercise. Let us give a short proof of (d). Using (1.5), (4.3) and (5.6), we have the chain of natural bijections

$$\begin{aligned} \mathrm{Hom}_{Alg}(S(V \oplus V'), A) &\cong \mathrm{Hom}(V \oplus V', A) \\ &\cong \mathrm{Hom}(V, A) \times \mathrm{Hom}(V', A) \\ &\cong \mathrm{Hom}_{Alg}(S(V), A) \times \mathrm{Hom}_{Alg}(S(V'), A) \\ &\cong \mathrm{Hom}_{Alg}(S(V) \otimes S(V'), A). \end{aligned}$$

We then successively take A to be $S(V \oplus V')$ and $S(V) \otimes S(V')$, which produces isomorphisms between these algebras, as in the second proof of Part (c) of Proposition 5.1. □

II.6 Exercises

1. If f and f' [resp. g and g'] are composable linear maps, show that

$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g).$$

2. Prove that if f is a surjective linear map, then so is $f \otimes \mathrm{id}_V$ for any vector space V. What about the kernel of $f \otimes \mathrm{id}_V$?

3. Prove that the map λ of (2.2) is injective.

4. Let U, V be finite-dimensional vector spaces, f [resp. g] be an endomorphism of U [resp. of V]. Show that $\mathrm{tr}(f \otimes g) = \mathrm{tr}(f)\,\mathrm{tr}(g)$.

5. Let $A = \bigoplus_{i \geq 0} A_i$ and $A' = \bigoplus_{i \geq 0} A'_i$ be graded algebras. Show that the tensor product algebra $A \otimes A'$ is graded with

$$(A \otimes A')_n = \bigoplus_{i+j=n} A_i \otimes A'_j.$$

6. (*Exterior algebra*) For any vector space V we define the exterior algebra (or Grassmann algebra) $\Lambda(V)$ as the quotient $\Lambda(V) = T(V)/I'(V)$ of $T(V)$ by the two-sided ideal $I'(V)$ generated by the elements $x \otimes x$ where x runs over V. If $x_1, \ldots, x_n$ are elements of V, denote by $x_1 \wedge \ldots \wedge x_n$ the class of $x_1 \otimes \ldots \otimes x_n$ in $\Lambda(V)$. The subspace of $\Lambda(V)$ generated by the elements $x_1 \wedge \ldots \wedge x_n$ is denoted $\Lambda^n(V)$. Let i_V be the canonical map from $V = T^1(V)$ to $\Lambda(V)$. Prove the following statements.

   (a) The algebra $\Lambda(V)$ is graded such that $\Lambda^n(V)$ is the subspace of degree n homogeneous elements.

   (b) For any algebra A and any linear map $f : V \to A$ satisfying $f(x)^2 = 0$ for all $x \in V$, there exists a unique algebra morphism $\bar{f} : \Lambda(V) \to A$ such that $\bar{f} \circ i_V = f$.

   (c) Let I be an *ordered* set indexing a basis $\{e_i\}_{i \in I}$ of V. Then the set $\{e_{i_1} \wedge \ldots \wedge e_{i_n}\}_{i_1 < \ldots < i_n \in I}$ is a basis of $\Lambda^n(V)$.

   (d) Assume V of finite dimension d. Prove that

$$\sum_{n \geq 0} \dim(\Lambda^n(V))\, t^n = (1+t)^d.$$

7. (*Symmetric and antisymmetric tensors*) The symmetric group S_n has a left action on $T^n(V)$ given by

$$\sigma(x_1 \otimes \ldots \otimes x_n) = x_{\sigma^{-1}(1)} \otimes \ldots \otimes x_{\sigma^{-1}(n)}$$

where $\sigma \in S_n$ and $x_1, \ldots, x_n \in V$. Define two endomorphisms Σ (the symmetrization operator) and A (the antisymmetrization operator) of $T^n(V)$ by

$$\Sigma(\alpha) = \sum_{\sigma \in S_n} \sigma(\alpha) \quad \text{and} \quad A(\alpha) = \sum_{\sigma \in S_n} \varepsilon(\sigma)\sigma(\alpha)$$

where $\varepsilon(\sigma)$ is the sign of the permutation σ. A tensor α of $T^n(V)$ is symmetric [resp. antisymmetric] if $\sigma(\alpha) = \alpha$ [resp. $\sigma(\alpha) = \varepsilon(\sigma)\sigma(\alpha)$] for any permutation σ. The subspace of symmetric [resp. antisymmetric] tensors of $T^n(V)$ is denoted $S'_n(V)$ [resp. $\Lambda'_n(V)$]. Prove that

   (a) $\Sigma(T^n(V)) \subset S'_n(V)$ and $A(T^n(V)) \subset \Lambda'_n(V)$,

(b) if $n!$ is invertible in the field k, the previous inclusions are equalities and the composition of the inclusion $S'_n(V) \to T^n(V)$ [resp. of the inclusion $\Lambda'_n(V) \to T^n(V)$] with the canonical projection $T^n(V) \to S^n(V)$ [resp. with the projection $T^n(V) \to \Lambda^n(V)$] is an isomorphism.

8. Let $A \otimes V$ be a free A-module. Prove that the space of A-linear maps from $A \otimes V$ to any A-module W is isomorphic to $\mathrm{Hom}(V, W)$.

II.7 Notes

For more details on the tensor, symmetric and exterior algebras as well as on the subspaces $S'_n(V)$ and $\Lambda'_n(V)$ of Exercise 7, see [Bou70], Chap. 3.

Chapter III
The Language of Hopf Algebras

In this chapter we introduce the fundamental concepts of coalgebras, bialgebras, Hopf algebras and comodules which we shall use extensively in the sequel. We shall also prove that the algebras $GL(2)$ and $SL(2)$ of Chapter I are Hopf algebras.

III.1 Coalgebras

The concept of a coalgebra is dual to the concept of an algebra in the following sense. Paraphrasing the definition of an algebra in I.1, we can say that an algebra is given by a triple (A, μ, η) where A is a vector space and $\mu : A \otimes A \to A$ and $\eta : k \to A$ are linear maps satisfying the following axioms (Ass) and (Un).

(Ass): The square

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\mu \otimes \mathrm{id}} & A \otimes A \\ \downarrow{\scriptstyle \mathrm{id} \otimes \mu} & & \downarrow{\scriptstyle \mu} \\ A \otimes A & \xrightarrow{\mu} & A \end{array} \tag{1.1}$$

commutes.

(Un): The diagram

$$\begin{array}{ccccc} k \otimes A & \xrightarrow{\eta \otimes \mathrm{id}} & A \otimes A & \xleftarrow{\mathrm{id} \otimes \eta} & A \otimes k \\ & \searrow{\scriptstyle \cong} & \downarrow{\scriptstyle \mu} & \swarrow{\scriptstyle \cong} & \\ & & A & & \end{array} \tag{1.2}$$

commutes.

The axiom (Ass) expresses the requirement that the multiplication μ is associative whereas Axiom (Un) means that the element $\eta(1)$ of A is a left and a right unit for μ. The algebra A is *commutative* if, in addition, it satisfies the axiom

(Comm): The triangle

$$\begin{tikzcd} A\otimes A \arrow[rr, "\tau_{A,A}"] \arrow[dr, "\mu"'] & & A\otimes A \arrow[dl, "\mu"] \\ & A & \end{tikzcd} \tag{1.3}$$

commutes, where $\tau_{A,A}$ is the flip switching the factors: $\tau_{A,A}(a\otimes a') = a'\otimes a$.

A morphism of algebras $f : (A, \mu, \eta) \to (A', \mu', \eta')$ is a linear map f from A to A' such that

$$\mu' \circ (f\otimes f) = f\circ\mu \quad \text{and} \quad f\circ\eta = \eta'. \tag{1.4}$$

We now get the definition of a coalgebra by systematically reversing all arrows in the previous diagrams.

Definition III.1.1. (a) *A coalgebra is a triple* (C, Δ, ε) *where* C *is a vector space and* $\Delta : C \to C\otimes C$ *and* $\varepsilon : C \to k$ *are linear maps satisfying the following axioms* (Coass) *and* (Coun).

(Coass)*: The square*

$$\begin{tikzcd} C \arrow[r, "\Delta"] \arrow[d, "\Delta"] & C\otimes C \arrow[d, "\mathrm{id}\otimes\Delta"] \\ C\otimes C \arrow[r, "\Delta\otimes\mathrm{id}"] & C\otimes C\otimes C \end{tikzcd} \tag{1.5}$$

commutes.

(Coun)*: The diagram*

$$\begin{tikzcd} k\otimes C & C\otimes C \arrow[l, "\varepsilon\otimes\mathrm{id}"'] \arrow[r, "\mathrm{id}\otimes\varepsilon"] & C\otimes k \\ & C \arrow[ul, "\cong"] \arrow[u, "\Delta"] \arrow[ur, "\cong"'] & \end{tikzcd} \tag{1.6}$$

commutes. The map Δ *is called the coproduct or the comultiplication while* ε *is called the counit of the coalgebra. The squares* (1.5–1.6) *express that the coproduct* Δ *is coassociative and counital.*

If, furthermore, the triangle (Cocomm)

$$\begin{tikzcd} & C \arrow[dl, "\Delta"'] \arrow[dr, "\Delta"] & \\ C\otimes C \arrow[rr, "\tau_{C,C}"] & & C\otimes C \end{tikzcd} \tag{1.7}$$

commutes, where $\tau_{C,C}$ *is the flip, we say that the coalgebra* C *is cocommutative.*

(b) *Consider two coalgebras* (C, Δ, ε) *and* $(C', \Delta', \varepsilon')$*. A linear map* f *from* C *to* C' *is a morphism of coalgebras or a coalgebra morphism if*

$$(f\otimes f)\circ\Delta = \Delta'\circ f \quad \textit{and} \quad \varepsilon = \varepsilon'\circ f. \tag{1.8}$$

It is easily checked that the composition of two morphisms of coalgebras is again a morphism of coalgebras.

Let us give a few examples of coalgebras.

Example 1. (*The ground coalgebra*) The field k has a natural coalgebra structure with $\Delta(1) = 1\otimes 1$ and $\varepsilon(1) = 1$. Moreover, for any coalgebra (C, Δ, ε), the map $\varepsilon : C \to k$ is a morphism of coalgebras.

Example 2. (*Opposite coalgebra*) For any coalgebra $C = (C, \Delta, \varepsilon)$ set

$$\Delta^{\mathrm{op}} = \tau_{C,C}\circ\Delta. \tag{1.9}$$

Then $(C, \Delta^{\mathrm{op}}, \varepsilon)$ is a coalgebra which we call the opposite coalgebra and denote by C^{cop}.

The next result relates algebras and coalgebras.

Proposition III.1.2. *The dual vector space of a coalgebra is an algebra.*

PROOF. Let (C, Δ, ε) be a coalgebra. Recall the map $\lambda : C^*\otimes C^* \to (C\otimes C)^*$ of Corollary II.2.2. Set $\overline{\lambda} = \lambda\circ\tau_{C^*,C^*}$. Define $A = C^*$, $\mu = \Delta^*\circ\overline{\lambda}$ and $\eta = \varepsilon^*$ where the superscript $*$ on a linear map indicates its transpose. Then (A, μ, η) is an algebra (use the commutative diagrams (1.1–1.2) and (1.5–1.6)). □

Example 3. (*Coalgebra of a set*) Let X be a set and $C = k[X] = \bigoplus_{x\in X} kx$ be the vector space with basis X. We put a coalgebra structure on C by defining

$$\Delta(x) = x\otimes x \quad \text{and} \quad \varepsilon(x) = 1 \tag{1.10}$$

where $x \in X$. The dual algebra C^* is the algebra of functions on X with values in k. Indeed, a linear form f on C is determined by its values on the basis X. Let f' be another linear form. Then

$$(ff')(x) = \mu(f\otimes f')(x) = \overline{\lambda}(f\otimes f')(\Delta(x)) = f(x)f'(x).$$

Finally, the unit of the algebra C^* is given by the constant function ε. We shall later return to this example when X has, in addition, a group structure.

In general, the dual vector space of an algebra does not carry a natural coalgebra structure. Nevertheless, we have the following result in the finite-dimensional case (see also Section 9).

Proposition III.1.3. *The dual vector space of a finite-dimensional algebra has a coalgebra structure.*

PROOF. Let (A, μ, η) be a finite-dimensional algebra. Then the map $\overline{\lambda}$ from $A^*\otimes A^*$ to $(A\otimes A)^*$ is an isomorphism, which allows us to define Δ by

$\Delta = \overline{\lambda}^{-1} \circ \mu^*$. We also set $\varepsilon = \eta^*$. Using the commutative diagrams (1.1–1.2) and (1.5–1.6), one checks that $(A^*, \Delta, \varepsilon)$ is a coalgebra. □

Example 4. (*The matrix coalgebra*) Let $A = M_n(k)$ be the algebra of $n \times n$-matrices with entries in k. Denote by E_{ij} the matrix with all entries equal to 0, except for the (i,j)-entry which is equal to 1. The set of matrices E_{ij} $(1 \leq i, j \leq n)$ is a basis of $M_n(k)$. Let $\{x_{ij}\}$ be the dual basis. Then A^* is the coalgebra defined by

$$\Delta(x_{ij}) = \sum_{k=1}^{n} x_{ik} \otimes x_{kj} \quad \text{and} \quad \varepsilon(x_{ij}) = \delta_{ij}. \tag{1.11}$$

Indeed, we have

$$\varepsilon(x_{ij}) = x_{ij}(\eta(1)) = x_{ij}(\sum_k E_{kk}) = \sum_k \delta_{ik}\delta_{kj} = \delta_{ij}$$

and

$$\begin{aligned}
\mu^*(x_{ij})(E_{k\ell} \otimes E_{mn}) &= x_{ij}(\mu(E_{k\ell} \otimes E_{mn})) \\
&= \delta_{\ell m} x_{ij}(E_{kn}) \\
&= \delta_{\ell m}\delta_{ik}\delta_{jn} \\
&= \sum_p \delta_{ik}\delta_{\ell p}\delta_{pm}\delta_{jn} \\
&= \sum_p x_{ip}(E_{k\ell}) x_{pj}(E_{mn}) \\
&= \overline{\lambda}\Big(\sum_p x_{ip} \otimes x_{pj}\Big)(E_{k\ell} \otimes E_{mn}).
\end{aligned}$$

Example 5. (*Tensor product of coalgebras*) The tensor product $C \otimes C'$ of two coalgebras (C, Δ, ε) and $(C', \Delta', \varepsilon')$ has a coalgebra structure with comultiplication $(\mathrm{id} \otimes \tau_{C,C'} \otimes \mathrm{id}) \circ (\Delta \otimes \Delta')$ and counit $\varepsilon \otimes \varepsilon'$.

We return to Example 3.

Proposition III.1.4. *Let X and Y be two sets and $X \times Y$ be the product set. There exists an isomorphism of coalgebras*

$$k[X] \otimes k[Y] \cong k[X \times Y].$$

PROOF. The isomorphism is given on the basis $\{x \otimes y\}_{(x,y) \in X \times Y}$ of the tensor product $k[X] \otimes k[Y]$ by

$$\psi(x \otimes y) = (x, y). \tag{1.12}$$

It is clear that

$$(\psi \otimes \psi)(\mathrm{id} \otimes \tau \otimes \mathrm{id})(\Delta \otimes \Delta)(x \otimes y) = (x, y) \otimes (x, y) = \Delta\psi(x \otimes y)$$

and $\varepsilon\psi(x \otimes y) = 1 = \varepsilon(x)\varepsilon(y)$, which shows that ψ is a morphism of coalgebras. □

We shall also need the following concept.

Definition III.1.5. *Let (C, Δ, ε) be a coalgebra. A subspace I of C is a coideal if $\Delta(I) \subset I \otimes C + C \otimes I$ and $\varepsilon(I) = 0$.*

When I is a coideal, then Δ factors through a map $\overline{\Delta}$ from C/I to

$$C \otimes C/(I \otimes C + C \otimes I) = C/I \otimes C/I.$$

Similarly, the counit factors through a map $\overline{\varepsilon} : C/I \to k$. Then clearly, the triple $(C/I, \overline{\Delta}, \overline{\varepsilon})$ is a coalgebra. It is called the *quotient-coalgebra*. We shall give examples later.

Notation 1.6. We now present Sweedler's sigma notation which we shall use continually in the sequel. If x is an element of a coalgebra (C, Δ, ε), the element $\Delta(x)$ of $C \otimes C$ is of the form

$$\Delta(x) = \sum_i x_i' \otimes x_i''. \tag{1.13}$$

In order to get rid of the subscripts, we henceforth agree to write the sum (1.13) in the form

$$\Delta(x) = \sum_{(x)} x' \otimes x''. \tag{1.14}$$

Using (1.14) we may express the coassociativity of Δ, i.e., the commutativity of the square (1.5), by

$$\sum_{(x)}\Big(\sum_{(x')} (x')' \otimes (x')''\Big) \otimes x'' = \sum_{(x)} x' \otimes \Big(\sum_{(x'')} (x'')' \otimes (x'')''\Big). \tag{1.15}$$

By convention again, we identify both sides of (1.15) with

$$\sum_{(x)} x' \otimes x'' \otimes x''', \tag{1.16}$$

also written $\sum_{(x)} x^{(1)} \otimes x^{(2)} \otimes x^{(3)}$. If we apply the comultiplication to (1.16), we get the following three equal expressions

$$\sum_{(x)} \Delta(x') \otimes x'' \otimes x''', \quad \sum_{(x)} x' \otimes \Delta(x'') \otimes x''', \quad \sum_{(x)} x' \otimes x'' \otimes \Delta(x''')$$

which we agree to write

$$\sum_{(x)} x' \otimes x'' \otimes x''' \otimes x'''' \tag{1.17}$$

or $\sum_{(x)} x^{(1)} \otimes x^{(2)} \otimes x^{(3)} \otimes x^{(4)}$. More generally, let $\Delta^{(n)} : C \to C^{\otimes(n+1)}$ be defined inductively on $n \geq 1$ by $\Delta^{(1)} = \Delta$ and

$$\Delta^{(n)} = (\Delta \otimes \mathrm{id}_{C^{\otimes(n-1)}}) \circ \Delta^{(n-1)} = (\mathrm{id}_{C^{\otimes(n-1)}} \otimes \Delta) \circ \Delta^{(n-1)}. \tag{1.18}$$

Then by convention, we write

$$\Delta^{(n)}(x) = \sum_{(x)} x^{(1)} \otimes \cdots \otimes x^{(n+1)}. \tag{1.19}$$

These conventions and the coassociativity of Δ imply for instance that

$$\begin{aligned}(\mathrm{id}_C \otimes \Delta \otimes \mathrm{id}_{C^{\otimes 2}})\Big(\sum_{(x)} x^{(1)} \otimes x^{(2)} \otimes x^{(3)} \otimes x^{(4)}\Big) \\ = \sum_{(x)} x^{(1)} \otimes x^{(2)} \otimes x^{(3)} \otimes x^{(4)} \otimes x^{(5)}\end{aligned} \tag{1.20}$$

Using the conventions (1.14), the condition (1.6) for counitality may be reformulated for any $x \in C$ as

$$\sum_{(x)} \varepsilon(x')x'' = x = \sum_{(x)} x'\varepsilon(x''). \tag{1.21}$$

As a consequence of (1.21) and of (1.19), we get identities such as

$$\sum_{(x)} x^{(1)} \otimes \varepsilon(x^{(2)}) \otimes x^{(3)} \otimes x^{(4)} \otimes x^{(5)} = \sum_{(x)} x^{(1)} \otimes x^{(2)} \otimes x^{(3)} \otimes x^{(4)}. \tag{1.22}$$

Indeed, the left-hand side may be rewritten as

$$\sum_{(x)} x^{(1)} \otimes (\varepsilon \otimes \mathrm{id})(\Delta(x^{(2)})) \otimes x^{(3)} \otimes x^{(4)}.$$

Then apply (1.21).

The coalgebra C is cocommutative if

$$\sum_{(x)} x' \otimes x'' = \sum_{(x)} x'' \otimes x' \tag{1.23}$$

for all $x \in C$.

The left Relation (1.8) defining a coalgebra morphism can be reformulated as

$$\sum_{(x)} f(x') \otimes f(x'') = \sum_{(f(x))} f(x)' \otimes f(x)''. \tag{1.24}$$

The comultiplication of the tensor product $C \otimes C'$ of the coalgebras C and C' (see Example 5) is given for $x \in C$ and $y \in C'$ by

$$\Delta(x \otimes y) = \sum_{(x \otimes y)} (x \otimes y)' \otimes (x \otimes y)'' = \sum_{(x)(y)} (x' \otimes y') \otimes (x'' \otimes y''). \tag{1.25}$$

We invite the reader to play with Sweedler's sigma notation in order to acquire some familiarity with this most useful convention.

III.2 Bialgebras

Let H be a vector space equipped simultaneously with an algebra structure (H, μ, η) and a coalgebra structure (H, Δ, ε). Let us discuss two compatibility conditions between these two structures. We give $H \otimes H$ the induced structures of a tensor product of algebras (see II.4) and of a tensor product of coalgebras (see Section 1, Example 5).

Theorem III.2.1. *The following two statements are equivalent.*

(i) *The maps μ and η are morphisms of coalgebras.*

(ii) *The maps Δ and ε are morphisms of algebras.*

Proof. It consists essentially in writing down the commutative diagrams expressing both statements. The fact that μ is a morphism of coalgebras is equivalent to the commutativity of the two squares

$$\begin{array}{ccc} H \otimes H & \xrightarrow{\mu} & H \\ \big\downarrow{\scriptstyle (\mathrm{id}\otimes\tau\otimes\mathrm{id})(\Delta\otimes\Delta)} & & \big\downarrow{\scriptstyle \Delta} \\ (H \otimes H) \otimes (H \otimes H) & \xrightarrow{\mu\otimes\mu} & H \otimes H \end{array} \qquad \begin{array}{ccc} H \otimes H & \xrightarrow{\varepsilon\otimes\varepsilon} & k \otimes k \\ \big\downarrow{\scriptstyle \mu} & & \big\downarrow{\scriptstyle \mathrm{id}} \\ H & \xrightarrow{\varepsilon} & k \end{array}$$

whereas the fact that η is a morphism of coalgebras is expressed by the commutativity of the two diagrams

$$\begin{array}{ccc} k & \xrightarrow{\eta} & H \\ \big\downarrow{\scriptstyle \mathrm{id}} & & \big\downarrow{\scriptstyle \Delta} \\ k \otimes k & \xrightarrow{\eta\otimes\eta} & H \otimes H \end{array} \qquad \begin{array}{ccc} k & \xrightarrow{\eta} & H \\ & {\searrow}{\scriptstyle \mathrm{id}} \quad {\swarrow}{\scriptstyle \varepsilon} & \\ & k & \end{array}$$

□

Observe that these four commutative diagrams are exactly the same as the following four diagrams whose commutativity express the fact that Δ and ε are morphisms of algebras:

$$\begin{array}{ccc} H \otimes H & \xrightarrow{\Delta\otimes\Delta} & (H \otimes H) \otimes (H \otimes H) \\ \big\downarrow{\scriptstyle \mu} & & \big\downarrow{\scriptstyle (\mu\otimes\mu)(\mathrm{id}\otimes\tau\otimes\mathrm{id})} \\ H & \xrightarrow{\Delta} & H \otimes H \end{array} \qquad \begin{array}{ccc} k & \xrightarrow{\eta} & H \\ \big\downarrow{\scriptstyle \mathrm{id}} & & \big\downarrow{\scriptstyle \Delta} \\ k \otimes k & \xrightarrow{\eta\otimes\eta} & H \otimes H \end{array}$$

and

$$\begin{tikzcd} H \otimes H \arrow[r, "\varepsilon\otimes\varepsilon"] \arrow[d, "\mu"] & k \otimes k \arrow[d, "\mathrm{id}"] \\ H \arrow[r, "\varepsilon"] & k \end{tikzcd} \qquad \begin{tikzcd} k \arrow[rr, "\eta"] \arrow[dr, "\mathrm{id}"'] & & H \arrow[dl, "\varepsilon"] \\ & k & \end{tikzcd}$$

This leads to the following definition.

Definition III.2.2. *A bialgebra is a quintuple $(H, \mu, \eta, \Delta, \varepsilon)$ where (H, μ, η) is an algebra and (H, Δ, ε) is a coalgebra verifying the equivalent conditions of Theorem 2.1. A morphism of bialgebras is a morphism for the underlying algebra and coalgebra structures.*

In the sequel, we shall mainly use Condition (ii) of Theorem 2.1 to define a bialgebra structure. Using the conventions of 1.6, we see that the condition $\Delta(xy) = \Delta(x)\Delta(y)$ is expressed for any pair (x, y) of elements in a bialgebra by

$$\sum_{(xy)} (xy)' \otimes (xy)'' = \sum_{(x)(y)} x'y' \otimes x''y''. \tag{2.1}$$

We also have

$$\Delta(1) = 1 \otimes 1, \quad \varepsilon(xy) = \varepsilon(x)\varepsilon(y), \quad \varepsilon(1) = 1. \tag{2.2}$$

The following proposition is easy to check.

Proposition III.2.3. *Let $H = (H, \mu, \eta, \Delta, \varepsilon)$ be a bialgebra. Then*

$$H^{\mathrm{op}} = (H, \mu^{\mathrm{op}}, \eta, \Delta, \varepsilon), \quad H^{\mathrm{cop}} = (H, \mu, \eta, \Delta^{\mathrm{op}}, \varepsilon),$$

and $H^{\mathrm{op\,cop}} = (H, \mu^{\mathrm{op}}, \eta, \Delta^{\mathrm{op}}, \varepsilon)$ are bialgebras.

Example 1. By Propositions 1.2–1.3 the dual vector space H^* of a finite-dimensional bialgebra H has a natural bialgebra structure.

Example 2. In Example 3 of Section 1 we associated a coalgebra $k[X]$ to a set X. Assume now that X comes with a unital *monoid* structure, i.e., with an associative map $\mu : X \times X \to X$ having a left and right unit e. The map μ induces an algebra structure on $k[X]$ with unit e. We have

$$\Delta(xy) = xy \otimes xy = (x \otimes x)(y \otimes y) = \Delta(x)\Delta(y)$$

and $\varepsilon(xy) = 1 = \varepsilon(x)\varepsilon(y)$, which implies that the maps Δ and ε are morphisms of algebras. Thus $k[X]$ becomes a bialgebra.

If, in addition, X is a finite set, then the dual of $k[X]$ also is a bialgebra. We have already observed that the algebra structure of the dual is the usual algebra structure of the space of k-valued functions on X. An easy computation shows that the comultiplication and the counit on the algebra of functions are given by

$$\Delta(f)(x \otimes y) = f(xy) \quad \text{and} \quad \varepsilon(f) = f(e). \tag{2.3}$$

Example 3. (*The bialgebra $M(n)$*) Let $M(n) = k[x_{11}, \ldots, x_{nn}]$ be the polynomial algebra in n^2 variables $\{x_{ij}\}_{1\leq i,j\leq n}$. For all i, j, set

$$\Delta(x_{ij}) = \sum_{k=1}^{n} x_{ik} \otimes x_{kj} \quad \text{and} \quad \varepsilon(x_{ij}) = \delta_{ij}. \tag{2.4}$$

These formulas define morphisms of algebras $\Delta : M(n) \to M(n) \otimes M(n)$ and $\varepsilon : M(n) \to k$ equipping $M(n)$ with a bialgebra structure. When $n = 2$, one recovers the bialgebra $M(2)$ of I.4.

We now endow the tensor algebra with a bialgebra structure.

Theorem III.2.4. *Given a vector space V, there exists a unique bialgebra structure on the tensor algebra $T(V)$ such that $\Delta(v) = 1 \otimes v + v \otimes 1$ and $\varepsilon(v) = 0$ for any element v of V. This bialgebra structure is cocommutative and for all $v_1, \ldots, v_n \in V$ we have*

$$\varepsilon(v_1 \ldots v_n) = 0 \tag{2.5}$$

and $\Delta(v_1 \ldots v_n)$

$$= 1 \otimes v_1 \ldots v_n + \sum_{p=1}^{n-1} \sum_{\sigma} v_{\sigma(1)} \cdots v_{\sigma(p)} \otimes v_{\sigma(p+1)} \cdots v_{\sigma(n)} + v_1 \ldots v_n \otimes 1 \tag{2.6}$$

where σ runs over all permutations of the symmetric group S_n such that

$$\sigma(1) < \sigma(2) \ldots < \sigma(p) \quad \text{and} \quad \sigma(p+1) < \sigma(p+2) \ldots < \sigma(n).$$

Such a permutation σ is called a *$(p, n-p)$-shuffle.*

PROOF. By universality of the tensor algebra, there exist unique algebra morphisms $\Delta : T(V) \to T(V) \otimes T(V)$ and $\varepsilon : T(V) \to k$ such that their restrictions to V are given by the formulas of the theorem. Now consider several elements $v_1, \ldots, v_n$ in V. Formula (2.5) is a trivial consequence of the multiplicativity of ε.

Let us now compute $\Delta(v_1 \ldots v_n)$. We shall do this by induction on n. Formula (2.6) holds for $n = 1$ by definition. Suppose it holds up to $n-1 \geq 1$. Then we have the series of equalities

$$\begin{aligned} &\Delta(v_1 \ldots v_n) \\ &= \Delta(v_1 \ldots v_{n-1})\Delta(v_n) \end{aligned}$$

$$\begin{aligned}
&= \Delta(v_1 \dots v_{n-1})(1 \otimes v_n + v_n \otimes 1)\\
&= \Big(1 \otimes v_1 \dots v_{n-1} + \sum_{p=1}^{n-2} \sum_{\sigma} v_{\sigma(1)} \cdots v_{\sigma(p)} \otimes v_{\sigma(p+1)} \cdots v_{\sigma(n-1)}\\
&\qquad + v_1 \dots v_{n-1} \otimes 1\Big)(1 \otimes v_n + v_n \otimes 1)\\
&= 1 \otimes v_1 \dots v_n + \sum_{p=1}^{n-2} \sum_{\sigma} v_{\sigma(1)} \cdots v_{\sigma(p)} \otimes v_{\sigma(p+1)} \cdots v_{\sigma(n-1)} v_n\\
&\quad + v_1 \dots v_{n-1} \otimes v_n + v_n \otimes v_1 \dots v_{n-1}\\
&\quad + \sum_{p=1}^{n-2} \sum_{\sigma} v_{\sigma(1)} \cdots v_{\sigma(p)} v_n \otimes v_{\sigma(p+1)} \cdots v_{\sigma(n-1)} + v_1 \dots v_n \otimes 1
\end{aligned}$$

where σ runs over all $(p, n-1-p)$-shuffles of S_{n-1}. Let us rewrite the last sum in the form

$$\begin{aligned}
1 \otimes v_1 \dots v_n &+ \sum_{p=1}^{n-2} \sum_{\rho} v_{\rho(1)} \cdots v_{\rho(p)} \otimes v_{\rho(p+1)} \cdots v_{\rho(n-1)} v_n\\
&+ v_1 \dots v_{n-1} \otimes v_n + v_n \otimes v_1 \dots v_{n-1}\\
+ \sum_{p=2}^{n-1} \sum_{\tau} & v_{\tau(1)} \cdots v_{\tau(p-1)} v_n \otimes v_{\tau(p)} \cdots v_{\tau(n-1)} + v_1 \dots v_n \otimes 1
\end{aligned}$$

where ρ runs over all $(p, n-1-p)$-shuffles of S_{n-1} and τ runs over all $(p-1, n-p)$-shuffles permuting the set $\{1, \dots, n\} \setminus \{p\}$. Now observe that if $\sigma \in S_n$ is a $(p, n-p)$-shuffle, then either $\sigma(n) = n$, hence the restriction ρ of σ to S_{n-1} is a $(p, n-1-p)$-shuffle, or $\sigma(p) = n$, hence $\tau = \sigma$ acting on $\{1, \dots, n\} \setminus \{p\}$ is a $(p-1, n-p)$-shuffle. This completes the proof of (2.6).

It remains to prove the coassociativity, the counitality and the cocommutativity of Δ. The counitality results from an easy computation using (2.5) and (2.6). The cocommutativity is a consequence of the fact that the permutation

$$\begin{pmatrix} 1 & 2 & \dots & p & p+1 & p+2 & \dots & n \\ p+1 & p+2 & \dots & n & 1 & 2 & \dots & p \end{pmatrix}$$

switches $(p, n-p)$-shuffles and $(n-p, p)$-shuffles. As for the coassociativity, one may check it directly using (2.6). But, we rather observe that $\Delta : T(V) \to T(V) \otimes T(V)$ is induced by the diagonal map $\delta(v) = (v, v)$ from V into $V \oplus V$. The coassociativity of Δ then results from the obvious relation $(\delta \otimes \mathrm{id}) \circ \delta = (\mathrm{id} \otimes \delta) \circ \delta$. □

We now introduce the concept of a primitive element.

Definition III.2.5. *Let (C, Δ, ε) be a coalgebra. An element x of C is primitive if we have*

$$\Delta(x) = 1 \otimes x + x \otimes 1.$$

We denote by $\mathrm{Prim}(C)$ *the subspace of all primitive elements of* C.

Proposition III.2.6. *If x is a primitive element of a bialgebra, then we have $\varepsilon(x) = 0$. If y is another one, then the commutator $[x, y] = xy - yx$ is primitive too.*

PROOF. By definition of the counit and of a primitive element we have

$$x = \varepsilon(1)x + \varepsilon(x)1 = x + \varepsilon(x)1.$$

The vanishing of $\varepsilon(x)$ follows immediately. As for the second assertion, we have

$$\Delta(xy) = (1 \otimes x + x \otimes 1)(1 \otimes y + y \otimes 1) = 1 \otimes xy + x \otimes y + y \otimes x + xy \otimes 1.$$

We deduce

$$\Delta([x, y]) = 1 \otimes [x, y] + [x, y] \otimes 1,$$

which implies that $[x, y]$ is primitive. □

The generators $v \in V$ of the tensor algebra $T(V)$ are primitive by Theorem 2.4. Let H be a bialgebra and $x_1, \dots, x_n$ be *primitive* elements of H. Consider a vector space V with basis $\{v_1, \dots, v_n\}$. There is a unique algebra morphism f from the tensor algebra $T(V)$ to H such that $f(v_i) = x_i$ for all i.

Proposition III.2.7. *The map $f : T(V) \to H$ is a morphism of bialgebras.*

PROOF. We have to check that

$$\varepsilon(f(\xi)) = \varepsilon(\xi) \quad \text{and} \quad (f \otimes f)\Delta(\xi) = \Delta(f(\xi)) \tag{2.7}$$

for all $\xi \in T(V)$. Since all maps involved in (2.7) are algebra maps, it is enough to check (2.7) when $\xi = v \in V$. In this case (2.7) holds because x_i is primitive and we have Proposition 2.6. □

As a consequence of Proposition 2.7, we see that for any set $\{x_1, \dots, x_n\}$ of primitive elements in a bialgebra, $\Delta(x_1, \dots, x_n)$ is given by Formula (2.6) of Theorem 2.4 after replacing v_i by x_i.

III.3 Hopf Algebras

Given an algebra (A, μ, η) and a coalgebra (C, Δ, ε) we define a bilinear map, the *convolution*, on the vector space $\mathrm{Hom}(C, A)$ of linear maps from C to A. By definition, if f, g are such linear maps, then the convolution $f \star g$ is the composition of the maps

$$C \xrightarrow{\Delta} C \otimes C \xrightarrow{f \otimes g} A \otimes A \xrightarrow{\mu} A. \tag{3.1}$$

Using Sweedler's sigma notation of 1.6, we have

$$(f \star g)(x) = \sum_{(x)} f(x')g(x'') \tag{3.2}$$

for any element $x \in C$. The convolution is clearly bilinear.

Proposition III.3.1. (a) *The triple* $(\mathrm{Hom}(C, A), \star, \eta \circ \varepsilon)$ *is an algebra.*
(b) *The map* $\lambda_{C,A} : A \otimes C^* \to \mathrm{Hom}(C, A)$ *of Corollary* II.2.3 *is a morphism of algebras where* $A \otimes C^*$ *is the tensor product algebra of* A *and of the algebra* C^* *dual to the coalgebra* C.

PROOF. (a) By (3.2), by the associativity of the product in A and by the coassociativity of the coproduct in C we have

$$\Big((f \star g) \star h\Big)(x) = \sum_{(x)} f(x')g(x'')h(x''') = \Big(f \star (g \star h)\Big)(x).$$

This proves that the convolution is associative. The map $\eta \circ \varepsilon$ is a left unit for the convolution in view of

$$((\eta\varepsilon) \star f)(x) = \sum_{(x)} \varepsilon(x')f(x'') = f\Big(\sum_{(x)} \varepsilon(x')x''\Big) = f(x),$$

which results from (1.21). One proves similarly that $\eta \circ \varepsilon$ is a right unit.
(b) Let $a, b \in A$ and $\alpha, \beta \in C^*$. Then for $x \in C$ we have

$$\begin{aligned}\Big(\lambda_{C,A}(a \otimes \alpha) \star \lambda_{C,A}(b \otimes \beta)\Big)(x) &= \sum_{(x)} \alpha(x')\beta(x'')\, ab \\ &= (\alpha\beta)(x)\, ab \\ &= \Big(\lambda_{C,A}(ab \otimes \alpha\beta)\Big)(x).\end{aligned}$$

This proves that $\lambda_{C,A}$ preserves the product. As for the unit, we have

$$\Big(\lambda_{C,A}(1 \otimes \varepsilon)\Big)(x) = \varepsilon(x)1 = (\eta \circ \varepsilon)(x).$$

□

Example 1. When $A = k$ the algebra structure $(\mathrm{Hom}(C, k), \star, \eta \circ \varepsilon)$ on the dual space C^* is the same as the one defined in Proposition 1.2.

When $(H, \mu, \eta, \Delta, \varepsilon)$ is a bialgebra we may consider the case $C = A = H$ and thus define the convolution on the vector space $\mathrm{End}(H)$ of endomorphisms of H.

Definition III.3.2. *Let* $(H, \mu, \eta, \Delta, \varepsilon)$ *be a bialgebra. An endomorphism* S *of* H *is called an antipode for the bialgebra* H *if*

$$S \star \mathrm{id}_H = \mathrm{id}_H \star S = \eta \circ \varepsilon.$$

A Hopf algebra is a bialgebra with an antipode. A morphism of Hopf algebras is a morphism between the underlying bialgebras commuting with the antipodes.

A bialgebra does not necessarily have an antipode. But if it does, it has only one. Indeed, if S and S' are antipodes, then

$$S = S \star (\eta\varepsilon) = S \star (\mathrm{id}_H \star S') = (S \star \mathrm{id}_H) \star S' = (\eta\varepsilon) \star S' = S'.$$

A Hopf algebra with an antipode S will be denoted by $(H, \mu, \eta, \Delta, \varepsilon, S)$.
Using Sweedler's convention 1.6, we see that an antipode satisfies the relations

$$\sum_{(x)} x'S(x'') = \varepsilon(x)1 = \sum_{(x)} S(x')x'' \tag{3.3}$$

for all $x \in H$. In any Hopf algebra we have relations such as

$$\begin{aligned}\sum_{(x)} x^{(1)} \otimes x^{(2)} \otimes S(x^{(3)}) \otimes x^{(4)} \otimes x^{(5)} &= \sum_{(x)} x^{(1)} \otimes \varepsilon(x^{(2)}) \otimes x^{(3)} \otimes x^{(4)} \\ &= \sum_{(x)} x^{(1)} \otimes x^{(2)} \otimes x^{(3)}.\end{aligned}$$

The first equality follows from (3.3), i.e., by definition of the antipode while the second one follows from (1.21), i.e., from the Axiom (Coun). Such computations will be performed later without further explanations.
We state the counterpart of Example 1 of Section 2.

Proposition III.3.3. *Let* H *be a finite-dimensional Hopf algebra with antipode* S. *Then the bialgebra* H^* *is a Hopf algebra with antipode* S^*.

PROOF. The endomorphism S^* of H^* is the transpose of S. Let us prove the first equality in (3.3). For all $\alpha \in H^*$ and $x \in H$ we have

$$\begin{aligned}\Big(\sum_{(\alpha)} \alpha' S^*(\alpha'')\Big)(x) &= \sum_{(\alpha)(x)} \alpha'(x')S^*(\alpha'')(x'') \\ &= \sum_{(\alpha)(x)} \alpha'(x')\alpha''(Sx'') \\ &= \alpha\Big(\sum_{(x)} x'(Sx'')\Big) \\ &= \alpha(\eta\varepsilon(x)) \\ &= \varepsilon^*\eta^*(\alpha)(x).\end{aligned}$$

One shows similarly that $\sum_{(\alpha)} S^*(\alpha')\alpha'' = \varepsilon^*\eta^*(\alpha)$. □

Example 2. Let G be a monoid and $k[G]$ the bialgebra of Section 2, Example 2. Then $k[G]$ has an antipode if and only if any element x of G has an inverse, i.e., if and only if G is a group. Indeed, if S exists, by definition of Δ we must have

$$xS(x) = S(x)x = \varepsilon(x)1 = 1$$

for any $x \in G$. This implies that $S(x) = x^{-1}$ for $x \in G$.

We state a few important properties of the antipode.

Theorem III.3.4. *Let $(H, \mu, \eta, \Delta, \varepsilon, S)$ be a Hopf algebra.*

(a) *Then S is a bialgebra morphism from H to $H^{\mathrm{op\,cop}}$, i.e., we have*

$$S(xy) = S(y)S(x), \quad S(1) = 1 \tag{3.4}$$

for all $x, y \in H$ and

$$(S \otimes S)\Delta = \Delta^{\mathrm{op}} S, \quad \varepsilon \circ S = \varepsilon. \tag{3.5}$$

(b) *The following three statements are equivalent:*
 (i) *we have $S^2 = \mathrm{id}_H$,*
 (ii) *for all $x \in H$ we have $\sum_{(x)} S(x'')x' = \varepsilon(x)1$,*
 (iii) *for all $x \in H$ we have $\sum_{(x)} x''S(x') = \varepsilon(x)1$.*

(c) *If H is commutative or cocommutative, then $S^2 = \mathrm{id}_H$.*

The left relation in (3.5) can be reformulated under Sweedler's convention 1.6 as

$$\sum_{(S(x))} S(x)' \otimes S(x)'' = \sum_{(x)} S(x'') \otimes S(x'). \tag{3.6}$$

PROOF. (a) Let us start with (3.4). Define maps ν, ρ in $\mathrm{Hom}(H \otimes H, H)$ by

$$\nu(x \otimes y) = S(y)S(x) \quad \text{and} \quad \rho(x \otimes y) = S(xy)$$

where $x, y \in H$. We have to show that $\rho = \nu$. It is enough to prove that $\rho \star \mu = \mu \star \nu = \eta\varepsilon$. Now, by (1.21), (2.1) and (3.2)

$$\begin{aligned}
(\rho \star \mu)(x \otimes y) &= \sum_{(x \otimes y)} \rho((x \otimes y)')\mu((x \otimes y)'') \\
&= \sum_{(x)(y)} \rho(x' \otimes y')\mu(x'' \otimes y'') \\
&= \sum_{(x)(y)} S(x'y')x''y'' \\
&= \sum_{(xy)} S((xy)')(xy)'' \\
&= \eta\varepsilon(xy).
\end{aligned}$$

On the other hand, we have

$$\begin{aligned}
(\mu \star \nu)(x \otimes y) &= \sum_{(x \otimes y)} \mu((x \otimes y)')\,\nu((x \otimes y)'') \\
&= \sum_{(x)(y)} x'y'S(y'')S(x'') \\
&= \sum_{(x)} x'\Big(\sum_{(y)} y'S(y'')\Big)S(x'') \\
&= \sum_{(x)} x'\varepsilon(y)S(x'') \\
&= \eta\varepsilon(x)\eta\varepsilon(y) \\
&= \eta\varepsilon(xy),
\end{aligned}$$

which is the same.

Applying $(\mathrm{id} \star S)(x) = \eta\varepsilon(x)$ to $x = 1$, one gets $S(1) = 1$. This proves (3.4).

Let us deal with (3.5). It is equivalent to prove $\Delta \circ S = (S \otimes S) \circ \Delta^{\mathrm{op}}$. We set $\rho = \Delta \circ S$ and $\nu = (S \otimes S) \circ \Delta^{\mathrm{op}}$. These are linear maps from H to $H \otimes H$. We wish to show that $\rho = \nu$. This will follow from $\rho \star \Delta = \Delta \star \nu = (\eta \otimes \eta)\varepsilon$, which we prove now. On the one hand, by (1.21)

$$\begin{aligned}
(\rho \star \Delta)(x) &= \sum_{(x)} \Delta(S(x'))\Delta(x'') = \Delta\Big(\sum_{(x)} S(x')x''\Big) \\
&= \Delta(\eta\varepsilon(x)) = ((\eta \otimes \eta)\varepsilon)(x)
\end{aligned}$$

for all $x \in H$. On the other hand, we have

$$\begin{aligned}
(\Delta \star \nu)(x) &= \sum_{(x)} \Delta(x')\Big((S \otimes S)(\Delta^{\mathrm{op}}(x''))\Big) \\
&= \sum_{(x)} (x' \otimes x'')\Big(S(x'''') \otimes S(x''')\Big) \\
&= \sum_{(x)} x'S(x'''') \otimes x''S(x''') \\
&= \sum_{(x)} x'S(x''') \otimes \varepsilon(x'')1 \\
&= \sum_{(x)} x'\varepsilon(x'')S(x''') \otimes 1 \\
&= \sum_{(x)} x'S(x'') \otimes 1 \\
&= \varepsilon(x)1 \otimes 1 \\
&= (\eta \otimes \eta)(\varepsilon(x)).
\end{aligned}$$

The fourth and seventh equalities follow from (3.3), the sixth one from (1.21).

We also derive

$$\varepsilon(S(x)) = \varepsilon\Big(S\big(\sum_{(x)} \varepsilon(x')x''\big)\Big) = \varepsilon\Big(\sum_{(x)} \varepsilon(x')S(x'')\Big) = \varepsilon(\eta\varepsilon(x)) = \varepsilon(x)$$

from (1.21). This completes the proof of (3.5).

(b) Let us prove that (ii) implies (i). By uniqueness of the inverse, it is enough to show that S^2 is a right inverse of S for the convolution, just as is id_H. Now, using (3.4) and Condition (ii), we get for all $x \in H$

$$\begin{aligned}(S \star S^2)(x) &= \sum_{(x)} S(x')S^2(x'') = S\Big(\sum_{(x)} S(x'')x'\Big)\\ &= S(\varepsilon(x)1) = \varepsilon(x)S(1) = \varepsilon(x)1.\end{aligned}$$

This implies that $S \star S^2 = \eta\varepsilon$, hence $S^2 = \mathrm{id}_H$. Let us prove the converse implication: if $S^2 = \mathrm{id}_H$ we have

$$\begin{aligned}\sum_{(x)} S(x'')x' &= S^2\Big(\sum_{(x)} S(x'')x'\Big)\\ &= S\Big(\sum_{(x)} S(x')S^2(x'')\Big)\\ &= S\Big(\sum_{(x)} S(x')x''\Big)\\ &= S(\varepsilon(x)1)\\ &= \varepsilon(x)1.\end{aligned}$$

One proves that (i) is equivalent to (iii) in a similar fashion.

(c) Recall Relations (3.3): we have

$$\sum_{(x)} x'S(x'') = \eta\varepsilon(x) = \sum_{(x)} S(x')x''$$

for all $x \in H$. When H is commutative, the first equality becomes

$$\sum_{(x)} S(x'')x' = \eta\varepsilon(x),$$

which implies $S^2 = \mathrm{id}_H$ by Part (b) (ii). When H is cocommutative, the second equality becomes

$$\eta\varepsilon(x) = \sum_{(x)} S(x'')x'$$

which again implies $S^2 = \mathrm{id}_H$ in view of Part (b) (iii). □

As an immediate consequence of Theorem 3.4, we have the following.

Corollary III.3.5. *Let $H = (H, \mu, \eta, \Delta, \varepsilon, S)$ be a Hopf algebra. Then*

$$H^{\mathrm{op\,cop}} = (H, \mu^{\mathrm{op}}, \eta, \Delta^{\mathrm{op}}, \varepsilon, S)$$

is another Hopf algebra and $S : H \to H^{\mathrm{op\,cop}}$ is a morphism of Hopf algebras. If, moreover, S is an isomorphism with inverse S^{-1}, then

$$H^{\mathrm{op}} = (H, \mu^{\mathrm{op}}, \eta, \Delta, \varepsilon, S^{-1}) \quad \textit{and} \quad H^{\mathrm{cop}} = (H, \mu, \eta, \Delta^{\mathrm{op}}, \varepsilon, S^{-1})$$

are isomorphic Hopf algebras, the isomorphism being given by S.

An endomorphism T of a bialgebra H such that

$$\sum_{(x)} T(x'')x' = \varepsilon(x)1 = \sum_{(x)} x''T(x') \tag{3.7}$$

for all $x \in H$ is sometimes called a *skew-antipode* for H. Alternatively, a skew-antipode for H is an antipode for the bialgebras H^{op} and H^{cop}. By Corollary 3.5 the inverse (if it exists) of an antipode is a skew-antipode.

It is not always easy to check the defining Relations (3.3) of an antipode for every element of a bialgebra, but it may be simpler to check only for some generators. It is convenient to have the following lemma.

Lemma III.3.6. *Let H be a bialgebra and $S : H \to H^{\mathrm{op}}$ be an algebra morphism. Assume that H is generated as an algebra by a subset X such that*

$$\sum_{(x)} x'S(x'') = \varepsilon(x)1 = \sum_{(x)} S(x')x''$$

for all $x \in X$. Then S is an antipode for H.

Proof. It is enough to check that if (3.3) holds for x and y, then it holds for the product xy. Now, by (3.3–3.4)

$$\begin{aligned}\sum_{(xy)} (xy)'S((xy)'') &= \sum_{(x)(y)} x'y'S(x''y'')\\ &= \sum_{(x)} x'\Big(\sum_{(y)} y'S(y'')\Big)S(x'')\\ &= \Big(\sum_{(x)} x'S(x'')\Big)\varepsilon(y)\\ &= \varepsilon(x)\varepsilon(y)\\ &= \varepsilon(xy).\end{aligned}$$

One proves $\sum_{(xy)} S((xy)')(xy)'' = \varepsilon(xy)$ similarly. □

Use the previous lemma to show that the following provide examples of Hopf algebras.

Example 3. The tensor bialgebra $H = T(V)$ is a Hopf algebra with an antipode determined by $S(1) = 1$ and for all $v_1, v_2, \dots, v_n \in V$ by

$$S(v_1 v_2 \dots v_n) = (-1)^n v_n \dots v_2 v_1.$$

Example 4. (*The symmetric bialgebra* $S(V)$) Let I be the kernel of the projection of $T(V)$ onto the symmetric algebra $S(V)$. Let us show that I is a coideal for the coalgebra structure put on $T(V)$ in Theorem 2.4. Any element of I is a sum of elements of the form $x[v,w]y$ where $x, y \in T(V)$ and $v, w \in V$. By Theorem 2.4 we have

$$\Delta(x[v,w]y) = \sum_{(x)(y)} \left(x'[v,w]y' \otimes x''y'' + x'y' \otimes x''[v,w]y''\right)$$

which belongs to $I \otimes T(V) + T(V) \otimes I$ and

$$\varepsilon(x[v,w]y) = \varepsilon(x)[\varepsilon(v), \varepsilon(w)]\varepsilon(y) = 0,$$

which proves that I is a coideal. It follows that the bialgebra structure of $T(V)$ induces a bialgebra structure on $S(V)$ for which the elements of V are primitive. One checks that $S(V)$ has an antipode which is the multiplication by $(-1)^n$ on $S^n(V)$.

Another useful concept is the concept of a *grouplike* element of a coalgebra (H, Δ, ε), i.e., an element $x \neq 0$ such that

$$\Delta(x) = x \otimes x. \tag{3.8}$$

The set of grouplike elements of H will be denoted by $\mathcal{G}(H)$.

Proposition III.3.7. *Let H be a bialgebra. Then $\mathcal{G}(H)$ is a monoid for the multiplication of H with unit 1. If, furthermore, H has an invertible antipode S, then any grouplike element x has an inverse in $\mathcal{G}(H)$ which is $S(x)$. Consequently, $\mathcal{G}(H)$ is a group.*

PROOF. The first assertion is clear. As for the second, observe that (3.6) and (3.8) imply $\Delta(S(x)) = S(x) \otimes S(x)$. It follows that $S(x)$ belongs to $\mathcal{G}(H)$. To complete the proof, one checks that $\varepsilon(x) = 1$ when x is grouplike, and one uses the computation in Example 2 in order to show that $S(x)$ is the inverse of x. □

Example 5. If $k[G]$ is the Hopf algebra associated to a group G as in Example 2, then the elements of G are the only grouplike elements of $k[G]$. In other words, we have

$$\mathcal{G}(k[G]) = G. \tag{3.9}$$

III.4 Relationship with Chapter I. The Hopf Algebras $GL(2)$ and $SL(2)$

The aim of this section is to show that the algebras $M(2)$, $GL(2)$ and $SL(2)$ defined in I.4 and I.5 are bialgebras. We use Proposition II.4.2 in order to identify $M(2)^{\otimes 2}$ with $M(2) \otimes M(2)$, $GL(2)^{\otimes 2}$ with $GL(2) \otimes GL(2)$ and $SL(2)^{\otimes 2}$ with $SL(2) \otimes SL(2)$. Let us show that the morphisms Δ of I.4 and ε of I.5 equip these algebras with a cocommutative bialgebra structure. Recall (I.4.4): we have

$$\begin{pmatrix} \Delta(a) & \Delta(b) \\ \Delta(c) & \Delta(d) \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \dot{\otimes} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{4.1}$$

and $\Delta(t) = t \otimes t$. In order to prove that Δ is coassociative, it suffices to check this on the generators a, b, c, d, and t, which results from the fact that t is grouplike and from the matrix equality

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \dot{\otimes} \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \dot{\otimes} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \dot{\otimes} \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \dot{\otimes} \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right).$$

Similarly, the counit axiom follows from $\varepsilon(t) = 1$ and from the matrix equalities

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{4.2}$$

The algebra morphism S defined in (I.5.2) is an antipode for the bialgebras $GL(2)$ and $SL(2)$ which become Hopf algebras in this way. Indeed, by Lemma 3.6, it is enough to check Relations (3.3) for the generators a, b, c, d, t. For a, b, c, d it follows from

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} S(a) & S(b) \\ S(c) & S(d) \end{pmatrix} = \begin{pmatrix} S(a) & S(b) \\ S(c) & S(d) \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \varepsilon(a) & \varepsilon(b) \\ \varepsilon(c) & \varepsilon(d) \end{pmatrix}. \tag{4.3}$$

As for t, we have $tS(t) = S(t)t = \varepsilon(t) = 1$ since $S(t) = t^{-1} = ad - bc$.

The antipode is an involution due to the fact that $GL(2)$ and $SL(2)$ are both commutative. This can also be checked directly on Formula (I.5.2) defining S.

III.5 Modules over a Hopf Algebra

Let A be an algebra. The tensor product $U \otimes V$ of two A-modules is an $A \otimes A$-module by

$$(a \otimes a')(u \otimes v) = au \otimes a'v \tag{5.1}$$

where $a, a' \in A$, $u \in U$ and $v \in V$. Now, if A possesses a bialgebra structure $(A, \mu, \eta, \Delta, \varepsilon)$, then the algebra morphism $\Delta : A \to A \otimes A$ enables us to equip the $A \otimes A$-module $U \otimes V$ with an A-module structure by

$$a(u \otimes v) = \Delta(a)(u \otimes v) = \sum_{(a)} a'u \otimes a''v. \tag{5.2}$$

The counit ε equips any vector space V with a *trivial* A-module structure by

$$av = \varepsilon(a)v \tag{5.3}$$

where $a \in A$ and $v \in V$.

The following is the natural extension of Proposition II.1.3 to the framework of A-modules.

Proposition III.5.1. *If A is a bialgebra, U, V and W are A-modules and k is given the trivial A-module structure, then the canonical isomorphisms of Proposition* II.1.3

$$(U \otimes V) \otimes W \cong U \otimes (V \otimes W) \quad \text{and} \quad k \otimes V \cong V \cong V \otimes k$$

are A-module isomorphisms. If, furthermore, A is cocommutative, then the flip $\tau_{V,W} : V \otimes W \cong W \otimes V$ is an isomorphism of A-modules.

PROOF. The proof is easy and is left to the reader. □

Let us show how an antipode allows us to give a natural A-module structure to the vector space $\mathrm{Hom}(V, V')$ of linear maps from V to V' when V and V' have A-module structures. We first observe that

$$\Big((a \otimes a')f\Big)(v) = af(a'v) \tag{5.4}$$

puts an $A \otimes A^{\mathrm{op}}$-module structure on $\mathrm{Hom}(V, V')$. Indeed, we have

$$\begin{aligned}
\Big((a \otimes a')(b \otimes b')f\Big)(v) &= \Big((ab \otimes b'a')f\Big)(v)\\
&= abf(b'a'v)\\
&= a\Big((b \otimes b')f\Big)(a'v)\\
&= \Big((a \otimes a')((b \otimes b')f)\Big)(v)
\end{aligned}$$

for $a, a', b, b' \in A$, $v \in V$ and $f \in \mathrm{Hom}(V, V')$. Now, if A is a Hopf algebra with antipode S, then the map $(\mathrm{id} \otimes S) \circ \Delta$ is a morphism of algebras from A to $A \otimes A^{\mathrm{op}}$. Pulling (5.4) back along this morphism, we get an A-module structure on $\mathrm{Hom}(V, V')$. Explicitly, if $a \in A$, $v \in V$ and $f \in \mathrm{Hom}(V, V')$, the action of A on $\mathrm{Hom}(V, V')$ is given by

$$(af)(v) = \sum_{(a)} a'f(S(a'')v). \tag{5.5}$$

In particular, if $V' = k$ is given the trivial A-module structure, then (5.5) induces an A-module structure on the dual vector space V^* which becomes

$$(af)(v) = f(S(a)v). \tag{5.6}$$

Indeed, by (5.5) and (1.21), we get

$$(af)(v) = \sum_{(a)} \varepsilon(a')f(S(a'')v) = f\Big(S(\sum_{(a)} \varepsilon(a')a'')v\Big) = f(S(a)v).$$

Proposition III.5.2. *Let $(A, \mu, \eta, \Delta, \varepsilon, S)$ be a Hopf algebra and U, U', V and V' be A-modules such that, either U or U', and, either V or V', are finite-dimensional vector spaces. Then the linear map*

$$\lambda : \mathrm{Hom}(U, U') \otimes \mathrm{Hom}(V, V') \to \mathrm{Hom}(V \otimes U, U' \otimes V')$$

of (II.2.2) *is A-linear if, in addition, the flip $\tau_{U^*,V'} : U^* \otimes V' \to V' \otimes U^*$ is A-linear. In particular, the maps*

$$\lambda : U^* \otimes V^* \to (V \otimes U)^* \quad \text{and} \quad \lambda_{U,V} : V \otimes U^* \to \mathrm{Hom}(U, V)$$

are A-linear.

PROOF. (a) Let $f : U \to U'$, $g : V \to V'$, $u \in U$, $v \in V$ and $a \in A$. Let us first compute $\lambda(a(f \otimes g))$ using (II.2.2), (5.2) and (5.5). We have

$$\begin{aligned}
Z_1 &= \Big(\lambda(a(f \otimes g))\Big)(v \otimes u)\\
&= \sum_{(a)} \lambda(a'f \otimes a''g)(v \otimes u)\\
&= \sum_{(a)} (a'f)(u) \otimes (a''g)(v)\\
&= \sum_{(a)} (a')'f(S((a')'')u) \otimes (a'')'g(S((a'')'')v)\\
&= \sum_{(a)} a'f(S(a'')u) \otimes a'''g(S(a'''')v)
\end{aligned}$$

using Sweedler's sigma notation. On the other hand, $a\lambda(f \otimes g)$ is given by

$$\begin{aligned}
Z_2 &= \Big(a\lambda(f \otimes g)\Big)(v \otimes u)\\
&= \sum_{(a)} a'\lambda(f \otimes g)(S(a'')(v \otimes u))\\
&= \sum_{(a)} a'\lambda(f \otimes g)(S(a'')'v \otimes S(a'')''u)
\end{aligned}$$

$$\begin{aligned}
&= \sum_{(a)} a'\lambda(f\otimes g)(S((a'')'')v \otimes S((a'')')u) \\
&= \sum_{(a)} a'\lambda(f\otimes g)(S(a''')v \otimes S(a'')u) \\
&= \sum_{(a)} a'\Big(f(S(a'')u)\otimes g(S(a''')v)\Big) \\
&= \sum_{(a)} (a')'f(S(a'')u)\otimes (a')''g(S(a''')v) \\
&= \sum_{(a)} a'f(S(a''')u)\otimes a''g(S(a'''')v).
\end{aligned}$$

We used (3.6) for the fourth equality. Observe that $Z_1 \neq Z_2$ in general.

(b) Let $V' = k$ be given the trivial action. Replacing a''' in Z_1 [resp. a'' in Z_2] by $\varepsilon(a''')$ [resp. by $\varepsilon(a'')$] and using (1.21), we get

$$Z_1 = Z_2 = \sum_{(a)} a'f(S(a'')u)\otimes g(S(a''')v),$$

which proves that $\lambda : \mathrm{Hom}(U,U')\otimes V^* \to \mathrm{Hom}(V\otimes U, U')$ is A-linear. We get the two special cases of Proposition 5.2 with $U' = k$ and with $U = k$.

For the general case, we use Lemma II.2.4 which expresses λ in terms of the special maps λ and of the flip $\tau_{U^*,V'}$. □

As a corollary of Proposition 5.2, we see that the general map λ of Theorem II.2.1 is A-linear when A is cocommutative. This happens, for instance, when A is a group algebra or an enveloping algebra.

As for the evaluation and the coevaluation maps, we have the following result.

Proposition III.5.3. *Let V be an A-module. Then the evaluation map $\mathrm{ev}_V : V^*\otimes V \to k$ is A-linear. If, moreover, the vector space V is finite-dimensional, then the coevaluation map $\delta_V : k \to V\otimes V^*$ of* II.3 *and the composition*

$$\mathrm{Hom}(V,W)\otimes \mathrm{Hom}(U,V) \xrightarrow{\circ} \mathrm{Hom}(U,W)$$

are A-linear too.

PROOF. (a) Let $a\in A$, $v \in V$ and $\alpha\in V^*$. Then

$$\begin{aligned}
\mathrm{ev}_V(a(\alpha\otimes v)) &= \sum_{(a)} \mathrm{ev}_V(a'\alpha\otimes a''v) \\
&= \sum_{(a)} (a'\alpha)(a''v) \\
&= \alpha(\sum_{(a)} S(a')a''v) \\
&= \alpha(\varepsilon(a)v) \\
&= \varepsilon(a)\alpha(v)
\end{aligned}$$

by the rightmost relation (3.3) and by (5.6). This implies that the evaluation map is A-linear.

(b) The coevaluation map δ_V is A-linear as the composition of the unit $\eta : k \to \mathrm{End}(V)$ and of $\lambda^{-1}_{V,V}$. The latter is A-linear by Proposition 5.2. So is the map $\eta : k \to \mathrm{End}(V)$ following

$$\begin{aligned}
(a\eta(1))(v) &= (a\mathrm{id}_V)(v) \\
&= \sum_{(a)} a'\mathrm{id}_V(S(a'')v) \\
&= \sum_{(a)} a'S(a'')v \\
&= \varepsilon(a)v \\
&= (\eta(a1))(v)
\end{aligned}$$

for all $v\in V$ and $a \in A$. Here we used the leftmost relation (3.3).

(c) For the composition map, one uses Lemma II.2.5. □

III.6 Comodules

Algebras act on modules, coalgebras coact on comodules. This section is devoted to the definition of the latter concept. Let A be an algebra. Recall that an A-module is a pair (M,μ_M) where M is a vector space and $\mu_M : A\otimes M \to M$ is a linear map such that the following axioms (Ass) and (Un) hold.

(Ass): The square

$$\begin{array}{ccc}
A\otimes A\otimes M & \xrightarrow{\mu\otimes \mathrm{id}} & A\otimes M \\
\big\downarrow{\scriptstyle \mathrm{id}\otimes\mu_M} & & \big\downarrow{\scriptstyle \mu_M} \\
A\otimes M & \xrightarrow{\mu_M} & M
\end{array} \tag{6.1}$$

commutes.

(Un): The diagram

$$\begin{array}{ccc}
k\otimes M & \xrightarrow{\eta\otimes \mathrm{id}} & A\otimes M \\
 & \searrow{\scriptstyle\cong} & \big\downarrow{\scriptstyle \mu_M} \\
 & & M
\end{array} \tag{6.2}$$

commutes.

A morphism of A-modules $f : (M,\mu_M) \to (M',\mu_{M'})$ is a linear map f from M to M' such that

$$\mu_{M'}\circ(\mathrm{id}\otimes f) = f\circ \mu_M\,. \tag{6.3}$$

The definition of a comodule over a coalgebra is obtained by reversing all arrows in the diagrams above.

Definition III.6.1. *Let (C, Δ, ε) be a coalgebra.*

(a) *A C-comodule is a pair (N, Δ_N) where N is a vector space and $\Delta_N : N \to C \otimes N$ is a linear map, called the coaction of C on N, such that the following axioms* (Coass) *and* (Coun) *are satisfied.*

(Coass)*: The square*

$$\begin{tikzcd} N \arrow[r, "\Delta_N"] \arrow[d, "\Delta_N"] & C \otimes N \arrow[d, "\mathrm{id}\otimes\Delta_N"] \\ C \otimes N \arrow[r, "\Delta\otimes\mathrm{id}"] & C \otimes C \otimes N \end{tikzcd} \tag{6.4}$$

commutes.

(Coun)*: The diagram*

$$\begin{tikzcd} k \otimes N & C \otimes N \arrow[l, "\varepsilon\otimes\mathrm{id}"'] \\ & N \arrow[u, "\Delta_N"'] \arrow[ul, "\cong"'] \end{tikzcd} \tag{6.5}$$

commutes.

(b) *Let (N, Δ_N) and $(N', \Delta_{N'})$ be C-comodules. A linear map f from N to N' is a morphism of C-comodules if*

$$(\mathrm{id} \otimes f) \circ \Delta_N = \Delta_{N'} \circ f. \tag{6.6}$$

(c) *A subspace N' of a C-comodule (N, Δ_N) is a subcomodule of N if $\Delta_N(N') \subset C \otimes N'$.*

Actually, the comodules we have just defined are left comodules. One similarly defines a right C-comodule N, using a map $N \otimes C \to N$ subject to relations parallel to (6.4–6.5). A right C-comodule is the same as a (left) comodule over the opposite coalgebra C^{cop}.

The composition of two morphisms of comodules is another morphism of comodules. Similarly, the inclusion of a subcomodule into a comodule is a morphism of comodules. Let us give a few examples of comodules.

Example 1. Let C be a coalgebra. Then (C, Δ) is a C-comodule.

Example 2. Let C be a coalgebra and C^* the dual vector space equipped with the dual algebra structure of Proposition 1.2. If (N, Δ_N) is a C-comodule, then the dual vector space N^* has the structure of a right C^*-module given by the composition of the maps

$$N^* \otimes C^* \xrightarrow{\lambda} (C \otimes N)^* \xrightarrow{\Delta_N^*} N^*. \tag{6.7}$$

Example 3. Let A be a *finite-dimensional algebra* and A^* be the dual vector space with the coalgebra structure given by Proposition 1.3. If (M, μ_M) is a right A-module, then the dual vector space M^* has a structure of A^*-comodule given by the composition of the maps

$$M^* \xrightarrow{\mu_M^*} (M \otimes A)^* \xrightarrow{\lambda^{-1}} A^* \otimes M^*. \tag{6.8}$$

In order to put a structure of comodule on the tensor product of two comodules, we need a bialgebra structure as in Section 5.

Example 4. (*Tensor product of comodules*) Let $(H, \mu, \eta, \Delta, \varepsilon)$ be a bialgebra and M and N be H-comodules. We define $\Delta_{M\otimes N}$ by

$$\Delta_{M\otimes N} = (\mu \otimes \mathrm{id}_{M\otimes N})(\mathrm{id}_H \otimes \tau_{M,H} \otimes \mathrm{id}_N)(\Delta_M \otimes \Delta_N). \tag{6.9}$$

The map $\Delta_{M\otimes N}$ endows the tensor product $M \otimes N$ with an H-comodule structure.

Example 5. (*Trivial comodule*) Let $(H, \mu, \eta, \Delta, \varepsilon)$ be a bialgebra and V be a vector space. The linear map

$$V \cong k \otimes V \xrightarrow{\eta\otimes\mathrm{id}_V} H \otimes V \tag{6.10}$$

equips V with an H-comodule structure. Such a comodule is called a trivial comodule.

Example 6. (*Free comodule*) Let (C, Δ, ε) be a coalgebra. The free C-comodule on a vector space V is the comodule $(C \otimes V, \Delta \otimes \mathrm{id}_V)$. This is a generalization of Example 1.

Proposition 5.1 has the following counterpart for comodules. The proof is left to the reader.

Proposition III.6.2. *If H is a bialgebra, M, N, P are H-comodules and k is given the trivial H-comodule structure of Example* 5, *then the canonical isomorphisms of Proposition* II.1.3

$$(M \otimes N) \otimes P \cong M \otimes (N \otimes P) \quad \text{and} \quad k \otimes M \cong M \cong M \otimes k$$

are isomorphisms of H-comodules. If, in addition, the bialgebra H is commutative, then the flip $\tau_{M,N} : M \otimes N \cong N \otimes M$ is an isomorphism of H-comodules too.

Notation 6.3. It is often convenient to use for comodules the same kind of notation as was introduced for coalgebras in Section 1. Let (C, Δ, ε) be a coalgebra and (N, Δ_N) be a C-comodule. By convention we shall write

$$\Delta_N(x) = \sum_{(x)} x_C \otimes x_N \tag{6.11}$$

for any $x \in N$. Relation (6.4) is equivalent to

$$\sum_{(x)} (x_C)' \otimes (x_C)'' \otimes x_N = \sum_{(x)} x_C \otimes (x_N)_C \otimes (x_N)_N \tag{6.12}$$

for all $x \in N$. Relation (6.5) is equivalent to

$$\sum_{(x)} \varepsilon(x_C) \otimes x_N = x. \tag{6.13}$$

A linear map $f : N \to N'$ is a morphism of C-comodules if

$$\sum_{(x)} x_C \otimes f(x_N) = \sum_{(x)} f(x)_C \otimes f(x)_{N'}. \tag{6.14}$$

III.7 Comodule-Algebras. Coaction of $SL(2)$ on the Affine Plane

The aim of this section is to define a coaction of the bialgebra $SL(2)$ on the affine plane of Chapter I. Before doing so, we introduce the following concept.

Definition III.7.1. *Let $(H, \mu_H, \eta_H, \Delta_H, \varepsilon_H)$ be a bialgebra and (A, μ_A, η_A) be an algebra. We say A is an H-comodule-algebra if*

(a) *the vector space A has an H-comodule structure given by a map $\Delta_A : A \to H \otimes A$, and*

(b) *the structure maps $\mu_A : A \otimes A \to A$ and $\eta_A : k \to A$ are morphisms of H-comodules, the tensor product $A \otimes A$ and the ground field k being given the H-comodule structures described in Section 6.*

We note the following useful characterization of comodule-algebra structures.

Proposition III.7.2. *Let H be a bialgebra and A be an algebra. Then A is an H-comodule-algebra if and only if*

(a) *the vector space A has an H-comodule structure given by a map $\Delta_A : A \to H \otimes A$, and*

(b) *the map $\Delta_A : A \to H \otimes A$ is a morphism of algebras.*

PROOF. It is similar to the proof of Theorem 2.1. We first express the fact that μ_A is a morphism of H-comodules with the commutative square

$$\begin{array}{ccc} A \otimes A & \xrightarrow{\mu_A} & A \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle \Delta_A} \\ H \otimes (A \otimes A) & \xrightarrow{\mathrm{id} \otimes \mu_A} & H \otimes A \end{array} \tag{7.1}$$

where $u = (\mu_H \otimes \mathrm{id} \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \tau_{A,H} \otimes \mathrm{id}) \circ (\Delta_A \otimes \Delta_A)$. The fact that η_A is a morphism of H-comodules is equivalent to the commutativity of the square

$$\begin{array}{ccc} k & \xrightarrow{\eta_A} & A \\ \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \Delta_A} \\ k \otimes k & \xrightarrow{\eta_H \otimes \eta_A} & H \otimes A \end{array} \tag{7.2}$$

Now, Diagrams (7.1–7.2) are exactly the same as Diagrams (7.3) below which express the fact that Δ_A is a morphism of algebras:

$$\begin{array}{ccc} A \otimes A & \xrightarrow{\Delta_A \otimes \Delta_A} & (H \otimes A) \otimes (H \otimes A) \\ \downarrow{\scriptstyle \mu_A} & & \downarrow{\scriptstyle v} \\ A & \xrightarrow{\Delta_A} & H \otimes A \end{array} \qquad \begin{array}{ccc} k & \xrightarrow{\cong} & k \otimes k \\ \downarrow{\scriptstyle \eta_A} & & \downarrow{\scriptstyle \eta_H \otimes \eta_A} \\ A & \xrightarrow{\Delta_A} & H \otimes A \end{array} \tag{7.3}$$

where $v = (\mu_H \otimes \mu_A) \circ (\mathrm{id} \otimes \tau_{A,H} \otimes \mathrm{id})$. Indeed, we have

$$(\mathrm{id} \otimes \mu_A) \circ u = v \circ (\Delta_A \otimes \Delta_A).$$

□

Using the conventions of Sections 1 and 6, we can rewrite Condition (b) of Proposition 7.2 as $\Delta_A(1) = 1 \otimes 1$ and

$$\sum_{(ab)} (ab)_H \otimes (ab)_A = \sum_{(a)(b)} a_H b_H \otimes a_A b_A \tag{7.4}$$

for all $a, b \in A$.

We now show that the affine plane $k[x, y]$ defined in I.3 possesses an comodule-algebra structure over the bialgebras $M(2)$ and $SL(2)$.

Theorem III.7.3. *There exists a unique $M(2)$-comodule-algebra structure and a unique $SL(2)$-comodule-algebra structure on the affine plane $A = k[x, y]$ such that*

$$\Delta_A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} x \\ y \end{pmatrix}.$$

This matrix notation is short for the two relations

$$\Delta_A(x) = a \otimes x + b \otimes y \quad \text{and} \quad \Delta_A(y) = c \otimes x + d \otimes y. \tag{7.5}$$

PROOF. We use Proposition 7.2. First observe that Formulas (7.5) define a morphism of algebras $\Delta_A : k[x, y] \to M(2) \otimes k[x, y]$. The projection of $M(2)$ onto $SL(2)$ being an algebra morphism too, so is the resulting composition $k[x, y] \to SL(2) \otimes k[x, y]$.

It remains to be checked that Δ_A defines a comodule structure, i.e., that for all $z \in k[x, y]$ we have

$$(\mathrm{id} \otimes \Delta_A) \circ \Delta_A(z) = (\Delta \otimes \mathrm{id}) \circ \Delta_A(z) \quad \text{and} \quad (\varepsilon \otimes \mathrm{id}) \circ \Delta_A(z) = 1 \otimes z \tag{7.6}$$

where Δ and ε are as in I.4–I.5. As both sides of each equality to be proved consist solely of algebra morphisms, it suffices to check (7.6) only for $z = x$ and $z = y$. The above matrix notation allows us to do this simultaneously. We have

$$\begin{aligned}\big((\mathrm{id}\otimes\Delta_A)\circ\Delta_A\big)\begin{pmatrix} x \\ y\end{pmatrix} &= \begin{pmatrix} a & b \\ c & d\end{pmatrix}\otimes\begin{pmatrix} a & b \\ c & d\end{pmatrix}\otimes\begin{pmatrix} x \\ y\end{pmatrix}\\ &= \big((\Delta\otimes\mathrm{id})\circ\Delta_A\big)\begin{pmatrix} x \\ y\end{pmatrix}\end{aligned}$$

in view of (4.1). On the other hand, using (I.5.2) we get

$$(\varepsilon\otimes\mathrm{id})\circ\Delta_A\begin{pmatrix} x \\ y\end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix}\otimes\begin{pmatrix} x \\ y\end{pmatrix} = 1\otimes\begin{pmatrix} x \\ y\end{pmatrix}.$$

□

Let us compute $\Delta_A(x^iy^j)$ in $M(2)\otimes k[x,y]$.

Lemma III.7.4. *For all $i,j\geq 0$ we have*

$$\Delta_A(x^iy^j) = \sum_{r=0}^{i}\sum_{s=0}^{j}\binom{i}{r}\binom{j}{s} a^rb^{i-r}c^sd^{j-s}\otimes x^{r+s}y^{i+j-r-s}.$$

PROOF. Since Δ_A is an algebra morphism, we have

$$\Delta_A(x^iy^j) = \Delta_A(x)^i\Delta_A(y)^j = (a\otimes x + b\otimes y)^i(c\otimes x + d\otimes y)^j.$$

Next, apply the binomial formula. □

Let us denote by $k[x,y]_n$ the subspace of homogeneous polynomials of total degree n in $A = k[x,y]$. Lemma 7.4 implies that $k[x,y]_n$ is a subcomodule of the affine plane due to the fact that

$$\Delta_A(k[x,y]_n)\subset M(2)\otimes k[x,y]_n.$$

Actually, the $M(2)$-[resp. $SL(2)$-]comodule $k[x,y]$ is the direct sum of the comodules $k[x,y]_n$.

According to Section 6, Example 2, the dual vector space $k[x,y]_n^*$ of the comodule $k[x,y]_n$ has a module structure over the algebra $SL(2)^*$, the dual of the coalgebra $SL(2)$. We shall identify this module in V.7.

III.8 Exercises

1. (*Tensor product of coalgebras*) Let (C,Δ,ε) and $(C',\Delta',\varepsilon')$ be coalgebras. Show that the linear maps $\pi : C\otimes C'\to C$ and $\pi' : C\otimes C'\to C'$ defined by $\pi(c\otimes c') = \varepsilon'(c')c$ and $\pi'(c\otimes c') = \varepsilon(c)c'$ are morphisms of coalgebras and that the coalgebra $C\otimes C'$ satisfies the following universal property: for any *cocommutative* coalgebra D and any pair $f : D\to C$ and $f' : D\to C'$ of coalgebra morphisms, there exists a unique morphism of coalgebras $f\otimes f' : D\to C\otimes C'$ such that $\pi\circ(f\otimes f') = f$ and $\pi'\circ(f\otimes f') = f'$.

2. (*Divided powers*) Consider the vector space $C = k[t]$ of polynomials in one variable. Prove that there exists a unique coalgebra structure (C,Δ,ε) on C such that
$$\Delta(t^n) = \sum_{p+q=n} t^p\otimes t^q \quad\text{and}\quad \varepsilon(t^n) = \delta_{n0}$$
for all $n\geq 0$. Show that C becomes a bialgebra when given the product
$$t^pt^q = \binom{p+q}{p}t^{p+q}.$$
Find an antipode.

3. (*Tensor coalgebra*) Let V be a vector space.
   (a) Show that the canonical isomorphisms $V^{\otimes(n+m)}\cong V^{\otimes n}\otimes V^{\otimes m}$ endow $T'(V) = \bigoplus_{n\geq 0} V^{\otimes n}$ with a coalgebra structure, called the *tensor coalgebra* of V.
   (b) Let p_V be the canonical projection of $T'(V)$ onto V. Prove that for any coalgebra C and any linear map $f : C\to V$, there exists a unique morphism of coalgebras $\bar f : C\to T'(V)$ such that $f = p_V\circ\bar f$.
   (c) Using the notation of Chapter II, Exercise 7, define the subspace $S'(V) = \bigoplus_{n\geq 0} S'_n(V)$ [resp. $\Lambda'(V) = \bigoplus_{n\geq 0}\Lambda'_n(V)$] of $T'(V)$ generated by all symmetric [resp. antisymmetric] tensors. Show that $S'(V)$ and $\Lambda'(V)$ are subcoalgebras of $T'(V)$.
   (d) Let C be a cocommutative coalgebra and f be a linear map from C to V. Prove the existence and the uniqueness of a coalgebra morphism $\bar f : C\to S'(V)$ such that $f = p_V\circ\bar f$.

4. (*Graded dual*) The graded dual vector space of a graded vector space $V = \bigoplus_{n\geq 0} V_n$ is the graded vector space $V^*_{gr} = \bigoplus_{n\geq 0} V^*_n$. Let $W = \bigoplus_{n\geq 0} W_n$ be another graded vector space. Show that there is a grading on the tensor product $V\otimes W$ such that
$$(V\otimes W)_n = \bigoplus_{i+j=n} V_i\otimes W_j.$$
Prove that $V^*_{gr}\otimes W^*_{gr}\cong(V\otimes W)^*_{gr}$ if V_n is finite-dimensional for each $n\geq 0$.

5. (*Graded coalgebra*) Keep the notation of the previous exercise. A coalgebra (C, Δ, ε) is graded if there exist subspaces $(C_n)_{n\geq 0}$ of C such that $C = \bigoplus_{n\geq 0} C_n$ and $\Delta(C_n) \subset \bigoplus_{i+j=n} C_i \otimes C_j$ for all $n \geq 0$ and $\varepsilon(C_n) = \{0\}$ for all $n > 0$.

   (a) Prove that the graded dual vector space of a graded coalgebra carries a natural graded algebra structure.

   (b) Let $A = \bigoplus_{n\geq 0} A_n$ be a graded algebra whose summands A_n are all finite-dimensional. Prove that the graded dual vector space of A carries a natural graded coalgebra structure.

   (c) Check that the coalgebra C of Exercise 2 is the graded dual vector space of the polynomial algebra $k[t]$.

   (d) (*Shuffle bialgebra*) Let V be a finite-dimensional vector space. Show that the tensor coalgebra $T'(V)$ of Exercise 3 is the graded dual of the tensor algebra $T(V)$. Deduce that $T'(V)$ has a bialgebra structure whose multiplication is given by

$$(v_1 \otimes \cdots \otimes v_p)(v_{p+1} \otimes \cdots \otimes v_{p+q}) = \sum_\sigma v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(p+q)}$$

   where $v_1, \ldots, v_{p+q}$ are elements of V and where σ runs over all (p, q)-shuffles of the symmetric group S_{p+q}.

   (e) Under the same hypotheses as before, show that $S'(V)$ and $\Lambda'(V)$ are subbialgebras of $T'(V)$ whose graded duals are the bialgebras $S(V)$ and $\Lambda(V)$ respectively.

6. (*Convolution algebra*) Let G be a finite group. Equip the vector space $C(G)$ of complex-valued functions on G with the convolution product

$$(ff')(x) = \sum_{y\in G} f(y)f'(y^{-1}x)$$

where $x \in G$ and $f, f' \in C(G)$. Show that $C(G)$ has a Hopf algebra structure such that the linear map $f \mapsto \sum_{x\in G} f(x)x$ is a Hopf algebra isomorphism from $C(G)$ to the group Hopf algebra $\mathbf{C}[G]$. Determine the unit, the comultiplication, the counit and the antipode of $C(G)$.

7. (*An example of a non-commutative, non-cocommutative Hopf algebra*) Let H be the quotient of the free algebra $k\{t, x\}$ by the two-sided ideal generated by $t^2 - 1, x^2, xt + tx$. Prove that H is a four-dimensional vector space and that

$$\Delta(t) = t \otimes t, \quad \Delta(x) = 1 \otimes x + x \otimes t,$$

$$\varepsilon(t) = 1, \quad \epsilon(x) = 0, \quad S(t) = t, \quad S(x) = tx$$

endow H with a Hopf algebra structure whose antipode is of order 4.

8. (*Convolution and composition*) Consider a morphism of algebras $f : A \to A'$ and a morphism of coalgebras $g : C' \to C$. Prove that the map $h \mapsto f \circ h \circ g$ from $\mathrm{Hom}(C, A)$ to $\mathrm{Hom}(C', A')$ is a morphism of algebras for the convolution $*$.

9. Use the previous exercise to show that a morphism of bialgebras between two Hopf algebras is necessarily a morphism of Hopf algebras (Hint: prove $S \circ f = f \circ S$ by applying left and right convolution with $f = f \circ \mathrm{id} = \mathrm{id} \circ f$).

10. Let $H = (H, \mu, \eta, \Delta, \varepsilon, S)$ be a Hopf algebra.

   (a) Set $\psi^0 = \eta\varepsilon$, and $\psi^n = \mathrm{id}_H^{\star n}$ (convolution of n morphisms all equal to the identity of H) if $n > 0$ and $\psi^n = S^{\star n}$ if $n < 0$. Prove that each map ψ^n is an endomorphism of algebras [resp. of coalgebras] when H is commutative [resp. cocommutative] and that, in both cases, we have $\psi^n \circ \psi^m = \psi^{n+m}$ for any pair (n, m) of integers.

   (b) Let $H = k[G]$ be a group. Show that ψ^n is the coalgebra endomorphism given by $\psi^n(g) = g^n$ $(g \in G)$.

   (c) Let $H = S(V)$ be a symmetric algebra. Then $\psi^n(x) = n^d x$ for any $x \in S^d(V)$.

   (d) Show that if $H = SL(2)$, then the algebra endomorphism ψ^n is determined by the matrix identity

$$\begin{pmatrix} \psi^n(a) & \psi^n(b) \\ \psi^n(c) & \psi^n(c) \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^n \qquad \text{if } n > 0$$

   and by

$$\begin{pmatrix} \psi^n(a) & \psi^n(b) \\ \psi^n(c) & \psi^n(c) \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}^n \qquad \text{if } n < 0.$$

11. Let H be a Hopf algebra, A be a *commutative* algebra and C be a *cocommutative* coalgebra. Prove that the set $\mathrm{Hom}_{Alg}(H, A)$ of algebra morphisms (resp. the set $\mathrm{Hom}_{Cog}(C, H)$ of coalgebra morphisms) is a group for the convolution, the inverse of a morphism f being given by $f \circ S$ [resp. by $S \circ f$].

12. Let A be a commutative algebra.

   (a) Let V be a finite-dimensional vector space. Consider the symmetric algebra $S(V)$ with the Hopf algebra structure described in Section 3, Example 4. Prove that the group $\mathrm{Hom}_{Alg}(S(V), A)$ is isomorphic to the additive group underlying $A^{\dim(V)}$.

(b) Show that $\mathrm{Hom}_{Alg}(k[\mathbf{Z}], A)$ is isomorphic to the group of invertible elements of A where $k[\mathbf{Z}]$ is the Hopf algebra of the group of integers.

(c) Let C be the Hopf algebra of Exercise 2. Determine the group $\mathrm{Hom}_{Alg}(C, A)$.

13. Let (C, Δ, ε) be a coalgebra and $(C \otimes V, \Delta \otimes \mathrm{id}_V)$ be a free comodule (see Section 6, Example 6). Prove that for any comodule N the map $f \mapsto (\varepsilon \otimes \mathrm{id}_V) \circ f$ is a linear isomorphism from the space of comodule maps from N to $C \otimes V$ to the space $\mathrm{Hom}(N, V)$.

14. Let C be a coalgebra and (N, Δ_N) be a C-comodule. Prove that Δ_N is an injective morphism of comodules from N to the free comodule $(C \otimes N, \Delta \otimes \mathrm{id}_N)$.

15. Let $\{x_i\}_{i \in I}$ be a basis of a C-comodule (N, Δ_N). Define elements c_i^j of the coalgebra (C, Δ, ε) by $\Delta_N(x_i) = \sum_{j \in I} c_i^j x_j$ for all $i \in I$.

(a) Prove that $\Delta(c_i^j) = \sum_{k \in I} c_i^k \otimes c_k^j$ and $\varepsilon(c_i^j) = \delta_{ij}$ for all $i, j \in I$.

(b) Show that the subspace C_N of C linearly generated by the elements $(c_i^j)_{i,j \in I}$ is the smallest subspace C' of C such that $\Delta_N(N) \subset C' \otimes N$. Check that C_N is a coalgebra.

(c) Assume that N is finite-dimensional. Prove that the element $t_N = \sum_{i \in I} c_i^i$ of C_N is independent of the basis $\{x_i\}_{i \in I}$.

16. Prove the structure theorem for bimodules over a Hopf algebra as stated in Section 9.

III.9 Notes

The concept of a Hopf algebra was developed by algebraic topologists abstracting the work of Hopf [Hop41] on manifolds admitting a product (such as Lie groups). A basic reference is the famous article [MM65] by Milnor and Moore. Hopf algebras also came up in the representation theory of Lie groups and algebraic groups (see [Abe80] [DG70] [Hoc81] [Ser93]). For abstract Hopf algebras, we refer to Abe's and Sweedler's monographs [Abe80] [Swe69].

All examples of bialgebras given in this chapter turn out to be either commutative or cocommutative, except for the Hopf algebra of Exercise 7 which is due to Sweedler. Not many examples of non-commutative, non-cocommutative bialgebras were known before the "quantum group" era (nevertheless, see [Par81], [Rad76], [Swe69], pages 89–90, [Taf71], [TW80]). This has dramatically changed in the 1980's with the appearance of quantum groups. For details on the order of the square of the antipode of a Hopf algebra, see [Rad76][Taf71][TW80].

(*Restricted dual*) We saw in Section 1 or in Exercise 5 how to put a coalgebra structure on the dual of an algebra $A = (A, \mu, \eta)$ which is either finite-dimensional or graded. In the general case one can proceed as follows. We know that the map $\lambda : A^* \otimes A^* \to (A \otimes A)^*$ of Corollary II.2.2 allows to identify $A^* \otimes A^*$ with a subspace of $(A \otimes A)^*$. Define

$$A^o = \{\alpha \in A^* \mid \mu^*(\alpha) \in A^* \otimes A^*\}.$$

If the algebra is finite-dimensional, then λ is an isomorphism and $A^o = A^*$. One can show that A^o is the subspace of linear forms whose kernel contains an ideal of finite codimension in A. The vector space A^o enjoys the following property: the embedding λ induces an isomorphism

$$A^o \otimes A^o \cong (A \otimes A)^o.$$

Consequently, $\mu^*(\alpha)$ belongs to $A^o \otimes A^o$ whenever α is in A^o. It results that $(A^o, \mu^*_{|A^o}, \eta^*)$ defines a coalgebra structure on A^o. If, in addition, A has a bialgebra [resp. a Hopf algebra] structure, then so has A^o. For more details, read [Abe80] [Swe69] [Tak85].

(*Restricted dual of a Hopf algebra and representations*) Let H be a Hopf algebra. Its restricted dual H^o also has a Hopf algebra structure. It has the following alternative definition based on representations. Let $\rho : H \to \mathrm{End}(V)$ be a representation of H on a finite-dimensional vector space V. Consider the transpose map $\rho^* : \mathrm{End}(V)^* \to H^*$. Its image $\mathrm{Im}(\rho^*)$, called the *coefficient space of the representation* ρ, sits in the restricted dual H^o. Then the restricted dual may also be defined as the sum of the coefficient spaces of all finite-dimensional representations. In the case when all finite-dimensional H-modules are semisimple, H^o is the direct sum of the coalgebras $\mathrm{Im}(\rho_i)$ where ρ_i runs over all finite-dimensional simple H-modules up to isomorphism. (see [Abe80] [Ser93] [Swe69]).

(*Bimodules*) Let H be a bialgebra. Let M be a vector space equipped with an H-module and an H-comodule structure given by maps

$$\mu_M : H \otimes M \to M \quad \text{and} \quad \Delta_M : M \to H \otimes M.$$

Give $H \otimes M$ the induced module and comodule structures. Then μ_M is a morphism of comodules if and only if Δ_M is a morphism of modules. If these equivalent conditions are satisfied, we say that M is an H-bimodule.

Given such a bimodule M, define the subspace

$$N = \{m \in M \mid \Delta_M(m) = 1 \otimes m\}.$$

It turns out that N is a subcomodule, but not a submodule of M. Put the induced comodule structure on the free H-module $H \otimes M$. Then $H \otimes M$ becomes a bimodule. The structure theorem for bimodules can be stated as follows: if H is a Hopf algebra, then the map $x \otimes m \mapsto xm$ from $H \otimes N$ to M is an isomorphism of H-bimodules. For details, see [Abe80] [Swe69].

Chapter IV
The Quantum Plane and Its Symmetries

In Chapter I we defined the affine plane as the algebra freely generated by two variables x and y subject to the trivial commutation relation $yx = xy$. This corresponds to our classical perception of plane geometry. In this chapter, we consider a modified commutation relation depending on a parameter q, namely

$$yx = q\,xy.$$

This new relation defines the quantum plane. In Section 2 we derive a few identities well-known to combinatorialists and to the experts in the theory of linear q-difference equations. Next, investigating the self-transformations of the quantum plane, we build a bialgebra $M_q(2)$ and Hopf algebras $GL_q(2)$ and $SL_q(2)$, which are one-parameter deformations of the bialgebras $M(2)$, $GL(2)$, and $SL(2)$ defined in Chapter I. The bialgebras obtained in this way are our first examples of quantum groups. They have the peculiarity of being neither commutative nor cocommutative.

IV.1 The Quantum Plane

Let q be an invertible element of the ground field k, and let I_q be the two-sided ideal of the free algebra $k\{x, y\}$ generated by the element $yx - qxy$. We define the *quantum plane* as the quotient-algebra

$$k_q[x, y] = k\{x, y\}/I_q. \tag{1.1}$$

When $q \neq 1$, the algebra $k_q[x, y]$ is non-commutative. If we give the free algebra $k\{x, y\}$ its natural grading, then the ideal I_q is generated by a homogeneous degree-two element. It follows that the quantum plane has a grading such that the generators x and y are of degree 1. We denote by $k_q[x, y]_n$ the vector subspace of all degree-n elements of $k_q[x, y]$.

Proposition IV.1.1. (a) *If α is the automorphism of the polynomial ring $k[x]$ determined by $\alpha(x) = qx$, then the algebra $k_q[x, y]$ is isomorphic to the Ore extension $k[x][y, \alpha, 0]$. Thus, $k_q[x, y]$ is Noetherian, has no zero divisors, and the set of monomials $\{x^i y^j\}_{i,j \geq 0}$ is a basis of the underlying vector space.*

(b) *For any pair (i, j) of nonnegative integers, we have*

$$y^j x^i = q^{ij}\, x^i y^j. \tag{1.2}$$

(c) *Given any k-algebra R, there is a natural bijection*

$$\mathrm{Hom}_{Alg}(k_q[x, y], R) \cong \{(X, Y) \in R \times R \mid YX = qXY\}. \tag{1.3}$$

A pair (X, Y) of elements of R subject to the relation $YX = qXY$ will be called an *R-point of the quantum plane.*

Proof. (a) We use the theory of Ore extensions as presented in I.7–8. Define an algebra morphism $\varphi : k\{x, y\} \to k[x][y, \alpha, 0]$ by $\varphi(x) = x$ and $\varphi(y) = y$. Since

$$\varphi(y)\varphi(x) - q\varphi(x)\varphi(y) = yx - qxy = \alpha(x)y - qxy = 0,$$

the morphism φ vanishes on the ideal I_q, thus defining a morphism of algebras, still denoted φ, on $k_q[x, y]$. The morphism φ is surjective because the Ore extension $k[x][y, \alpha, 0]$ is generated by x and y. In order to show that φ is an isomorphism, we only have to construct a linear map ψ from $k[x][y, \alpha, 0]$ to $k_q[x, y]$ such that $\psi \circ \varphi = \mathrm{id}$. We define ψ on the basis $\{x^i y^j\}_{i,j \geq 0}$ of $k[x][y, \alpha, 0]$ by $\psi(x^i y^j) = x^i y^j$. The rest of the proof of (i) follows from I.7 and I.8.

Part (b) is proved by an easy induction. Part (c) is a consequence of the universal property (I.2.4) and of the definition (1.1). □

We give an example of an R-point of the quantum plane.

Example 1. Let A be the algebra of smooth complex functions on $\mathbf{C} \setminus \{0\}$ and let q be a complex number different from 0 and from 1. Consider the linear endomorphisms τ_q and δ_q in $R = \mathrm{End}(A)$ defined by

$$\tau_q(f)(x) = f(qx) \quad \text{and} \quad \delta_q(f)(x) = \frac{f(qx) - f(x)}{(qx - x)}.$$

The pair $\{\tau_q, \delta_q\}$ is an R-point of $k_q[x, y]$. The "limit" of the operator δ_q when q tends to 1 is the usual derivative d/dx.

IV.2 Gauss Polynomials and the q-Binomial Formula

We fix an invertible element q of the field k. For future applications, we need to compute the powers of $x+y$ in the quantum plane $k_q[x,y]$. To this end, we introduce the so-called Gauss polynomials which are polynomials in one variable q whose values at $q=1$ are equal to the classical binomial coefficients.

Let us start with some notation. For any integer $n>0$, set

$$(n)_q = 1+q+\cdots+q^{n-1} = \frac{q^n-1}{q-1}. \tag{2.1}$$

Define the q-factorial of n by $(0)!_q = 1$ and

$$(n)!_q = (1)_q(2)_q\dots(n)_q = \frac{(q-1)(q^2-1)\dots(q^n-1)}{(q-1)^n} \tag{2.2}$$

when $n>0$. The q-factorial of n is a polynomial in q with integral coefficients and with value at $q=1$ equal to the usual factorial $n!$. We define the *Gauss polynomials* for $0\le k\le n$ by

$$\binom{n}{k}_q = \frac{(n)!_q}{(k)!_q\,(n-k)!_q}. \tag{2.3}$$

Proposition IV.2.1. *Let $0\le k\le n$.*

(a) $\binom{n}{k}_q$ *is a polynomial in q with integral coefficients and with value at $q=1$ equal to the binomial coefficient $\binom{n}{k}$.*

(b) *We have*

$$\binom{n}{k}_q = \binom{n}{n-k}_q. \tag{2.4}$$

(c) *(q-Pascal identity) We also have*

$$\binom{n}{k}_q = \binom{n-1}{k-1}_q + q^k\binom{n-1}{k}_q = \binom{n-1}{k}_q + q^{n-k}\binom{n-1}{k-1}_q. \tag{2.5}$$

PROOF. Relations (2.4–2.5) follow from easy computations. For Part (a), one proceeds by induction on n using (2.5). □

We return to the quantum plane of Section 1 and prove the q-binomial formula.

Proposition IV.2.2. *Let x and y be variables subject to the quantum plane relation $yx=qxy$. Then for all $n>0$ we have*

$$(x+y)^n = \sum_{0\le k\le n}\binom{n}{k}_q x^ky^{n-k}.$$

PROOF. Because of the universal property of the quantum plane, it suffices to prove the statement in $k_q[x,y]$. Expanding $(x+y)^n$ and using (1.2), we see that the monomials in the expansion are all scalar multiples of monomials of the form x^ky^{n-k}. We therefore have

$$(x+y)^n = \sum_{0\le k\le n}\binom{n}{k}' x^ky^{n-k}$$

where $\binom{n}{k}'$ is a polynomial with integral coefficients in q. Let us prove by induction on n that we have

$$\binom{n}{k}' = \binom{n}{k}_q. \tag{2.6}$$

Relation (2.6) clearly holds for $n=1$. It thus suffices to check that the coefficients $\binom{n}{k}'$ satisfy (2.5). Using (1.2), we have

$$\begin{aligned}\sum_{0\le k\le n}\binom{n}{k}' x^ky^{n-k} &= (x+y)\Big(\sum_{0\le k\le n-1}\binom{n-1}{k}' x^ky^{n-1-k}\Big)\\ &= \sum_{0\le k\le n-1}\binom{n-1}{k}' x^{k+1}y^{n-1-k}\\ &\qquad + \sum_{0\le k\le n-1} q^k\binom{n-1}{k}' x^ky^{n-k}\\ &= \sum_{0\le k\le n}\Big(\binom{n-1}{k-1}' + q^k\binom{n-1}{k}'\Big)x^ky^{n-k}.\end{aligned}$$

We get (2.5) in view of the linear independence of the monomials $\{x^ky^{n-k}\}_k$. □

We now derive a few q-identities from the q-binomial formula. These identities will not be needed in the sequel. The first one is the q-analogue of the *Chu-Vandermonde formula.*

Proposition IV.2.3. *For $m\ge p\le n$, we have*

$$\binom{m+n}{p}_q = \sum_{0\le k\le p} q^{(m-k)(p-k)}\binom{m}{k}_q\binom{n}{p-k}_q.$$

PROOF. Expand both sides of the identity $(x+y)^{m+n} = (x+y)^m(x+y)^n$ using Proposition 2.2 and identify the terms corresponding to $x^p y^{m+n-p}$. □

We introduce a q-variant of the exponential. Let z be a variable (commuting with q). We define the *q-exponential* as the formal series

$$e_q(z) = \sum_{n\geq 0} \frac{z^n}{(n)!_q}. \tag{2.7}$$

Observe that this series is well-defined provided q is not a root of unity, which we assume until the end of this section.

Proposition IV.2.4. *Let x and y be variables such that $yx = qxy$. Then*

$$e_q(x+y) = e_q(x)e_q(y).$$

PROOF. By application of Proposition 2.2, we have

$$\begin{aligned}\Big(\sum_{k\geq 0}\frac{x^k}{(k)!_q}\Big)\Big(\sum_{\ell\geq 0}\frac{y^\ell}{(\ell)!_q}\Big) &= \sum_{n\geq 0}\frac{1}{(n)!_q}\Big(\sum_{k+\ell=n}\frac{(n)!_q}{(k)!_q(\ell)!_q}x^k y^\ell\Big)\\ &= \sum_{n\geq 0}\frac{(x+y)^n}{(n)!_q}.\end{aligned}$$

□

The q-exponential is an invertible formal series, but, in contrast to the case $q = 1$, we have $e_q(z)^{-1} \neq e_q(-z)$. In order to compute the inverse of $e_q(z)$, we consider the algebra of formal series $k[[z]]$ and the algebra $\mathrm{End}(k[[z]])$ of linear endomorphisms of $k[[z]]$. Define two elements Z and τ_q of $\mathrm{End}(k[[z]])$ by $(Zf)(z) = zf(z)$ and $(\tau_q f)(z) = f(qz)$. An easy computation shows that (Z, τ_q) is an $\mathrm{End}(k[[z]])$-point of the quantum plane, which is to say we have the following lemma.

Lemma IV.2.5. *We have $\tau_q Z = q\, Z\tau_q$ in $\mathrm{End}(k[[z]])$.*

If for any scalar a of the field k we apply the endomorphism $((a-Z)\tau_q)^n$ to the constant formal series 1, we get

$$\Big((a-Z)\tau_q\Big)^n(1) = (a-z)(a-qz)\dots(a-q^{n-1}z). \tag{2.8}$$

In particular, for $a = 0$ we have

$$(-Z\tau_q)^n(1) = (-1)^n\, q^{n(n-1)/2}\, z^n. \tag{2.9}$$

Proposition IV.2.6. *The inverse of $e_q(z)$ is given by*

$$e_q(z)^{-1} = \sum_{n\geq 0}(-1)^n\, q^{n(n-1)/2}\,\frac{z^n}{(n)!_q}.$$

PROOF. Lemma 2.5 implies $(-Z\tau_q)Z = qZ(-Z\tau_q)$. Using Proposition 2.4, we get the following identity in $\mathrm{End}(k[[z]])$:

$$e_q(Z(1-\tau_q)) = e_q(Z)\circ e_q(-Z\tau_q). \tag{2.10}$$

Let us apply both sides of (2.10) to the constant formal series 1. On the one hand, we have $e_q(Z(1-\tau_q))(1) = 1$ because $(1-\tau_q)(1) = 0$. On the other hand, by (2.9) we get

$$e_q(Z)\Big(e_q(-Z\tau_q)(1)\Big) = e_q(z)\Big(\sum_{n\geq 0}(-1)^n\, q^{n(n-1)/2}\,\frac{z^n}{(n)!_q}\Big).$$

□

Here are two more general q-identities.

Proposition IV.2.7. *For any scalar a we have*

$$(a-z)(a-qz)\dots(a-q^{n-1}z) = \sum_{k=0}^{n}(-1)^k\binom{n}{k}_q q^{k(k-1)/2}\, a^{n-k} z^k$$

and

$$e_q(a) = e_q(z)\Big(\sum_{n=0}^{\infty}\frac{1}{(n)!_q}\,(a-z)(a-qz)\dots(a-q^{n-1}z)\Big).$$

PROOF. One proceeds as in the proof of Proposition 2.6, but now with the operator identity $(a\tau_q)(-Z\tau_q) = q(-Z\tau_q)(a\tau_q)$. By Propositions 2.2 and 2.4, we get

$$\Big((a-Z)\tau_q\Big)^n = \sum_{k=0}^{n}(-1)^k\binom{n}{k}_q (Z\tau_q)^k\circ(a\tau_q)^{n-k}$$

and

$$e_q((a-Z)\tau_q) = e_q(-Z\tau_q)\circ e_q(a)$$

in $\mathrm{End}(k[[z]])$. Applying again these identities to the constant formal series 1, we get the desired relations in view of $e_q(-Z\tau_q)(1) = e_q(z)^{-1}$, which was proved above. □

IV.3 The Algebra $M_q(2)$

From now on, we assume that $q^2 \neq -1$. Let us define a q-analogue of the algebra $M(2)$ of I.4. In addition to variables x, y subject to the quantum plane relation $yx = qxy$, consider four variables a, b, c, d commuting with x and y. Define x', y', x'', and y'' using the following matrix relations

$$\begin{pmatrix}x'\\y'\end{pmatrix} = \begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} \quad\text{and}\quad \begin{pmatrix}x''\\y''\end{pmatrix} = \begin{pmatrix}a & c\\ b & d\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}. \tag{3.1}$$

Theorem IV.3.1. *Under the previous hypotheses, there is an equivalence between*
(i) *the two relations* $y'x' = qx'y'$ *and* $y''x'' = qx''y''$, *and*
(ii) *the six relations*

$$ba = qab, \qquad db = qbd, \tag{3.2}$$

$$ca = qac, \qquad dc = qcd, \tag{3.3}$$

$$bc = cb, \quad ad - da = (q^{-1} - q)\,bc. \tag{3.4}$$

PROOF. Let us check that (i) implies (ii). By (3.1) we have

$$(cx + dy)(ax + by) = q\,(ax + by)(cx + dy).$$

Identifying the coefficients of x^2, y^2, and of xy, we obtain

$$ca = qac, \quad db = qbd, \quad cb + qda = qad + q^2bc. \tag{3.5}$$

Dividing the latter by q yields

$$ad - da = q^{-1}cb - qbc. \tag{3.6}$$

Using x'' and y'' in a similar fashion leads to three more relations obtained from (3.5–3.6) by exchanging b and c, namely

$$ba = qab, \quad dc = qcd, \quad ad - da = q^{-1}bc - qcb. \tag{3.7}$$

From (3.6–3.7) we derive $(q^{-1} + q)(bc - cb) = 0$, which is equivalent to $bc = cb$ since $q^2 \neq -1$. We have proved that (i) implies (ii). The converse implication follows from similar straightforward computations. □

Definition IV.3.2. *The algebra* $M_q(2)$ *is the quotient of the free algebra* $k\{a, b, c, d\}$ *by the two-sided ideal* J_q *generated by the six relations* (3.2–3.4) *of Theorem* 3.1.

When $q = 1$, the algebra $M_q(2)$ is clearly isomorphic to the algebra $M(2)$ of I.4. Since the ideal J_q is generated by quadratic elements, the natural grading of the free algebra induces a grading on $M_q(2)$ such that the generators a, b, c, d are of degree 1.

Given an algebra R, we define an *R-point of $M_q(2)$* to be a quadruple $(A, B, C, D) \in R^4$ satisfying the relations

$$BA = qAB, \qquad DB = qBD, \tag{3.8}$$

$$CA = qAC, \qquad DC = qCD, \tag{3.9}$$

$$BC = CB, \quad AD - DA = (q^{-1} - q)\,BC. \tag{3.10}$$

By the very definition of $M_q(2)$, the set of R-points of $M_q(2)$ is in bijection with the set $\mathrm{Hom}_{Alg}(M_q(2), R)$ of algebra morphisms from $M_q(2)$ to R. It

will sometimes be convenient and more enlightening to write an R-point (A, B, C, D) of $M_q(2)$ in the matrix form

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}. \tag{3.11}$$

Theorem 3.1 can be paraphrased using the language of R-points as follows: a quadruple $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ of elements of an algebra R is an R-point of $M_q(2)$ if and only if the following pairs (X', Y') and (X'', Y'') are R'-points of the quantum plane, where X', Y', X'', Y'' are matricially defined by

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} X'' \\ Y'' \end{pmatrix} = \begin{pmatrix} A & C \\ B & D \end{pmatrix}\begin{pmatrix} X \\ Y \end{pmatrix}$$

and where R' is the tensor product algebra

$$R' = R \otimes k_q[X, Y] = R\{X, Y\}/(YX - qXY).$$

We now introduce the quantum determinant $\det_q$ as the following element of the algebra $M_q(2)$.

Proposition IV.3.3. *The element* $\det_q = ad - q^{-1}bc = da - qbc$ *of* $M_q(2)$ *is central.*

PROOF. It suffices to show that $\det_q$ commutes with the generators a, b, c, d. Now, by (3.2–3.4) we have

$$(ad - q^{-1}bc)a = a(da - qbc), \quad (ad - q^{-1}bc)b = b(ad - q^{-1}bc),$$

$$(ad - q^{-1}bc)c = c(ad - q^{-1}bc), \quad (da - qbc)d = d(ad - q^{-1}bc). \qquad \square$$

Given an R-point $m = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ of $M_q(2)$, the element

$$\mathrm{Det}_q(m) = AD - q^{-1}BC = DA - qBC$$

of R is called the *quantum determinant* of m.

Proposition IV.3.4. *Let R be an algebra and*

$$m = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \quad \textit{and} \quad m' = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix}$$

be two R-points of $M_q(2)$ such that the elements A, B, C, D commute with the elements A', B', C', D'.

(a) *The element $m'm$ defined by the matrix product*

$$m'm = \begin{pmatrix} A'' & B'' \\ C'' & D'' \end{pmatrix} = \begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

is an R-point of $M_q(2)$.

(b) *We have* $\mathrm{Det}_q(m'm) = \mathrm{Det}_q(m')\,\mathrm{Det}_q(m)$ *in R.*

(c) *The quadruple*

$$\begin{pmatrix} D & -qB \\ -q^{-1}C & A \end{pmatrix}$$

is an R-point of $M_{q^{-1}}(2)$ and an R^{op}-point of $M_q(2)$.

PROOF. (a) We use the reformulation of Theorem 3.1 stated a few lines ahead of Proposition 3.3. Let R' be the tensor product algebra

$$R' = R \otimes k_q[X, Y] = R\{X, Y\}/(YX - qXY).$$

Define X', Y', X'', Y'' by

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} X'' \\ Y'' \end{pmatrix} = \begin{pmatrix} A' & C' \\ B' & D' \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}.$$

By definition, the elements X, Y of R' commute with the other variables A, A', etc. It results from Theorem 3.1 that the pairs (X', Y') and (X'', Y'') are R'-points of the quantum plane. Now, by hypothesis, the elements A', B', C', D' of R' commute with X' and Y' and the elements A, B, C, D commute with X'' and Y''. By a second application of Theorem 3.1,

$$\begin{pmatrix} A' & B' \\ C' & D' \end{pmatrix} \begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} A'' & B'' \\ C'' & D'' \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$$

and

$$\begin{pmatrix} A & C \\ B & D \end{pmatrix} \begin{pmatrix} X'' \\ Y'' \end{pmatrix} = \begin{pmatrix} A'' & C'' \\ B'' & D'' \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$$

are R'-points of the quantum plane. It follows that $m'm$ is an R-point of $M_q(2)$.

(b) This follows from computations we leave to the reader. A more conceptual method is suggested as an exercise at the end of this chapter.

(c) Define $A' = D$, $B' = -qB$, $C' = -q^{-1}C$, and $D' = A$. Then Relations (3.8–3.10) imply

$$A'B' = qB'A', \qquad B'D' = qD'B',$$

$$A'C' = qC'A', \qquad C'D' = qD'C',$$

$$C'B' = B'C', \quad D'A' - A'D' = (q^{-1} - q)\,B'C',$$

which means precisely that (A', B', C', D') is an R-point of $M_{q^{-1}}(2)$ or an R^{op}-point of $M_q(2)$. □

IV.4 Ring-Theoretical Properties of $M_q(2)$

The aim of this section is to show that the algebra $M_q(2)$, though non-commutative, retains certain properties of the commutative algebra $M(2)$. We freely use the notations and the results of I.7–8.

Theorem IV.4.1. *The algebra $M_q(2)$ is Noetherian and has no zero divisors. A basis for the underlying vector space is given by the set of monomials* $\{a^i b^j c^k d^\ell\}_{i,j,k,\ell \geq 0}$.

We shall prove this theorem by building a tower

$$A_0 = k \subset A_1 \subset A_2 \subset A_3 \subset A_4 = M_q(2)$$

of algebras such that each A_i is an Ore extension of A_{i-1}. As a consequence of Corollary I.7.2, we conclude that the set $\{\sigma(a)^i \sigma(b)^j \sigma(c)^k \sigma(d)^\ell\}_{i,j,k,\ell \geq 0}$ is also a basis of $M_q(2)$ for any permutation σ of the set $\{a, b, c, d\}$. Define the algebras $A_1 = k[a]$, $A_2 = k\{a, b\}/(ba - qab)$, and

$$A_3 = k\{a, b, c\}/(ba - qab, ca - qac, cb - bc).$$

The algebra A_1 is trivially an Ore extension of A_0. Let α_1 be the automorphism of A_1 determined by $\alpha_1(a) = qa$.

Lemma IV.4.2. *There is an isomorphism between A_2 and the Ore extension $A_1[b, \alpha_1, 0]$. Furthermore, the set $\{a^i b^j\}_{i,j \geq 0}$ is a basis of A_2.*

Observe that the algebra A_2 is isomorphic to the quantum plane $k_q[x, y]$ (the isomorphism sends a onto x and b onto y).

PROOF. Let us define $\varphi_1 : A_2 \to A_1[b, \alpha_1, 0]$ by $\varphi_1(a) = a$ and $\varphi_1(b) = b$. Since

$$\varphi_1(b)\varphi_1(a) - q\varphi_1(a)\varphi_1(b) = ba - qab = \alpha_1(a)b - qab = 0,$$

φ_1 defines a morphism of algebras. This morphism is surjective since the algebra $A_1[b, \alpha_1, 0]$ is generated by a and b. In order to show that it is an isomorphism, we only have to build a linear map $\psi_1 : A_1[b, \alpha_1, 0] \to A_2$ such that $\psi_1 \circ \varphi_1 = \mathrm{id}$. We define ψ_1 on the basis $\{a^i b^j\}_{i,j \geq 0}$ of $A_1[b, \alpha_1, 0]$ by $\psi_1(a^i b^j) = a^i b^j$. □

It is easy to check that $\alpha_2(a) = qa$ and $\alpha_2(b) = b$ define an automorphism α_2 of the algebra A_2. We have the following result whose proof follows the same lines as the proof of Lemma 4.2.

Lemma IV.4.3. *The algebra A_3 is isomorphic to the algebra $A_2[c, \alpha_2, 0]$; the set $\{a^i b^j c^k\}_{i,j,k \geq 0}$ is a basis of A_3.*

The last step consists in building A_4 out of A_3. This is the only step involving a non-zero derivation. First, one checks that

$$\alpha_3(a) = a, \quad \alpha_3(b) = qb, \quad \alpha_3(c) = qc$$

define an algebra automorphism of A_3. We define another endomorphism δ of A_3 on the basis $\{a^i b^j c^k\}_{i,j,k\geq 0}$ by $\delta(b^j c^k) = 0$ and by

$$\delta(a^i b^j c^k) = (q - q^{-1})\frac{1-q^{2i}}{1-q^2}\, a^{i-1} b^{j+1} c^{k+1} \tag{4.1}$$

if $i > 0$. The proof of the following result is left to the reader.

Lemma IV.4.4. *The endomorphism δ is an α_3-derivation of A_3.*

We use this result to prove the next one.

Lemma IV.4.5. *The algebra $A_4 = M_q(2)$ is isomorphic to the Ore extension $A_3[d, \alpha_3, \delta]$, and $\{a^i b^j c^k d^\ell\}_{i,j,k,\ell\geq 0}$ is a basis of A_4.*

PROOF. Set $\varphi_4(a) = a$, $\varphi_4(b) = b$, $\varphi_4(c) = c$, $\varphi_4(d) = d$. This defines a surjective morphism of algebras φ_4 from A_4 onto the Ore extension $A_3[d, \alpha_3, \delta]$, provided we check that $(\varphi_4(a), \varphi_4(b), \varphi_4(c), \varphi_4(d))$ is an $A_3[d, \alpha_3, \delta]$-point of $M_q(2)$. This implies checking the six relations (3.8–3.10). Now the three relations not involving d already hold in A_3. As for the three remaining, namely

$$db = qbd, \quad dc = qcd, \quad da = ad + (q - q^{-1})bc,$$

they hold in $A_3[d, \alpha_3, \delta]$ by the very definition of α_3 and of δ. To complete the proof, one constructs a linear map ψ_4 such $\psi_4 \circ \varphi_4 = \mathrm{id}$ as in the proof of Lemma 4.2. □

Theorem 4.1 is now a consequence of Lemmas 4.2, 4.3 and 4.5, of Corollary I.7.2, and of Theorem I.8.3.

IV.5 Bialgebra Structure on $M_q(2)$

We now endow the algebra $M_q(2)$ with a bialgebra structure. The comultiplication and the counit will be the same as the comultiplication and the counit put on $M(2)$ in I.4 (see also III.4).

Theorem IV.5.1. *There exist morphisms of algebras*

$$\Delta : M_q(2) \to M_q(2) \otimes M_q(2) \quad \textit{and} \quad \varepsilon : M_q(2) \to k$$

uniquely determined by

$$\Delta(a) = a \otimes a + b \otimes c, \quad \Delta(b) = a \otimes b + b \otimes d, \tag{5.1}$$

$$\Delta(c) = c \otimes a + d \otimes c, \quad \Delta(d) = c \otimes b + d \otimes d, \tag{5.2}$$

$$\varepsilon(a) = \varepsilon(d) = 1, \quad \varepsilon(b) = \varepsilon(c) = 0. \tag{5.3}$$

Equipped with these morphisms, the algebra $M_q(2)$ becomes a bialgebra that is neither commutative nor cocommutative. Furthermore, we have

$$\Delta(\det_q) = \det_q \otimes \det_q \quad \textit{and} \quad \varepsilon(\det_q) = 1. \tag{5.4}$$

We may rewrite Relations (5.1–5.3) in the abridged matrix form

$$\Delta\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad \varepsilon\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{5.5}$$

PROOF. In order to show that Δ is a morphism of algebras, it suffices to check that $(\Delta(a), \Delta(b), \Delta(c), \Delta(d))$ is an $M_q(2) \otimes M_q(2)$-point of $M_q(2)$. This follows from Proposition 3.4 (a). A simple computation shows that $(\varepsilon(a), \varepsilon(b), \varepsilon(c), \varepsilon(d))$ is a k-point of $M_q(2)$, thus proving that ε also defines an algebra morphism.

We now have to check the coassociativity and counit axioms. Let us start with

$$(\Delta \otimes \mathrm{id})\Delta = (\mathrm{id} \otimes \Delta)\Delta. \tag{5.6}$$

Since both sides of (5.6) are morphisms of algebras, it is enough to verify it on the generators a, b, c, d. Using the matrix form, we have

$$\begin{aligned}
\big((\Delta \otimes \mathrm{id})\Delta\big)\begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) \\
&= \big((\mathrm{id} \otimes \Delta)\Delta\big)\begin{pmatrix} a & b \\ c & d \end{pmatrix}.
\end{aligned}$$

A similar argument shows that the counit axiom follows from the matrix identity

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

As for the computation of $\Delta(\det_q)$, it results from Proposition 3.4 (b). □

IV.6 The Hopf Algebras $GL_q(2)$ and $SL_q(2)$

We proceed by analogy with I.5. Using the quantum determinant $\det_q$ of Proposition 3.3, we define the algebras

$$GL_q(2) = M_q(2)[t]/(t \det_q - 1)$$

and

$$SL_q(2) = M_q(2)/(\det_q - 1) = GL_q(2)/(t-1).$$

Given an algebra R, we define an *R-point of $GL_q(2)$* [resp. *of $SL_q(2)$*] as an R-point $m = (A, B, C, D)$ of $M_q(2)$ whose quantum determinant

$$\mathrm{Det}_q(m) = AD - q^{-1}BC$$

is invertible in R [resp. is equal to 1]. Denoting $GL_q(2)$ and $SL_q(2)$ by G_q, we see that the set of R-points of G_q is in bijection with the set $\mathrm{Hom}_{Alg}(G_q, R)$ of algebra morphisms from G_q to R.

Theorem IV.6.1. *Relations* (5.1–5.3) *defining the comultiplication Δ and the counit ε of $M_q(2)$ equip the algebras $GL_q(2)$ and $SL_q(2)$ with Hopf algebra structures such that the antipode S is given in matrix form by*

$$\begin{pmatrix} S(a) & S(b) \\ S(c) & S(d) \end{pmatrix} = \det_q{}^{-1} \begin{pmatrix} d & -qb \\ -q^{-1}c & a \end{pmatrix}. \qquad (6.1)$$

PROOF. (a) We first have to show that Δ and ε are well-defined on $GL_q(2)$ and on $SL_q(2)$. For $SL_q(2)$ this results from the following computations: by (5.4)

$$\Delta(\det_q - 1) = (\det_q - 1) \otimes \det_q + 1 \otimes (\det_q - 1)$$

and $\varepsilon(\det_q - 1) = 0$. A similar argument works for $GL_q(2)$ provided we set

$$\Delta(t) = t \otimes t \quad \text{and} \quad \varepsilon(t) = 1. \qquad (6.2)$$

The coassociativity and counit axioms hold for $GL_q(2)$ and for $SL_q(2)$ since they already hold for $M_q(2)$.

(b) It remains to check that $GL_q(2)$ and $SL_q(2)$ have antipodes. Set

$$S'(a) = d, \quad S'(b) = -qb, \quad S'(c) = -q^{-1}c, \quad S'(d) = a. \qquad (6.3)$$

By Proposition 3.4 (c), the quadruple $(S'(a), S'(b), S'(c), S'(d))$ is a $M_q(2)^{\mathrm{op}}$-point of $M_q(2)$. Consequently, S' defines a morphism of algebras from $M_q(2)$ to $M_q(2)^{\mathrm{op}}$. Next, we extend S' to $GL_q(2)$ and to $SL_q(2)$ by setting $S'(t) = t$. This is a well-defined algebra morphism because

$$S'(t)S'(\det_q) = \big(S'(d)S'(a) - q^{-1}S'(c)S'(b)\big)S'(t) = (ad - q^{-1}bc)\, t = 1.$$

Since the quantum determinant is invertible and central in $G_q = GL_q(2)$ and $SL_q(2)$, it is possible to define an algebra morphism S from G_q to G_q^{op} by $S(t) = t^{-1}$ and

$$\begin{pmatrix} S(a) & S(b) \\ S(c) & S(d) \end{pmatrix} = \det_q{}^{-1} \begin{pmatrix} S'(a) & S'(b) \\ S'(c) & S'(d) \end{pmatrix} = \det_q{}^{-1} \begin{pmatrix} d & -qb \\ -q^{-1}c & a \end{pmatrix}.$$

Finally, to check that S is an antipode, it suffices to work with the generators a, b, c, d, according to Lemma III.3.6. Relations (III.3.3) are equivalent to the matrix identities

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -qb \\ -q^{-1}c & a \end{pmatrix} = \begin{pmatrix} d & -qb \\ -q^{-1}c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \det_q \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

□

In contrast to the inversion in a group and to the antipode of $GL(2)$ and of $SL(2)$, the antipode S of $GL_q(2)$ and of $SL_q(2)$ is in general not involutive. Indeed, from (6.1) we derive

$$\begin{pmatrix} S^{2n}(a) & S^{2n}(b) \\ S^{2n}(c) & S^{2n}(d) \end{pmatrix} = \begin{pmatrix} a & q^{2n}b \\ q^{-2n}c & d \end{pmatrix} = \begin{pmatrix} q^n & 0 \\ 0 & q^{-n} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} q^{-n} & 0 \\ 0 & q^n \end{pmatrix}$$

for any positive integer n. Fix such an n and let q be a root of unity of order exactly n. Then we obtain two examples of Hopf algebras for which the square of the antipode has order n. For results on the order of S^2 previous to the quantum group era, see [Rad76] [Taf71] [TW80].

IV.7 Coaction on the Quantum Plane

We saw in III.7 that the affine plane $k[x, y]$ was a comodule-algebra over either one of the bialgebras $M(2)$ and $SL(2)$. We now develop a quantum version of this.

Theorem IV.7.1. *There exists a unique $M_q(2)$-comodule-algebra structure and a unique $SL_q(2)$-comodule-algebra structure on the quantum plane $A = k_q[x, y]$ such that*

$$\Delta_A(x) = a \otimes x + b \otimes y \quad \textit{and} \quad \Delta_A(y) = c \otimes x + d \otimes y.$$

We rewrite these formulas in the matrix form

$$\Delta_A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} x \\ y \end{pmatrix}. \qquad (7.1)$$

PROOF. We use Proposition III.7.2. We first check that (7.1) defines an algebra morphism Δ_A from A to $M_q(2) \otimes A$. It is enough to verify that

$$\Delta_A(y)\Delta_A(x) = q\, \Delta_A(x)\Delta_A(y)$$

in $M_q(2) \otimes A$. Now, by (3.2–3.4), we have

$$\begin{aligned}\Delta_A(y)\Delta_A(x) &= (c\otimes x + d\otimes y)(a\otimes x + b\otimes y)\\ &= qac\otimes x^2 + (bc+qda)\otimes xy + qbd\otimes y^2\\ &= q\left(ac\otimes x^2 + (q^{-1}bc+ad)\otimes xy + bd\otimes y^2\right)\\ &= q\,(a\otimes x + b\otimes y)(c\otimes x + d\otimes y)\\ &= q\,\Delta_A(x)\Delta_A(y).\end{aligned}$$

Since the projection of $M_q(2)$ onto $SL_q(2)$ is a morphism of algebras, the resulting map $A \to SL_q(2)\otimes A$ is an algebra morphism too.

It remains to check that Δ_A defines a comodule structure on the quantum plane. This is done as in the proof of Theorem III.7.3. □

We record the following quantum version of Lemma III.7.4.

Lemma IV.7.2. *For $i, j \geq 0$ we have*

$$\Delta_A(x^i y^j) = \sum_{r=0}^{i}\sum_{s=0}^{j} q^{(i-r)s}\binom{i}{r}_{q^2}\binom{j}{s}_{q^2} a^r b^{i-r} c^s d^{j-s}\otimes x^{r+s}y^{i+j-r-s}.$$

PROOF. We first observe that $\Delta_A(x^i y^j) = \Delta_A(x)^i\Delta_A(y)^j$ since Δ_A is an algebra morphism. Next, we have

$$(b\otimes y)(a\otimes x) = q^2\,(a\otimes x)(b\otimes y) \quad\text{and}\quad (d\otimes y)(c\otimes a) = q^2\,(c\otimes a)(d\otimes y)$$

in the algebra $M_q(2)\otimes A$. This allows us to apply Proposition 2.2 to both

$$\Delta_A(x)^i = (a\otimes x + b\otimes y)^i \quad\text{and}\quad \Delta_A(y)^j = (c\otimes a + d\otimes y)^j. \qquad \square$$

Denote by $k_q[x,y]_n$ the subspace of degree n elements of $A = k_q[x,y]$. As a consequence of Lemma 7.2, we see that $k_q[x,y]_n$ is a subcomodule of the quantum plane. Actually, the quantum plane is the direct sum of the comodules $k_q[x,y]_n$. By III.6, Example 2, the dual vector space $k_q[x,y]_n^*$ is a module over the algebra $SL_q(2)^*$ dual to the coalgebra $SL_q(2)$. We shall identify this module in VII.5.

IV.8 Hopf $*$-Algebras

The standing assumption in this section is that the ground field k is the field of complex numbers. Given a complex number z, we denote its complex conjugate by $\bar{z}$. Recall that an $\mathbf{R}$-linear map $u : V \to V'$ between complex vector spaces is said to be *antilinear* if $u(\lambda v) = \bar{\lambda} v$ for all $\lambda \in \mathbf{C}$ and $v \in V$.

Definition IV.8.1. *Let $(H, \mu, \eta, \Delta, \varepsilon, S)$ be a complex Hopf algebra. We say that H is a Hopf $*$-algebra if there exists an antilinear involution * on H satisfying the two conditions*

(i) the map * is an antimorphism of real algebras, i.e., an algebra morphism from H into $H^{\rm op}$, as well as a morphism of real coalgebras, and

(ii) we have $S(S(x)^*)^* = x$ for all $x \in H$.

Two Hopf $*$-algebra structures $*_1$ and $*_2$ on H are equivalent if there exists a Hopf algebra automorphism φ of H such that $\varphi(x^{*_1}) = \varphi(x)^{*_2}$ for all x in H.

We wish to show that the Hopf algebras $GL_q(2)$ and $SL_q(2)$ have natural Hopf $*$-algebra structures given by matrix transposition. We shall need the following equivalent formulation.

Lemma IV.8.2. *A Hopf algebra H has a Hopf $*$-algebra structure if and only if there exists an antilinear automorphism γ of H such that*

(i) the map γ is a morphism of real algebras and an antimorphism of real coalgebras, and

(ii) we have $\gamma^2 = (S\gamma)^2 = \mathrm{id}_H$.

PROOF. Suppose we have an involution $*$ as in Definition 8.1. Define γ by $\gamma(x) = S^{-1}(x^*)$ for all $x \in H$. It is clear that γ is an antilinear algebra automorphism. It is an antimorphism of coalgebras because so are the antipode S and its inverse by Theorem III.3.4 (a). We have $S\gamma = *$, which shows that $S\gamma$ is an involution. Finally, γ is an involution too, as can been seen from

$$\gamma^2 = (S^{-1}*)^2 = ((*S)^2)^{-1} = \mathrm{id}_H^{-1} = \mathrm{id}_H.$$

The second equality follows from $*$ being an involution while the third one follows from Definition 8.1 (ii). Conversely, define $* = S\gamma$ from an automorphism γ as in Lemma 8.2. It is an involution by Lemma 8.2 (ii). Let us check Condition (ii) of Definition 8.1. We have

$$(*S)^2 = (S\gamma S)^2 = (S\gamma)^2\gamma^{-1}(S\gamma)^2\gamma^{-1} = \gamma^{-2} = \mathrm{id}_H. \qquad \square$$

We now present the main result of this section. We freely use the notation of the previous sections. Recall the inverse t of the element $\det_q = ad - q^{-1}bc$ of $GL_q(2)$. In $SL_q(2)$ we have $t = 1$.

Theorem IV.8.3. *There exist unique Hopf $*$-algebra structures on the Hopf algebras $GL_q(2)$ and $SL_q(2)$ such that*

$$a^* = td, \quad b^* = -q\,tc, \quad c^* = -q^{-1}tb, \quad d^* = ta, \quad t^* = t^{-1}.$$

PROOF. By Theorem 3.1, the transpose $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is an $M_q(2)$-point of $M_q(2)$. Consequently, there exists a unique antilinear algebra endomorphism γ of $M_q(2)$ defined by the matrix identity

$$\begin{pmatrix} \gamma(a) & \gamma(b) \\ \gamma(c) & \gamma(d) \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}. \tag{8.1}$$

Since transposition is involutive, so is γ. The map γ is an antimorphism of coalgebras in view of the formula (5.5) giving the comultiplication on $M_q(2)$ and of the fact that matrix transposition reverses products.

We now extend γ to $GL_q(2)$ by $\gamma(t) = t$. Since $\gamma(t\det_q - 1) = t\det_q - 1$, it defines an antilinear algebra automorphism both on $GL_q(2)$ and on $SL_q(2)$. Let us check that $S\gamma$ is an involution. It is enough to verify this on the generators a, b, c, d, and t. For t, this is clear. For the remaining generators, we have

$$(S\gamma)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = t\begin{pmatrix} d & -qc \\ -q^{-1}b & a \end{pmatrix}.$$

Therefore,

$$\begin{aligned}(S\gamma)^2\begin{pmatrix} a & b \\ c & d \end{pmatrix} &= (S\gamma)\begin{pmatrix} d & -qc \\ -q^{-1}b & a \end{pmatrix}(S\gamma)(t) \\ &= t\begin{pmatrix} a & b \\ c & d \end{pmatrix}t^{-1} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}.\end{aligned}$$

We conclude the proof by recalling that $* = S\gamma$. □

IV.9 Exercises

1. (*Gauss*) Show that

$$\sum_{0\leq k\leq n} (-1)^k \begin{pmatrix} n \\ k \end{pmatrix}_q = \begin{cases} 0 & \text{if } n \text{ is odd} \\ (1-q)(1-q^3)\dots(1-q^{n-1}) & \text{if } n \text{ is even.} \end{cases}$$

2. (*Gauss*) Show that

$$\begin{pmatrix} n+m+1 \\ m+1 \end{pmatrix}_q = \sum_{0\leq k\leq n} q^k \begin{pmatrix} m+k \\ m \end{pmatrix}_q.$$

3. Let F be a finite field of order q.

(a) Show that $\begin{pmatrix} n \\ k \end{pmatrix}_q$ is equal to the number of k-dimensional subspaces of a n-dimensional vector space over F.

(b) Prove Relations (2.4–2.5) using the previous assertion.

4. (*q-differentiation*) Consider the linear endomorphisms Z, τ_q, and δ_q of the polynomial algebra $k[z]$ and of the algebra $k[[z]]$ of formal series, defined by

$$(Zf)(z) = zf(z), \quad (\tau_q(f))(z) = f(qz), \quad (\delta_q(f))(z) = \frac{f(qz) - f(z)}{(qz - z)}.$$

(a) Check that

$$\delta_q\tau_q = q\,\tau_q\delta_q, \quad [\delta_q, Z] = \tau_q, \quad \delta_q Z - q\,Z\delta_q = 1.$$

(b) Prove that τ_q is an algebra automorphism and that δ_q is a τ_q-derivation.

(c) Show that any τ_q-derivation δ of $k[z]$ is of the form $\delta = P\delta_q$ for some polynomial P. If, moreover, $\delta\tau_q = q\,\tau_q\delta$, then P has to be a constant.

(d) Assume that q is not a root of unity. Check that

$$\delta_q\Big(\frac{z^n}{(n)!_q}\Big) = \frac{z^{n-1}}{(n-1)!_q}$$

for all $n \geq 1$. Deduce that the q-exponential $e_q(z)$ is, up to a multiplicative constant, the only formal series solution of the equation $\delta_q(f) = f$.

5. Let $\Lambda_q[\xi, \eta]$ be the algebra $k\{\xi, \eta\}/(\xi^2, \eta^2, \xi\eta + q\,\eta\xi)$. Set

$$\begin{pmatrix} \xi' \\ \eta' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \xi \\ \eta \end{pmatrix}$$

where a, b, c and d are variables commuting with ξ and η. Assume that $q^2 \neq -1$.

(a) Prove that Assertions (i) and (ii) of Theorem 3.1 are equivalent to the relations

$$y'x' = qx'y' \quad \text{and} \quad \xi'^2 = \eta'^2 = \xi\eta + q\,\eta\xi = 0.$$

(b) Check that $(a\xi + b\eta)(c\xi + d\eta) = \det_q \xi\eta$. Deduce Part (b) of Proposition 3.4.

(c) Find a $M_q(2)$-comodule-algebra structure on $\Lambda_q[\xi, \eta]$.

6. Show that the centre of $M_q(2)$ is the subalgebra generated by $\det_q$ when q is not a root of unity.

7. (*Basis of $SL_q(2)$*) Show that the set $\{a^ib^jc^k\}_{i,j,k\geq 0}\cup\{b^ic^jd^k\}_{i,j\geq 0,k>0}$ is a basis of $SL_q(2)$.

8. Let q be a root of unity of order $d>1$. Prove that $yx=qxy$ implies
$$(x+y)^d = x^d + y^d.$$

9. Let H be a complex Hopf $*$-algebra whose counit is denoted ε. Show that $\varepsilon(x^*)=\overline{\varepsilon(x)}$ for all elements x of H.

IV.10 Notes

The content of Section 2 on q-identities, as well as Exercises 1–3, is classical. We borrowed it from [And76], Chap. 3 and from [Cig79].

The q-exponential is an example of a *q-hypergeometric series* or *basic hypergeometric series*, i.e., of a formal series $\sum_{n\geq 0} a_n z^n$ such that each quotient a_{n+1}/a_n is a rational function of q^n (where q is a complex parameter different from 0 and from 1). Basic hypergeometric series first appeared in a note published by Heine [Hei46] in 1846. Since, q-analogues of most classical functions and identities have been found. F.H. Jackson [Jac10] introduced the q-differentiation operator δ_q and its inverse which is the q-integration. Nowadays, q-series appear in combinatorics, in number theory, in statistical mechanics, and in the theory of Lie algebras. There are many monographs on this vast subject, e.g., [GR90] [Sla66].

The operator τ_q introduced in Section 2 is fundamental in the theory of linear q-difference equations with polynomial coefficients. Such an equation is a functional equation of the form
$$\sum_{i=0}^{n} P_i(z)f(q^iz) = Q(z)$$
where $P_0(z),\dots,P_n(z),Q(z)$ are polynomials and $f(z)$ is a function. Using the operator τ_q, one can rewrite the equation above as $(\sum_{i=0}^n P_i\tau_q^i)(f)=Q$. The articles by Adams [Ada29] and by Trjitzinsky [Trj33] are two classical references on the formalism of the q-difference equations.

Sections 3, 5 and 6 are taken from Manin's book [Man88]. With Section 3 we entered the heart of the subject of Part I of this book. The bialgebras $M_q(2)$, $GL_q(2)$, and $SL_q(2)$ of Sections 5–6 depend on one parameter. There also exist two-parameter versions such as the algebra $M_{p,q}(2)$ generated by four generators a, b, c, d and the six relations

$$ba = pab, \qquad db = qbd,$$
$$ca = qac, \qquad dc = pcd,$$
$$bc = pq^{-1}cb, \quad ad - da = (q^{-1}-p)\,cb.$$

It has the same bialgebra structure as $M(2)$. With the additional relation $ad - p^{-1}bc = 1$, one gets the Hopf algebra $SL_{p,q}(2)$ of [AST91].

In higher dimension $n>2$, Faddeev, Reshetikhin, Takhtadjian [RTF89] defined the bialgebra $M_q(n)$ generated by the generators $(T_i^j)_{1\leq i,j\leq n}$ and the relations
$$T_i^mT_i^k = q\,T_i^kT_i^m, \qquad T_j^mT_i^m = q\,T_i^mT_j^m,$$
$$T_i^mT_j^k = T_j^kT_i^m, \quad T_i^kT_j^m - T_j^mT_i^k = (q^{-1}-q)\,T_i^mT_j^k$$
for $i<j$ and $k<m$. The comultiplication and the counit are given by
$$\Delta(T_i^j) = \sum_{k=1}^{n} T_i^k\otimes T_k^j \quad\text{and}\quad \varepsilon(T_i^j)=\delta_{ij}.$$

The algebra $M_q(n)$ is an iterated Ore extension and, like $M_q(2)$, it possesses a remarkable grouplike central element that is
$$\det_q = \sum_{\sigma\in S_n} (-q)^{-\ell(\sigma)}\,T_1^{\sigma(1)}\dots T_n^{\sigma(n)},$$
where $\ell(\sigma)$ is the length of a minimal decomposition of the permutation σ in product of transpositions. The quantum determinant $\det_q$ allows one to construct $GL_q(n)$ and $SL_q(n)$ as in the case $n=2$ discussed in this chapter. The bialgebra $M_q(n)$ has two interesting comodule-algebras: the first one
$$A_q^{n|0} = k\{x_1,\dots,x_n\}/(x_jx_i - qx_ix_j \;\text{ for } i<j)$$
generalizes the quantum plane whereas the second one
$$A_q^{0|n} = k\{\xi_1,\dots,\xi_n\}/(\xi_i^2, \xi_j\xi_i + q\xi_i\xi_j \;\text{ for } i<j)$$
generalizes the algebra $\Lambda_q[\xi,\eta]$ of Exercise 5.

Both algebras $A_q^{n|0}$ and $A_q^{0|n}$ are examples of *quadratic algebras*, i.e., of quotients of free algebras by ideals generated by degree-two homogeneous elements. For authors like Manin, quadratic algebras form the starting point of the theory of quantum groups. Manin assigns to every quadratic algebra a universal Hopf algebra over which the given quadratic algebra is a comodule-algebra. When applied to the quantum plane, Manin's construction yields $GL_q(2)$. For further reading, see [Man87] [Man88].

We have just mentioned the quantum groups $SL_q(n)$. There exist quantum groups for all classical Lie groups and supergroups. For instance, Takeuchi [Tak89] constructed quantum versions of the symplectic and orthogonal groups.

Woronowicz exhibited Hopf $*$-algebra structures on quantum groups in the framework of C^*-algebras. See [Wor87b] [Wor87a] [Wor88].

The reader will find more examples of and more details on quantum groups in [AST91] [Mal90] [Mal93] [Man89] [PW91] [Res90] [Sud90] [Tak92c].

Chapter V

The Lie Algebra of $SL(2)$

...is chapter we investigate the enveloping Hopf algebra $U = U(\mathfrak{sl}(2))$ of ... Lie algebra $\mathfrak{sl}(2)$ of traceless two-by-two matrices. This Hopf algebra ... duality with $SL(2)$. We also describe the finite-dimensional repre... tions of U. Chapter V prepares for Chapters VI–VII where we shall ... truct a q-deformation U_q of U and study its finite-dimensional repre... tions. The statements and proofs for U_q will essentially be copied from ... of the present chapter. We start by recalling the classical concepts of ... lgebras and enveloping algebras. As usual, we denote the ground field ...

Lie Algebras

...ition V.1.1. (a) *A Lie algebra L is a vector space with a bilinear* $[\,,\,] : L \times L \to L$, *called the Lie bracket, satisfying the following two* ...*ions for all* $x, y, z \in L$:

(antisymmetry)

$$[x, y] = -[y, x],$$

(Jacobi identity)

$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0.$$

A Lie subalgebra L' of a Lie algebra L is a subspace L' of L such ...*r any* $(x, y) \in L' \times L'$ *we have* $[x, y] \in L'$. *An ideal I of a Lie algebra*

L is a subspace I of L such that for any element $(x, y) \in L \times I$ we have $[x, y] \in I$.

(c) *A morphism of Lie algebras f from the Lie algebra L into the Lie algebra L' is a linear map $f : L \to L'$ such that $f([x, y]) = [f(x), f(y)]$ for all $x, y \in L$.*

(d) *A Lie algebra is abelian if its Lie bracket is zero.*

Let us give a few examples of Lie algebras.

1. If L and L' are Lie algebras, we equip the direct sum $L \oplus L'$ with a Lie bracket given by

$$[(x, x'), (y, y')] = ([x, y], [x', y'])$$

for $x, y \in L$ and $x', y' \in L'$. The canonical injections of L and L' into $L \oplus L'$ and the canonical projections of $L \oplus L'$ onto L and L' are morphisms of Lie algebras.

2. Given a Lie algebra L, we define the opposite Lie algebra L^{op} as the vector space L with Lie bracket $[-, -]^{\mathrm{op}}$ given by

$$[x, y]^{\mathrm{op}} = [y, x] = -[x, y].$$

The linear map $\mathrm{op}(x) = -x$ is a Lie algebra isomorphism from L to L^{op}.

3. Let I be an ideal of a Lie algebra L. There exists a unique Lie algebra structure on the quotient vector space L/I such that the canonical projection from L onto L/I is a morphism of Lie algebras.

4. Let $f : L \to L'$ be a morphism of Lie algebras. Its kernel $\mathrm{Ker}\,(f)$ is an ideal of L, the image $f(L)$ is a subalgebra of L', and the induced map $L/\mathrm{Ker}\,(f) \to f(L)$ is an isomorphism of Lie algebras.

5. Let A be an (associative) algebra. Set $[a, b] = ab - ba$ for $a, b \in A$. It is easy to show that this bilinear map is antisymmetric and satisfies the Jacobi identity. We also have $[a, bc] = [a, b]c + b[a, c]$ for all $a, b, c \in A$. This Lie algebra will be denoted by $\mathrm{L}(A)$.

For any vector space V, we denote the Lie algebra $\mathrm{L}(\mathrm{End}(V))$ of all endomorphisms of V by $\mathfrak{gl}(V)$. When V is of finite dimension n, then $\mathfrak{gl}(V)$ is isomorphic to the Lie algebra $\mathfrak{gl}(n) = \mathrm{L}(M_n(k))$ of $n \times n$-matrices with entries in the field k. It is clear that the commutator of two matrices with zero trace is of trace zero. Consequently, the vector space $\mathfrak{sl}(n)$ of traceless n by n matrices is a Lie subalgebra of $\mathfrak{gl}(n)$.

V.2 Enveloping Algebras

To any Lie algebra L we assign an (associative) algebra $U(L)$, called the *enveloping algebra* of L, and a morphism of Lie algebras $i_L : L \to \mathrm{L}(U(L))$. We define the enveloping algebra as follows. Let $I(L)$ be the two-sided

ideal of the tensor algebra $T(L)$ generated by all elements of the form $xy - yx - [x, y]$ where x, y are elements of L. We define

$$U(L) = T(L)/I(L).$$

The above generators of $I(L)$ are not homogeneous for the grading of $T(L)$ defined in II.5. Therefore there is no grading on the enveloping algebra compatible with the grading of the tensor algebra. Nevertheless, $U(L)$ is filtered as a quotient algebra of $T(L)$.

We define a map i_L as the composition of the canonical injection of L into $T(L)$ and of the canonical surjection of the tensor algebra onto the enveloping algebra. By definition of i_L, we have $i_L([x, y]) = xy - yx$, which shows that i_L is a morphism of Lie algebras.

Example 1. If L is an abelian Lie algebra, then $U(L)$ coincides with the symmetric algebra $S(L)$. In particular, if L is the zero Lie algebra $\{0\}$, then $U(\{0\}) = k$. We also have $U(L^{\mathrm{op}}) = U(L)^{\mathrm{op}}$.

We now state the universal property of $U(L)$.

Theorem V.2.1. *Let L be a Lie algebra. Given any associative algebra A and any morphism of Lie algebras f from L into $\mathrm{L}(A)$, there exists a unique morphism of algebras $\varphi : U(L) \to A$ such that $\varphi \circ i_L = f$.*

If we denote by $\mathrm{Hom}_{\mathrm{Lie}}(L, L')$ the set of morphisms of Lie algebras from L into L', we can express Theorem 2.1 by a natural bijection

$$\mathrm{Hom}_{\mathrm{Lie}}(L, \mathrm{L}(A)) \cong \mathrm{Hom}_{Alg}(U(L), A).$$

PROOF. By definition of the tensor algebra, f extends to a morphism of algebras $\bar{f}$ from $T(L)$ to A defined by $\bar{f}(x_1 \ldots x_n) = f(x_1) \ldots f(x_n)$ for $x_1, \ldots, x_n$ in L. The existence of φ follows from $\bar{f}(I(L)) = \{0\}$. In order to prove this fact, we only have to show that $\bar{f}(xy - yx - [x, y])$ vanishes for any pair (x, y) of elements of L. Now,

$$\bar{f}(xy - yx - [x, y]) = f(x)f(y) - f(y)f(x) - f([x, y]),$$

which is zero since f is a morphism of Lie algebras.

The uniqueness of φ is due to the fact that L generates the algebra $T(L)$, hence $U(L)$. □

We derive two corollaries from Theorem 2.1.

Corollary V.2.2. (a) *For any morphism of Lie algebras $f : L \to L'$, there exists a unique morphism of algebras $U(f) : U(L) \to U(L')$ such that $U(f) \circ i_L = i_{L'} \circ f$. We also have $U(\mathrm{id}_L) = \mathrm{id}_{U(L)}$.*

(b) *If $f' : L \to L''$ is another morphism of Lie algebras, then*

$$U(f' \circ f) = U(f') \circ U(f).$$

PROOF. (a) Apply Theorem 2.1 to $A = U(L')$ and to the morphism of Lie algebras $i_{L'} \circ f$.

(b) We have

$$U(f') \circ U(f) \circ i_L = U(f') \circ i_{L'} \circ f = i_{L''} \circ f' \circ f = U(f' \circ f) \circ i_L.$$

One concludes by appealing to the uniqueness of $U(f' \circ f)$ proved in Part (a). The uniqueness assertion also implies that $U(\mathrm{id}_L)$ is the identity of $U(L)$. □

Corollary V.2.3. *Let L and L' be Lie algebras and $L \oplus L'$ their direct sum. Then*

$$U(L \oplus L') \cong U(L) \otimes U(L').$$

PROOF. We first construct an algebra morphism φ from $U(L \oplus L')$ to the algebra $U(L) \otimes U(L')$. For any $x \in L$ and $x' \in L'$, set

$$f(x, x') = i_L(x) \otimes 1 + 1 \otimes i_{L'}(x').$$

This formula defines a linear map f from $L \oplus L'$ into $U(L) \otimes U(L')$. Let us show that f is a morphism of Lie algebras. For $x, y \in L$ and $x', y' \in L'$ we have

$$\begin{aligned}
[f(x,x'), f(y,y')] &= (i_L(x) \otimes 1 + 1 \otimes i_{L'}(x'))(i_L(y) \otimes 1 + 1 \otimes i_{L'}(y')) \\
&\quad - (i_L(y) \otimes 1 + 1 \otimes i_{L'}(y'))(i_L(x) \otimes 1 + 1 \otimes i_{L'}(x')) \\
&= [i_L(x), i_L(y)] \otimes 1 + 1 \otimes [i_{L'}(x'), i_{L'}(y')] \\
&= i_L([x,y]) \otimes 1 + 1 \otimes i_{L'}([x', y']) \\
&= f([x,y], [x', y']) = f([(x,x'), (y,y')]).
\end{aligned}$$

Applying Theorem 2.1, we get an algebra morphism φ from $U(L \oplus L')$ to $U(L) \otimes U(L')$.

We now use the universal property of the tensor product of two algebras in order to build a morphism of algebras $\psi : U(L) \otimes U(L') \to U(L \oplus L')$. The compositions of the canonical injections of L and of L' into $L \oplus L'$ and of the map $i_{L \oplus L'}$ are morphisms of Lie algebras. By Theorem 2.1 there exist morphisms of algebras $\psi_1 : U(L) \to U(L \oplus L')$ and $\psi_2 : U(L') \to U(L \oplus L')$ such that, for any $x \in L$ and $x' \in L'$, we have

$$\psi_1(x) = i_{L \oplus L'}(x, 0) \quad \text{and} \quad \psi_2(x') = i_{L \oplus L'}(0, x').$$

By Proposition II.4.1, the formula $\psi(a \otimes a') = \psi_1(a)\psi_2(a')$ defines an algebra morphism ψ from $U(L) \otimes U(L')$ into $U(L \oplus L')$ provided we show that $\psi_1(a)\psi_2(a') = \psi_2(a')\psi_1(a)$ for all $a \in U(L)$ and $a' \in U(L')$. We prove the latter by observing that it is enough to check that $\psi_1(a)$ and $\psi_2(a')$ commute when $a = x \in L$ and $a' = x' \in L'$. Now,

$$\begin{aligned}
[\psi_1(x), \psi_2(x')] &= [i_{L \oplus L'}(x, 0), i_{L \oplus L'}(0, x')] \\
&= i_{L \oplus L'}([(x,0), (0,x')]) \\
&= i_{L \oplus L'}([x,0], [0,x']) \\
&= 0.
\end{aligned}$$

We claim that the morphisms φ and ψ are inverse of each other. Let us consider the composition $\psi \circ \varphi$. It is an endomorphism of the algebra $U(L \oplus L')$ restricting to the identity on the image of $L \oplus L'$. Indeed, for all $x \in L$ and $x' \in L'$

$$\psi(\varphi(x, x')) = \psi(x \otimes 1) + \psi(1 \otimes x') = i_{L \oplus L'}((x, 0) + (0, x')) = i_{L \oplus L'}(x, x').$$

Consequently, $\psi \circ \varphi = \mathrm{id}$. A similar argument shows that $\varphi \circ \psi = \mathrm{id}$. □

Corollaries 2.2 and 2.3 allow us to put a Hopf algebra structure on the enveloping algebra $U(L)$. Indeed, a comultiplication Δ on $U(L)$ is defined by $\Delta = \varphi \circ U(\delta)$, where δ is the diagonal map $x \mapsto (x, x)$ from L into $L \oplus L$ and φ is the isomorphism $U(L \oplus L) \to U(L) \otimes U(L)$ that was built in the proof of Corollary 2.3. The counit is given by $\varepsilon = U(0)$ where 0 is the zero morphism from L into the zero Lie algebra $\{0\}$. Finally, the antipode is defined by $S = U(\mathrm{op})$ where op is the isomorphism from L onto L^{op} of Example 1.2.

Proposition V.2.4. *The enveloping algebra $U(L)$ is a cocommutative Hopf algebra for the maps Δ, ε, and S defined above. For $x_1, \ldots, x_n \in L$, we have*

$$\begin{aligned}
\Delta(x_1 \ldots x_n) &= 1 \otimes x_1 \ldots x_n + \sum_{p=1}^{n-1} \sum_{\sigma} x_{\sigma(1)} \cdots x_{\sigma(p)} \otimes x_{\sigma(p+1)} \cdots x_{\sigma(n)} \\
&\quad + x_1 \ldots x_n \otimes 1
\end{aligned}$$

where σ runs over all (p,q)-shuffles of the symmetric group S_n, and

$$S(x_1 x_2 \ldots x_n) = (-1)^n \, x_n \ldots x_2 x_1.$$

PROOF. The coassociativity axiom (III.1.5) is satisfied as a consequence of the commutativity of the square

$$\begin{tikzcd}
L \arrow[r, "\delta"] \arrow[d, "\delta"] & L \oplus L \arrow[d, "\mathrm{id} \oplus \delta"] \\
L \oplus L \arrow[r, "\delta \oplus \mathrm{id}"] & L \oplus L \oplus L
\end{tikzcd}$$

the counit axiom (III.1.6) because of the commutativity of the diagram

$$\begin{tikzcd}
0 \oplus L & L \oplus L \arrow[l, "0 \oplus \mathrm{id}"'] \arrow[r, "\mathrm{id} \oplus 0"] & L \oplus 0 \\
& L \arrow[ul, "\cong"] \arrow[u, "\delta"] \arrow[ur, "\cong"'] &
\end{tikzcd}$$

and the cocommutativity (III.1.7) thanks to the commutativity of the triangle

$$\begin{tikzcd} & L \arrow[dl, "\delta"'] \arrow[dr, "\delta"] & \\ L \oplus L \arrow[rr, "\tau"] & & L \oplus L \end{tikzcd}$$

The formula for Δ results from Theorem III.2.4. The definition of S and Lemma III.3.6 imply that S is an antipode for $U(L)$. □

For the sake of completeness, we give two additional important properties of enveloping algebras.

Theorem V.2.5. *Let L be a Lie algebra.*

(a) *The algebra $U(L)$ is filtered as a quotient of the tensor algebra $T(L)$ (graded as in II.5) and the corresponding graded algebra is isomorphic to the symmetric algebra on L:*

$$\operatorname{gr} U(L) \cong S(L).$$

Hence, if $\{v_i\}_{i\in I}$ is a totally ordered basis of L, $\{v_{i_1}\cdots v_{i_n}\}_{i_1\leq\ldots\leq i_n\in I,\, n\in\mathbf{N}}$ is a basis of $U(L)$.

(b) *When the characteristic of the field k is zero, the symmetrization map $\eta : S(L) \to U(L)$ defined by*

$$\eta(v_1\ldots v_n) = \frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}\cdots v_{\sigma(n)} \tag{2.1}$$

for $v_1,\ldots,v_n \in L$, is an isomorphism of coalgebras.

Part (a) of the statement is known as the *Poincaré-Birkhoff-Witt Theorem.* For a proof of Theorem 2.5, we refer to [Bou60] [Dix74] [Hum72] [Jac79].

We end this section by a few remarks on the representations of Lie algebras. By definition, an L-module is a $U(L)$-module in the sense of I.1, which is the same as a morphism of algebras $\rho : U(L) \to \operatorname{End}(V)$. In view of the universal property of $U(L)$ stated in Theorem 2.1, it is equivalent to a morphism (still denoted ρ) of Lie algebras $\rho : L \to \mathfrak{gl}(V)$. For $x \in L$ and $v \in V$, set $xv = \rho(x)(v)$. We observe that $(x,v) \mapsto xv$ is a bilinear map from $L \times V$ to V such that

$$[x,y]v = x(yv) - y(xv) \tag{2.2}$$

for $x, y \in L$ and $v \in V$. Conversely, any bilinear map from $L\times V$ to V such that Relation (2.2) holds for all $x, y \in L$ and $v \in V$, defines an L-module.

The L-module V is trivial in the sense of III.5 if we have $xv = 0$ for all $x \in L$ and $v \in V$. By definition of the coproduct in the enveloping algebra, the structure of L-module on the tensor product of two L-modules V and V' is given by

$$x(v\otimes v') = xv\otimes v' + v\otimes xv' \tag{2.3}$$

for $x \in L$, $v \in V$, and $v' \in V'$. According to III.5, the Lie algebra acts on $\operatorname{Hom}(V, V')$ by

$$(xf)(v) = xf(v) - f(xv), \tag{2.4}$$

which can also be expressed as $\rho(x)(f) = [\rho(x), f]$ for $f \in \operatorname{Hom}(V,V')$. In particular, if V' is the trivial module k, then L acts on the dual vector space $V^* = \operatorname{Hom}(V,k)$ by

$$(xf)(v) = -f(xv). \tag{2.5}$$

Finally, L acts on itself by the so-called *adjoint representation* which is given for $x, x' \in L$ by

$$xx' = [x,x']. \tag{2.6}$$

V.3 The Lie Algebra $\mathfrak{sl}(2)$

To simplify matters, we assume for the rest of this chapter that the ground field k is the field of complex numbers. The Lie algebra $\mathfrak{gl}(2) = \mathrm{L}(M_2(k))$ of 2×2-matrices with complex entries is four-dimensional. The four matrices

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

$$H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

form a basis of $\mathfrak{gl}(2)$. Their commutators are easily computed. We get

$$[X,Y] = H, \quad [H,X] = 2X, \quad [H,Y] = -2Y,$$

and

$$[I,X] = [I,Y] = [I,H] = 0. \tag{3.1}$$

The matrices of trace zero in $\mathfrak{gl}(2)$ form the subspace $\mathfrak{sl}(2)$ spanned by the basis $\{X,Y,H\}$. Relations (3.1) show that $\mathfrak{sl}(2)$ is an ideal of $\mathfrak{gl}(2)$ and that there is an isomorphism of Lie algebras

$$\mathfrak{gl}(2) \cong \mathfrak{sl}(2) \oplus kI,$$

which reduces the investigation of the Lie algebra $\mathfrak{gl}(2)$ to that of $\mathfrak{sl}(2)$.

The enveloping algebra $U = U(\mathfrak{sl}(2))$ of $\mathfrak{sl}(2)$ is isomorphic to the algebra generated by the three elements X, Y, H with the three relations

$$[X,Y] = H, \quad [H,X] = 2X, \quad [H,Y] = -2Y. \tag{3.2}$$

We prove some relations in U.

Lemma V.3.1. *The following relations hold in U for any $p, q \geq 0$:*

$$X^pH^q = (H-2p)^qX^p, \quad Y^pH^q = (H+2p)^qY^p,$$
$$[X, Y^p] = pY^{p-1}(H-p+1) = p(H+p-1)Y^{p-1},$$
$$[X^p, Y] = pX^{p-1}(H+p-1) = p(H-p+1)X^{p-1}.$$

PROOF. One proves the first two relations by an easy double induction on p and q using the relations $XH = (H-2)X$ and $YH = (H+2)Y$, which is another way of expressing the commutation relations (3.2).

We prove the third relation by induction on p. It trivially holds for $p = 1$. When $p > 1$, we have

$$\begin{aligned}
[X, Y^p] &= [X, Y^{p-1}]Y + Y^{p-1}[X, Y] \\
&= (p-1)Y^{p-2}(H-p+2)Y + Y^{p-1}H \\
&= Y^{p-1}\Big((p-1)(H-p) + H\Big) \\
&= pY^{p-1}(H-p+1).
\end{aligned}$$

We conclude by letting Y^{p-1} jump over H according to the second relation.

As for the last relation, it can be obtained from the third one by applying the automorphism σ of $\mathfrak{sl}(2)$ defined by

$$\sigma(X) = Y, \quad \sigma(Y) = X, \quad \sigma(H) = -H. \tag{3.3}$$

□

Proposition V.3.2. *The set $\{X^iY^jH^k\}_{i,j,k\in\mathbf{N}}$ is a basis of $U(\mathfrak{sl}(2))$.*

PROOF. It is a consequence of the Poincaré-Birkhoff-Witt Theorem 2.5. Another proof can be given, using Ore extensions, along the lines of the proof of Proposition VI.1.4. □

We close this section by a few remarks on the centre of U. Let us consider the *Casimir element* defined as the element

$$C = XY + YX + \frac{H^2}{2} \tag{3.4}$$

of the enveloping algebra U.

Lemma V.3.3. *The Casimir element C belongs to the centre of U.*

PROOF. It is enough to show that the Lie brackets of C with H, X, Y vanish. Now,

$$\begin{aligned}
[H, C] &= [H, X]Y + X[H, Y] + [H, Y]X + Y[H, X] + \frac{1}{2}[H, H^2] \\
&= 2XY - 2XY - 2YX + 2YX = 0.
\end{aligned}$$

We also have

$$\begin{aligned}
[X, C] &= X[X, Y] + [X, Y]X + \frac{1}{2}[X, H]H + \frac{1}{2}H[X, H] \\
&= XH + HX - XH - HX = 0.
\end{aligned}$$

One shows $[Y, C] = 0$ in a similar fashion. □

Harish-Chandra constructed an isomorphism of algebras from the centre of U to the polynomial algebra $k[t]$. This isomorphism sends C to the generator t (see for instance [Bou60], Chap. 8 or [Dix74], Chap. 7). As a consequence, the Casimir element generates the centre of the enveloping algebra. We shall give full details in the quantum case (see VI.4).

V.4 Representations of $\mathfrak{sl}(2)$

We now determine all finite-dimensional U-modules. We start with the concept of a highest weight vector.

Definition V.4.1. *Let V be a U-module and λ be a scalar. A vector $v \neq 0$ in V is said to be of weight $\lambda \in k$ if $Hv = \lambda v$. If, in addition, we have $Xv = 0$, then we say that v is a highest weight vector of weight λ.*

Proposition V.4.2. *Any non-zero finite-dimensional U-module V has a highest weight vector.*

PROOF. Since k is algebraically closed and V is finite-dimensional, the operator H has an eigenvector $w \neq 0$ with eigenvalue α: $Hw = \alpha w$. If $Xw = 0$, then w is a highest weight vector and we are done. If not, let us consider the sequence of vectors X^nw. By Lemma 3.1, we have

$$H(X^nw) = (\alpha + 2n)(X^nw).$$

Consequently, $(X^nw)_{n\geq 0}$ is a sequence of eigenvectors for H with distinct eigenvalues. As V is finite-dimensional, H can have but a finite number of eigenvalues; consequently, there exists an integer n such that $X^nw \neq 0$ and $X^{n+1}w = 0$. The vector X^nw is a highest weight vector. □

Lemma V.4.3. *Let v be a highest weight vector of weight λ. For $p \in \mathbf{N}$, set $v_p = \frac{1}{p!}Y^pv$. Then*

$$Hv_p = (\lambda - 2p)\, v_p, \quad Xv_p = (\lambda - p + 1)\, v_{p-1}, \quad Yv_p = (p+1)\, v_{p+1}.$$

PROOF. The third relation is trivial; the first two result from Lemma 3.1. □

We now state the theorem describing simple finite-dimensional U-modules.

Theorem V.4.4. (a) *Let V be a finite-dimensional U-module generated by a highest weight vector v of weight λ. Then*

(i) *The scalar λ is an integer equal to* $\dim(V) - 1$.

(ii) *Setting $v_p = 1/p!\, Y^p v$, we have $v_p = 0$ for $p > \lambda$ and, in addition, $\{v = v_0, v_1, \ldots, v_\lambda\}$ is a basis for V.*

(iii) *The operator H acting on V is diagonalizable with the $(\lambda+1)$ distinct eigenvalues $\{\lambda, \lambda-2, \ldots, \lambda-2\lambda = -\lambda\}$.*

(iv) *Any other highest weight vector in V is a scalar multiple of v and is of weight λ.*

(v) *The module V is simple.*

(b) *Any simple finite-dimensional U-module is generated by a highest weight vector. Two finite-dimensional U-modules generated by highest weight vectors of the same weight are isomorphic.*

PROOF. (a) According to Lemma 4.3, the sequence $\{v_p\}_{p\geq 0}$ is a sequence of eigenvectors for H with distinct eigenvalues. Since V is finite-dimensional, there has to exist an integer n such that $v_n \neq 0$ and $v_{n+1} = 0$. The formulas of Lemma 4.3 then show that $v_m = 0$ for all $m > n$ and $v_m \neq 0$ for all $m \leq n$. We get $n = \lambda$ since we have $0 = Xv_{n+1} = (\lambda - n)v_n$ by Lemma 4.3. The family $\{v = v_0, \ldots, v_\lambda\}$ is free, for it is composed of non-zero eigenvectors for H with distinct eigenvalues. It also generates V; indeed, the formulas of Lemma 4.3 show that any element of V, which is generated by v as a module, is a linear combination of the set $\{v_i\}_i$. It results that $\dim(V) = \lambda + 1$. We have thus proved (i) and (ii). The assertion (iii) is also a consequence of Lemma 4.3.

(iv) Let v' be another highest weight vector. It is an eigenvector for the action of H; hence, it is a scalar multiple of some vector v_i. But, again by Lemma 4.3, the vector v_i is killed by X if and only $i = 0$.

(v) Let V' be a non-zero U-submodule of V and let v' be a highest weight vector of V'. Then v' also is a highest weight vector for V. By (iv), v' is a non-zero scalar multiple of v. Therefore v is in V'. Since v generates V, we must have $V \subset V'$, which proves that V is simple.

(b) Let v be a highest weight vector of V; if V is simple, then the submodule generated by v is necessarily equal to V. Consequently, V is generated by a highest weight vector.

If V and V' are generated by highest weight vectors v and v' with the same weight λ, then the linear map sending v_i to v'_i for all i is an isomorphism of U-modules. □

Up to isomorphism, the simple U-modules are classified by the nonnegative integers: given such an integer n, there exists a unique (up to isomorphism) simple U-module of dimension $n+1$, generated by a highest weight vector of weight n. We denote this module by $V(n)$ and the corresponding morphism of Lie algebras by $\rho(n) : \mathfrak{sl}(2) \to \mathfrak{gl}(n+1)$.

For instance, we have $V(0) = k$ and $\rho(0) = 0$, which means that the module $V(0)$ is trivial, as is also the case for all modules of dimension 1.

More generally, any trivial U-module is isomorphic to a direct sum of copies of $V(0)$.

Observe that the morphism $\rho(1) : \mathfrak{sl}(2) \to \mathfrak{gl}(2)$ is the natural embedding of $\mathfrak{sl}(2)$ into $\mathfrak{gl}(2)$ and that the module $V(2)$ is isomorphic to the adjoint representation of $\mathfrak{sl}(2)$ via the map sending the highest weight vector v_0 onto X, v_1 onto $-H$ and v_2 onto Y.

As for the higher-dimensional module $V(n)$, the generators X, Y, and H act by operators represented by the following matrices in the basis $\{v_0, v_1, \ldots, v_n\}$:

$$\rho(n)(X) = \begin{pmatrix} 0 & n & 0 & \cdots & 0 \\ 0 & 0 & n-1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & 1 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix},$$

$$\rho(n)(Y) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 2 & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & n & 0 \end{pmatrix},$$

and

$$\rho(n)(H) = \begin{pmatrix} n & 0 & \cdots & 0 & 0 \\ 0 & n-2 & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -n+2 & 0 \\ 0 & 0 & \cdots & 0 & -n \end{pmatrix}.$$

Let us determine the action of the Casimir element on the simple module $V(n)$.

Lemma V.4.5. *Any central element of U acts by a scalar on the simple module $V(n)$. In particular, the Casimir element C acts on $V(n)$ by multiplication by the scalar $\frac{n(n+2)}{2}$, which is non-zero when $n > 0$.*

PROOF. Let Z be a central element in U. It commutes with H which decomposes $V(n)$ into a direct sum of one-dimensional eigenspaces. Consequently, the operator Z is diagonal with the same eigenvectors $\{v = v_0, \ldots, v_n\}$ as H. In particular, there exist scalars $\alpha_0, \ldots, \alpha_n$ such that $Zv_p = \alpha_p v_p$ for all p. Now

$$\alpha_{p+1} Y v_p = \alpha_{p+1}(p+1)v_{p+1} = (p+1)Zv_{p+1} = ZYv_p = YZv_p = \alpha_p Y v_p.$$

Consequently, all scalars α_p are equal, which shows that Z acts as a scalar.

In order to determine the action of the Casimir element on $V(n)$, we have only to compute Cv for the highest weight vector v. By (3.4) and by Lemma 4.3 we get

$$Cv = XYv + YXv + \frac{H^2}{2}v = nv + \frac{n^2}{2}v = \frac{n(n+2)}{2}\,v.$$

□

We finally show that any finite-dimensional U-module is a direct sum of simple U-modules.

Theorem V.4.6. *Any finite-dimensional U-module is semisimple.*

PROOF. By Proposition I.1.3, it suffices to show that for any finite-dimensional U-module V and any submodule V' of V, there exists another submodule V'' such that V is isomorphic to the direct sum $V' \oplus V''$. Set $L = \mathfrak{sl}(2)$.

1. We shall first prove the existence of such a submodule V'' in the case when V' is of codimension 1 in V. We proceed by induction on the dimension of V'.

If $\dim(V') = 0$, we may take $V'' = V$. If $\dim(V') = 1$, then necessarily V' and V/V' are trivial one-dimensional representations. Therefore there exists a basis $\{v_1 \in V', v_2\}$ of V such that $Lv_1 = 0$ and $Lv_2 \subset V' = kv_1$. Consequently, we have $[L,L]v_i = 0$ for $i = 1, 2$. Formulas (3.2) show that the action of L on V is trivial. We thus may take for V'' any supplementary subspace of V' in V.

We now assume that $\dim(V') = p > 1$ and that the assertion to be proved holds in all dimensions $< p$. We have the following alternative: either V' is simple, or it is not.

1.a. Let us first suppose that V' is not simple; then there exists a submodule V_1 of V' such that $0 < \dim(V_1) < \dim(V') = p$. Let π be the canonical projection of V onto $\overline{V} = V/V_1$. The module $\overline{V'} = \pi(V')$ is a submodule of $\overline{V}$ of codimension one and its dimension is $< p$. This allows us to apply the induction hypothesis and to find a submodule $\overline{V''}$ of $\overline{V}$ such that $\overline{V} \cong \overline{V'} \oplus \overline{V''}$. Lifting this isomorphism to V, we get

$$V = V' + \pi^{-1}(\overline{V''}).$$

Now, since $\dim(\overline{V''}) = 1$, the vector space V_1 is a submodule of codimension one of $\pi^{-1}(\overline{V''})$. We again apply the induction hypothesis in order to find a submodule V'' of $\pi^{-1}(\overline{V''})$ such that $\pi^{-1}(\overline{V''}) \cong V_1 \oplus V''$. Let us prove that the one-dimensional submodule V'' has the expected properties, namely $V \cong V' \oplus V''$. Indeed, the above argument implies that $V = V' + V_1 + V''$; now V_1 is contained in V', which shows that V is the sum of V' and of V''. The formula $\dim(V) = \dim(V') + \dim(V'')$ implies that this is a direct sum.

1.b. If the submodule V' is simple of dimension > 1, then Lemma 4.5 implies that the Casimir element C acts on V' as a scalar $\alpha \neq 0$. Consequently, the operator C/α is the identity on V'. Now V/V' is one-dimensional, hence a trivial module. Therefore C sends V into the submodule V', which means that the map C/α is a projector of V onto V'. As C/α commutes with any element of U, the map C/α is a morphism of U-modules. By Proposition I.1.3, the submodule $V'' = \operatorname{Ker}(C/\alpha)$ is a supplementary submodule to V'.

2. *General case.* We are now given two finite-dimensional modules $V' \subset V$ without any restriction on the codimension. We shall reduce the situation to the codimension-one case by considering vector spaces $W' \subset W$ defined as follows: W [resp. W'] is the subspace of all linear maps from V to V' whose restriction to V' is a homothety [resp. is zero]. It is clear that W' is of codimension one in W. In order to reduce to Part 1, we have to equip W and W' with U-module structures. We give $\operatorname{Hom}(V, V')$ the U-module structure defined by Relation (2.4). Let us check that W and W' are U-submodules. For $f \in W$, let α be the scalar such that $f(v) = \alpha v$ for all $v \in V'$; then for any $x \in L$, we have

$$(xf)(v) = xf(v) - f(xv) = x(\alpha v) - \alpha(xv) = 0.$$

A similar argument proves that W' is a submodule. Applying Part 1, we get a one-dimensional submodule W'' such that $W \cong W' \oplus W''$. Let f be a generator of W''. By definition, it acts on V' as a scalar $\alpha \neq 0$. It follows that f/α is a projector of V onto V'. To conclude, it suffices to check that f (hence f/α) is a morphism of modules. Now, since W'' is a one-dimensional submodule, it is trivial. Therefore, we have $xf = 0$ for all $x \in L$, which by (2.4) translates into $xf(v) - f(xv) = 0$ for all $v \in V$. □

V.5 The Clebsch-Gordan Formula

Given two finite-dimensional U-modules, we consider their tensor product equipped with the module structure given by Relation (2.3). By Theorem 4.6 it can be decomposed in simple modules. By the distributivity of the tensor product with respect to direct sums and by Theorems 4.4 and 4.6, it is enough to decompose $V(n) \otimes V(m)$ into simple modules. This is the object of the next assertion known as the *Clebsch-Gordan formula*.

Proposition V.5.1. *Consider two nonnegative integers $n \geq m$. Then there exists an isomorphism of U-modules*

$$V(n) \otimes V(m) \cong V(n+m) \oplus V(n+m-2) \oplus \cdots \oplus V(n-m+2) \oplus V(n-m).$$

PROOF. It is enough to prove that, for all p with $0 \leq p \leq m$, the module $V(n) \otimes V(m)$ contains a highest weight vector of weight $n+m-2p$. In effect, if so, there exists a non-zero morphism of modules from $V(n+m-2p)$ into

$V(n)\otimes V(m)$. The module $V(n+m-2p)$ being simple, the kernel of such a morphism has to be zero, which means that the morphism is an embedding of $V(n+m-2p)$ into $V(n)\otimes V(m)$. The submodules $V(n+m-2p)$ being simple and of distinct highest weights, their sum in $V(n)\otimes V(m)$ is direct. Thus, the right-hand side of the Clebsch-Gordan formula embeds into the left-hand side. To conclude, it suffices to check that both sides have the same dimension. Now the dimension of $V(n+m)\oplus V(n+m-2)\oplus\cdots\oplus V(n-m)$ equals

$$\begin{aligned}\sum_{p=0}^{m}(n+m-2p+1) &= (n+1)(m+1)\\ &= \dim(V(n))\dim(V(m))\\ &= \dim(V(n)\otimes V(m)).\end{aligned}$$

Proposition 5.1 will then be a consequence of the following lemma. □

Lemma V.5.2. *Let v be a highest weight vector of $V(n)$ and v' be a highest weight vector of $V(m)$. Define $v_p = \frac{1}{p!}Y^p v$ and $v'_p = \frac{1}{p!}Y^p v'$ for $p \geq 0$. Then*

$$\sum_{i=0}^{p}(-1)^i\,\frac{(m-p+i)!(n-i)!}{(m-p)!n!}\,v_i\otimes v'_{p-i}$$

is a highest weight vector of $V(n)\otimes V(m)$ of weight $n+m-2p$.

PROOF. Set

$$\alpha_i = (-1)^i\,\frac{(m-p+i)!(n-i)!}{(m-p)!n!} \quad\text{and}\quad w=\sum_{i=0}^{p}\alpha_i\,v_i\otimes v'_{p-i}.$$

It is enough to check that $Xw = 0$ and $Hw = (n+m-2p)w$. The latter holds because the tensors $v_i\otimes v'_{p-i}$ all are of weight $n+m-2p$. Indeed, by Lemma 4.3, we have

$$H(v_i\otimes v'_{p-i}) = H(v_i)\otimes v'_{p-i} + v_i\otimes H(v'_{p-i}) = (n+m-2p)\,v_i\otimes v'_{p-i}.$$

Let us compute Xw. By Lemma 4.3 again, we have

$$\begin{aligned}Xw &= \sum_{i=0}^{p}\alpha_i\,X(v_i)\otimes v'_{p-i} + \sum_{i=0}^{p}\alpha_i\,v_i\otimes X(v'_{p-i})\\ &= \sum_{i=0}^{p}\alpha_i(n-i+1)\,v_{i-1}\otimes v'_{p-i} + \sum_{i=0}^{p}\alpha_i(m-p+i+1)\,v_i\otimes v'_{p-i-1}\\ &= \sum_{i=1}^{p}\Big(\alpha_i(n-i+1)+\alpha_{i-1}(m-p+i)\Big)\,v_{i-1}\otimes v'_{p-i}.\end{aligned}$$

Now,

$$\begin{aligned}&\alpha_i(n-i+1)+\alpha_{i-1}(m-p+i)\\ &\quad= (-1)^i\,\frac{(m-p+i)!(n-i)!}{(m-p)!n!}(n-i+1)\\ &\qquad + (-1)^{i-1}\,\frac{(m-p+i-1)!(n-i+1)!}{(m-p)!n!}(m-p+i)\\ &\quad= 0.\end{aligned}$$

□

Remark 5.3. (a) One deduces from Proposition 5.1 that the adjoint representation $V(2)$ is related to $V(0)$ and $V(1)$ by

$$V(1)^{\otimes 2}\cong V(2)\oplus V(0).$$

(b) The dual module $V(n)^*$ is isomorphic to the simple module $V(n)$ (prove it). Consequently, we have the U-linear isomorphisms

$$\mathrm{Hom}(V(n),V(m))\cong V(m)\otimes V(n)^*\cong V(m)\otimes V(n).$$

V.6 Module-Algebra over a Bialgebra. Action of $\mathfrak{sl}(2)$ on the Affine Plane

We now introduce a concept that formalizes nicely many situations where an algebra acts on another one.

Definition V.6.1. *Let H be a bialgebra and A an algebra. We call A a module-algebra over H if*

(a) *the vector space underlying A is an H-module, and*

(b) *the multiplication $\mu : A\otimes A\to A$ and the unit $\eta : k\to A$ of A are morphisms of H-modules, the tensor product $A\otimes A$ and the ground field k being given the H-module structures described by Relations* (III.5.2–5.3).

In the literature, module-algebras over a bialgebra H are also called *H-algebras*. By making explicit Condition (b) of Definition 6.1, we see that A is a module-algebra over H if the action of H on A satisfies the following two compatibility relations with the product and the unit of A:

$$x(ab)=\sum_{(x)}(x'a)(x''b) \tag{6.1}$$

and

$$x1=\varepsilon(x)1 \tag{6.2}$$

where x is an element of H and a, b are elements of A. Here we used Sweedler's sigma notation (see III.1.6). The map ε is the counit of the bialgebra H while 1 is the unit of A.

It is not always convenient to check Relation (6.1) for all elements x of H. The following result shows that it is enough to check it for a set of generators.

Lemma V.6.2. *Let H be a bialgebra and A be an algebra with a structure of H-module such that Relation (6.2) holds. Assume that H is generated as an algebra by a subset X whose elements x satisfy Relation (6.1) for all elements a and b in A. Then A is a module-algebra over H.*

PROOF. It suffices to check that if Relation (6.1) holds for x and y in H, then it also holds for their product xy. Now, for all $a, b \in A$, we have

$$\begin{aligned}(xy)(ab) &= x(y(ab)) \\ &= x\Big(\sum_{(y)} (y'a)(y''b)\Big) \\ &= \sum_{(x)(y)} \Big(x'(y'(a))\Big)\Big(x''(y''(b))\Big) \\ &= \sum_{(x)(y)} \Big((x'y')a\Big)\Big((x''y'')b\Big) \\ &= \sum_{(xy)} \Big((xy)'a\Big)\Big((xy)''b\Big).\end{aligned}$$

□

The following examples show that module-algebra structures appear in a number of situations.

Example 1. Let φ be an automorphism of an algebra A. Consider the algebra $k[\mathbf{Z}]$ of the group of integers with the bialgebra structure described in III.2, Example 2. If $k[\mathbf{Z}]$ acts on A by sending a generator of $\mathbf{Z}$ on φ, then A becomes a module-algebra over $k[\mathbf{Z}]$.

Let us describe module-algebras over enveloping algebras.

Lemma V.6.3. *Let L be a Lie algebra. An algebra A is a module-algebra over $U(L)$ if and only if A has an L-module structure such that the elements of L act on A as derivations.*

PROOF. From Section 2 we know that a $U(L)$-module is an L-module and conversely. Assume that A is a module-algebra over $U(L)$. If $x \in L$ we have $\Delta(x) = x \otimes 1 + 1 \otimes x$. For such an x, Relation (6.1) becomes

$$x(ab) = x(a)b + ax(b)$$

for all $a, b \in A$, which shows that x acts as a derivation. The converse statement results from Lemma 6.2. □

We now return to the Lie algebra $\mathfrak{sl}(2)$ and show how the affine plane becomes a module-algebra over the enveloping algebra $U(\mathfrak{sl}(2))$.

Theorem V.6.4. *Define an action of the Lie algebra $\mathfrak{sl}(2)$ on the polynomial algebra $k[x, y]$ by*

$$XP = x\frac{\partial P}{\partial y}, \quad YP = y\frac{\partial P}{\partial x}, \quad HP = x\frac{\partial P}{\partial x} - y\frac{\partial P}{\partial y}$$

where P denotes any polynomial of $k[x, y]$.

(a) *Then $k[x, y]$ becomes a module-algebra over $U(\mathfrak{sl}(2))$.*

(b) *The subspace $k[x, y]_n$ of homogeneous polynomials of degree n is a submodule of $k[x, y]$ isomorphic to the simple $\mathfrak{sl}(2)$-module $V(n)$.*

We have thus succeeded in packing into a single module all simple finite-dimensional $U(\mathfrak{sl}(2))$-modules, thanks to the notion of module-algebra.

PROOF. (a) We shall first check that the above formulas define an action of $\mathfrak{sl}(2)$ on $k[x, y]$. We have

$$\begin{aligned}[X, Y]P &= x\frac{\partial}{\partial y}\Big(y\frac{\partial P}{\partial x}\Big) - y\frac{\partial}{\partial x}\Big(x\frac{\partial P}{\partial y}\Big) \\ &= x\frac{\partial P}{\partial x} + xy\frac{\partial^2 P}{\partial y \partial x} - y\frac{\partial P}{\partial y} - yx\frac{\partial^2 P}{\partial x \partial y} \\ &= HP.\end{aligned}$$

One similarly shows that $[H, X]P = 2XP$ and $[H, Y]P = -2YP$.

In order to conclude that we have a module-algebra structure, it is enough in view of Lemma 6.3 to check that the generators X, Y, H act on $k[x, y]$ as derivations, which is clearly the case.

(b) Fix a non-negative integer n and set $v = x^n \in k[x, y]_n$. Clearly, v is a highest weight vector of weight n. For all $p \geq 0$ we have

$$v_p = \frac{1}{p!} Y^p v = \binom{n}{p} x^{n-p} y^p$$

if $p \leq n$ and $v_p = 0$ if $p > n$. Since the monomials $\{v_p\}_p$ generate $k[x, y]_n$, the latter is a $\mathfrak{sl}(2)$-module generated by a highest weight vector of weight n. Hence, by Theorem 4.4, it is isomorphic to the simple module $V(n)$. □

V.7 Duality between the Hopf Algebras $U(\mathfrak{sl}(2))$ and $SL(2)$

The main objective of this section is to relate this chapter to Chapter I by building a duality between $U = U(\mathfrak{sl}(2))$ and the Hopf algebra $SL(2)$ defined in I.5. We start with the following definition due to Takeuchi [Tak81].

Definition V.7.1. *Given bialgebras $(U,\mu,\eta,\Delta,\varepsilon)$ and $(H,\mu,\eta,\Delta,\varepsilon)$ and a bilinear form $< \, , \, >$ on $U \times H$, we say that the bilinear form realizes a duality between U and H, or that the bialgebras U and H are in duality, if we have*

$$< uv, x > = \sum_{(x)} < u, x' >< v, x'' >, \tag{7.1}$$

$$< u, xy > = \sum_{(u)} < u', x >< u'', y >, \tag{7.2}$$

$$< 1, x > = \varepsilon(x), \tag{7.3}$$

and

$$< u, 1 > = \varepsilon(u) \tag{7.4}$$

for all $u, v \in U$ and $x, y \in H$.

If, in addition, U and H are Hopf algebras with antipodes S, then they are said to be in duality if the underlying bialgebras are in duality and if, moreover, we have

$$< S(u), x > = < u, S(x) > \tag{7.5}$$

for all $u \in U$ and $x \in H$.

Let us motivate this definition. Let φ be the linear map from U to the dual vector space H^* defined by

$$\varphi(u)(x) = < u, x > .$$

Similarly, $\psi(x)(u) = < u, x >$ defines a linear map from H to U^*. From Proposition III.1.2 we know that the dual spaces U^* and H^* carry natural algebra structures. If, in addition, the vector space H is finite-dimensional, then the dual space H^* has a natural bialgebra structure induced by the one on H (see III.2, Example 1). We are now ready to state a characterization for duality between bialgebras.

Proposition V.7.2. *Given bialgebras U and H and a bilinear form $< \, , \, >$ on $U \times H$, the bilinear form realizes a duality between U and H if and only if the linear maps φ and ψ are morphisms of algebras.*

If, moreover, H is finite-dimensional, then the bilinear form realizes a duality if and only if φ is a morphism of bialgebras.

We shall say that the duality between U and H is *perfect* when both maps φ and ψ are injective. In case U and H are finite-dimensional, a perfect duality between them induces isomorphisms of bialgebras between U and H^* and between H and U^*.

PROOF. Let us express that φ is a morphism of algebras. Recall that the unit of H^* is equal to the counit ε of H and that the product of two linear

forms α and β of H^* is given by

$$(\alpha\beta)(x) = \sum_{(x)} \alpha(x')\beta(x'')$$

for all $x \in H$. Then the relations $\varphi(1) = 1$ and $\varphi(uv) = \varphi(u)\varphi(v)$ imply $< 1, x > = \varphi(1)(x) = \varepsilon(x)$ and

$$\begin{aligned} < uv, x > &= \varphi(uv)(x) = (\varphi(u)\varphi(v))(x) \\ &= \sum_{(x)} \varphi(u)(x')\varphi(v)(x'') = \sum_{(x)} < u, x' >< v, x'' > . \end{aligned}$$

It results that Relations (7.1) and (7.3) of Definition 7.1 are equivalent to the fact that φ is a morphism of algebras. By symmetry, we see that Relations (7.2) and (7.4) are equivalent to the fact that ψ is a morphism of algebras.

Now assume that H is finite-dimensional. Then the dual space H^* is a bialgebra. We have already expressed the fact that φ is a morphism of algebras. Let us express that it is a morphism of coalgebras. On one hand, the relation $\varepsilon\varphi = \varepsilon$ expressing that φ preserves the counit reads

$$\varepsilon(u) = (\varepsilon\varphi)(u) = \varphi(u)(1) = < u, 1 > .$$

On the other hand, if φ preserves the comultiplication, we have

$$\begin{aligned} < u, xy > &= \varphi(u)(xy) = \Delta(\varphi(u))(x \otimes y) \\ &= \sum_{(u)} \varphi(u')(x)\varphi(u'')(y) \\ &= \sum_{(u)} < u', x >< u'', y > . \end{aligned}$$

Thus, the map φ is a morphism of coalgebras if and only if Relations (7.2) and (7.4) are satisfied. □

We return to the enveloping algebra $U = U(\mathfrak{sl}(2))$. We wish to set it in duality with the Hopf algebra $SL(2)$. Our first task is to construct a morphism of algebras ψ from the algebra $M(2) = k[a,b,c,d]$ (introduced in I.4) to the dual algebra U^*. We shall deduce a bilinear form on $U \times M(2)$ defined by $< u, x > = \psi(x)(u)$ and satisfying Relations (7.2) and (7.4). Now, building ψ is equivalent to giving four pairwise commuting elements A, B, C, D of U^*.

The definitions of A, B, C, and D use the simple U-module $V(1)$ with the basis $\{v_0, v_1\}$ described in Section 4. Given an element u in U, we set

$$\rho(u) = \begin{pmatrix} A(u) & B(u) \\ C(u) & D(u) \end{pmatrix}$$

where ρ is the representation $\rho(1)$ corresponding to $V(1)$. This defines four linear forms on U, hence four elements A, B, C, D of the dual space U^* U^*. The comultiplication of U being cocommutative, the dual algebra U^* is commutative. Therefore, the quadruple (A, B, C, D) defines a unique morphism of algebras $\psi : M(2) \to U^*$ such that

$$\psi(a) = A, \quad \psi(b) = B, \quad \psi(c) = C, \quad \psi(d) = D. \tag{7.6}$$

Proposition V.7.3. *The bilinear form $< u, x > = \psi(x)(u)$ realizes a duality between the bialgebras U and $M(2)$.*

PROOF. It remains to check Relations (7.1) and (7.3). We start with (7.3). The identity $\rho(1) = 1$ yields

$$\begin{pmatrix} <1,a> & <1,b> \\ <1,c> & <1,d> \end{pmatrix} = \begin{pmatrix} A(1) & B(1) \\ C(1) & D(1) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} \varepsilon(a) & \varepsilon(b) \\ \varepsilon(c) & \varepsilon(d) \end{pmatrix} \tag{7.7}$$

by definition of the counit in $M(2)$. Now, from Relation (7.2) we get

$$< 1, xy > = < 1, x >< 1, y > .$$

Both maps $x \mapsto < 1, x >$ and ε are morphisms of algebras and they coincide on the generators a, b, c, d of $M(2)$ by (7.7). Therefore, they have to be equal, which proves Relation (7.3).

We now turn to the proof of Relation (7.1). Let us denote by $C(x)$ the following condition on an element x of $M(2)$: For any pair (u, v) of elements of U, we have

$$< uv, x > = \sum_{(x)} < u, x' >< v, x'' > .$$

Let us first show that $C(1)$ is satisfied. Indeed, from (7.4) we get

$$< uv, 1 > = \varepsilon(uv) = \varepsilon(u)\varepsilon(v) = < u, 1 >< v, 1 > .$$

We next prove that Conditions $C(a), C(b), C(c), C(d)$ hold. By definition, we have

$$\rho(u) = \begin{pmatrix} A(u) & B(u) \\ C(u) & D(u) \end{pmatrix} = \begin{pmatrix} < u,a > & < u,b > \\ < u,c > & < u,d > \end{pmatrix}.$$

Let us express that $\rho(uv) = \rho(u)\rho(v)$. We have

$$\begin{pmatrix} < uv,a > & < uv,b > \\ < uv,c > & < uv,d > \end{pmatrix}$$
$$= \begin{pmatrix} < u,a > & < u,b > \\ < u,c > & < u,d > \end{pmatrix} \begin{pmatrix} < v,a > & < v,b > \\ < v,c > & < v,d > \end{pmatrix}. \tag{7.8}$$

Expanding this matrix product, we get exactly the four desired conditions since, as we know from Chapter I, the coproduct on $M(2)$ is defined by the matrix relation

$$\Delta \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

In order to conclude the proof of (7.1), we need to check Condition $C(x)$ for an arbitrary element x of $M(2)$. To this end, we first observe that if $C(x)$ and $C(y)$ are verified, then so is $C(\lambda x + y)$ for any scalar λ; second, we use the following lemma, which completes the proof of the proposition. □

Lemma V.7.4. *If Conditions $C(x)$ and $C(y)$ hold, then so does $C(xy)$.*

PROOF. Relation (7.2), and Conditions $C(x)$ and $C(y)$ imply that

$$\begin{aligned} < uv, xy > &= \sum_{(uv)} < (uv)', x >< (uv)'', y > \\ &= \sum_{(u)(v)} < u'v', x >< u''v'', y > \\ &= \sum_{(u)(v)(x)(y)} < u', x' >< v', x'' >< u'', y' >< v'', y'' > . \end{aligned}$$

They also yield

$$\begin{aligned} &\sum_{(xy)} < u, (xy)' >< v, (xy)'' > \\ &= \sum_{(x)(y)} < u, x'y' >< v, x''y'' > \\ &= \sum_{(u)(v)(x)(y)} < u', x' >< u'', y' >< v', x'' >< v'', y'' > \\ &= < uv, xy > . \end{aligned}$$

□

The duality between $M(2)$ and U is not perfect: the morphism ψ is not injective as the following lemma shows.

Lemma V.7.5. *We have $\psi(ad - bc) = 1$.*

Equivalently, $< u, ad - bc > = \varepsilon(u)$ for all elements u of U.

PROOF. Lemma I.5.2 as rephrased in (II.4.5) means that the element $ad - bc$ is grouplike. Consequently, by (7.1) we have

$$< uv, ad - bc > = < u, ad - bc >< v, ad - bc >$$

for any pair (u, v) of elements of U. On the other hand, by (7.3) we have

$$< 1, ad - bc > = \varepsilon(ad - bc) = 1.$$

This implies that the linear map $u \mapsto < u, ad - bc >$ is a morphism of algebras from U to k. To show that this morphism coincides with the counit ε, it suffices to check that both maps have the same values on the generators X, Y and H. Now we have

$$\begin{aligned} &< X, ad - bc > \\ &= \varepsilon(a) < X, d > + < X, a > \varepsilon(d) - \varepsilon(b) < X, c > - < X, b > \varepsilon(c) \\ &= 0 = \varepsilon(X). \end{aligned}$$

Similarly, we get $< Y, ad - bc > = 0 = \varepsilon(Y)$. Finally,

$$\begin{aligned} &< H, ad - bc > \\ &= \varepsilon(a) < H, d > + < H, a > \varepsilon(d) - \varepsilon(b) < H, c > - < H, b > \varepsilon(c) \\ &= -1 + 1 = 0 = \varepsilon(H). \end{aligned}$$

□

As a consequence of the previous lemma, the morphism of algebras $\psi : M(2) \to U^*$ factors through $SL(2) = M(2)/(ad - bc - 1)$. We still denote by ψ the induced morphism of algebras from $SL(2)$ to U^* and by $< \, , \, >$ the corresponding bilinear form.

Theorem V.7.6. *The bilinear form $< u, x > = \psi(x)(u)$ realizes a duality between the Hopf algebras U and $SL(2)$.*

PROOF. We already know that ψ is a morphism of algebras. By Proposition 7.2 we are left with showing that $\varphi : U \to SL(2)^*$ is a morphism of algebras too. Now, the projection from $M(2)$ onto $SL(2)$ dualizes to an injective morphism from $SL(2)^*$ into $M(2)^*$. It is clear that, when composing the latter with φ, we get the morphism of algebras $\varphi : U \to M(2)^*$ investigated earlier. Consequently, $\varphi : U \to SL(2)^*$ is a morphism of algebras. This shows that we have a duality between bialgebras.

It remains to examine the antipodes and to check Relation (7.5). Let us start with the generators. In the abridged matrix form we have

$$\begin{aligned} < S(X), \begin{pmatrix} a & b \\ c & d \end{pmatrix} > &= \rho(S(X)) = -\rho(X) \\ &= \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix} \\ &= < X, \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} > \\ &= < X, \begin{pmatrix} S(a) & S(b) \\ S(c) & S(d) \end{pmatrix} > . \end{aligned}$$

One proceeds similarly with Y, H, and 1.

For arbitrary elements of U and $SL(2)$, we use the following result. □

Lemma V.7.7. *Let u, v be elements of U. If*

$$< S(u), x > = < u, S(x) > \quad \textit{and} \quad < S(v), x > = < v, S(x) >$$

for all $x \in SL(2)$, then $< S(uv), x > = < uv, S(x) >$. Similarly, let x, y be elements of $SL(2)$. If

$$< S(u), x > = < u, S(x) > \quad \textit{and} \quad < S(u), y > = < u, S(y) >$$

for all $u \in U$, then $< S(u), xy > = < u, S(xy) >$.

PROOF. Theorem III.3.4 (a) and Definition 7.1 imply that

$$\begin{aligned} < S(uv), x > &= < S(v)S(u), x > \\ &= \sum_{(x)} < S(v), x' >< S(u), x'' > \\ &= \sum_{(x)} < u, S(x'') >< v, S(x') > \\ &= \sum_{(S(x))} < u, S(x)' >< v, S(x)'' > \\ &= < uv, S(x) > . \end{aligned}$$

The proof of the second assertion is similar. □

To the duality between U and $SL(2)$ corresponds a duality between U-modules and $SL(2)$-comodules. We now investigate this. In III.7 we showed that the vector space $k[x, y]_n$ of homogeneous polynomials of total degree n had a natural $SL(2)$-comodule structure. By duality, the dual vector space $k[x, y]_n^*$ has a module structure over the algebra $SL(2)^*$, hence over the algebra U via the morphism $\varphi : U \to SL(2)^*$. The following result gives the structure of $k[x, y]_n^*$ as a U-module.

Theorem V.7.8. *The U-module $k[x, y]_n^*$ is simple with highest weight n.*

In other words, the $SL(2)$-comodule $k[x, y]_n$ corresponds by duality to the U-module $V(n)$.

PROOF. We shall show that the linear form on $k[x, y]_n$ defined by

$$f(x^i y^{n-i}) = \delta_{ni}$$

is a highest weight vector with weight n of the U-module $k[x, y]_n^*$, which will imply that $k[x, y]_n^*$ contains a submodule isomorphic to the simple module $V(n)$. Since

$$\dim(V(n)) = n + 1 = \dim(k[x, y]_n^*),$$

we get $k[x, y]_n^* \cong V(n)$.

In order to prove that f is a highest weight vector, we need the identity

$$(uf)(x^i y^{n-i}) = < u, a^i c^{n-i} > \tag{7.9}$$

for all $u \in U$ and for all i such that $0 \leq i \leq n$. Indeed, by definition of f, by III.6, Example 2 and by Lemma III.7.4 we have

$$\begin{aligned}
&(uf)(x^i y^{n-i}) \\
&= (u \otimes f)(\Delta_A(x^i y^{n-i})) \\
&= \sum_{r=0}^{i}\sum_{s=0}^{n-i} \binom{i}{r}\binom{n-i}{s} < u, a^r b^{i-r} c^s d^{n-i-s} > f(x^{r+s} y^{n-r-s}) \\
&= \sum_{r=0}^{i}\sum_{s=0}^{n-i} \binom{i}{r}\binom{n-i}{s} < u, a^r b^{i-r} c^s d^{n-i-s} > \delta_{n,r+s} \\
&= \sum_{r=0}^{i}\sum_{s=0}^{n-i} \binom{i}{r}\binom{n-i}{s} < u, a^r b^{i-r} c^s d^{n-i-s} > \delta_{i,r}\delta_{n-i,s} \\
&= < u, a^i c^{n-i} > .
\end{aligned}$$

Let us apply Relation (7.9) to H. A straightforward computation using (7.2–7.3) and the definition of the bilinear form yields

$$< H, a^i c^j >= i\delta_{j0}.$$

Consequently, we have $(Hf)(x^i y^{n-i}) = n\delta_{ni}$, which implies that $Hf = nf$.
It remains to prove that $Xf = 0$. This is a consequence of Relation (7.9) applied to X and of the fact that $< X, a^i c^j >= 0$ for all i and j. Let us prove the latter. First, we have $< X, 1 >= \varepsilon(X) = 0$. Next, if $i > 0$, we have by (7.2–7.3)

$$\begin{aligned}
< X, a^i > &= \varepsilon(a) < X, a^{i-1} > + < X, a > \varepsilon(a^{i-1}) \\
&= < X, a^{i-1} > = \ldots = < X, a > = 0.
\end{aligned}$$

Similarly, if $j > 0$ we get

$$< X, c^j > = \varepsilon(c) < X, c^{j-1} > + < X, c > \varepsilon(c^{j-1}) = 0.$$

Consequently,

$$< X, a^i c^j > = \varepsilon(a)^i < X, c^j > + < X, a^i > \varepsilon(c^j) = 0.$$

□

V.8 Exercises

1. Let L be a Lie algebra. Show that $[L, L]$ is an ideal of L and that the quotient Lie algebra $L^{\mathrm{ab}} = L/[L, L]$ is abelian. Prove that if f is a morphism of Lie algebras from L to any abelian Lie algebra V, then there exists a unique linear map f^{ab} from L^{ab} into V such that f is the composition of f^{ab} and of the canonical projection from L onto L^{ab}.

2. For any Lie algebra L determine the group of grouplike elements of the Hopf algebra $U(L)$.

3. Let A be an algebra and $\mathrm{Der}(A)$ the vector space of all derivations of A. Show that the commutator of any two derivations is again a derivation and that $\mathrm{Der}(A)$ is a Lie subalgebra of $\mathfrak{gl}(A)$.

4. Show that any algebra A is a module-algebra over the enveloping algebra of the Lie algebra $\mathrm{Der}(A)$ and over the bialgebra $k[G]$ where G is the group of algebra automorphisms of A.

5. Let L be a Lie algebra and $\rho : L \to \mathfrak{gl}(V)$ a finite-dimensional representation of L. Define a symmetric bilinear form on L by

$$< x, y >_\rho = \mathrm{tr}(\rho(x)\rho(y))$$

where tr denotes the trace of endomorphisms.

(a) Prove that this form is invariant, i.e., we have

$$< [x, y], z >_\rho = < x, [y, z] >_\rho$$

for all $x, y, z \in L$.

(b) Let $\{x_i\}_{1 \leq i \leq d}$ be a basis of L. Assume the form $< \, , \, >_\rho$ non-degenerate. Define a new basis $\{x^i\}_{1 \leq i \leq d}$ of L by requiring that $< x_i, x^j >_\rho = \delta_{ij}$. We get an element $C_\rho = \sum_{1 \leq i \leq d} x_i x^i$ of $U(L)$. Show that C_ρ belongs to the centre of the enveloping algebra and that $\mathrm{tr}(\rho(C_\rho)) = d = \dim(L)$.

(c) (*Whitehead Lemma*) Let $f : L \to V$ be a linear map satisfying the relation

$$f([x, y]) = xf(y) - yf(x)$$

for all $x, y \in L$. Assume that the form $< \, , \, >_\rho$ is non-degenerate and that C_ρ is well-defined. Show that we have

$$C_\rho f(x) = x\Big(\sum_{1 \leq i \leq d} x_i f(x^i)\Big).$$

Deduce that, when $\rho(C_\rho)$ is invertible, there exists a vector v in V such that $f(x) = xv$ for all x in L.

6. Find all invariant symmetric bilinear forms of $\mathfrak{sl}(2)$ (as defined in the previous exercise; assume that the field k is of characteristic zero).

7. Show that the enveloping algebra $U(\mathfrak{sl}(2))$ is Noetherian and has no divisors of zero. Find its centre (Hint: proceed by analogy with VI.4).

8. Assume that k is a field of characteristic zero. Show that the Lie algebra $\mathfrak{sl}(2)$ has no ideals but $\{0\}$ and the algebra itself. Deduce that $\mathfrak{sl}(2) = [\mathfrak{sl}(2), \mathfrak{sl}(2)]$.

9. Show that the dual of the U-module $V(n)$ is isomorphic to $V(n)$.

10. Determine all Hopf algebra automorphisms of $U(\mathfrak{sl}(2))$.

11. Check that there is an antiautomorphism T of algebras of $U(\mathfrak{sl}(2))$ such that $T(X) = Y$, $T(Y) = X$, and $T(H) = H$. Prove that T is a morphism of coalgebras. Find all non-degenerate symmetric bilinear forms $(\, , \,)$ on the simple module $V(n)$ such that $(xv, v') = (v, T(x)v')$ for all $x \in U(\mathfrak{sl}(2))$ and $v, v' \in V(n)$. Show that the basis of $V(n)$ consisting of the vectors $v_0, \ldots, v_n$ (defined in Section 4) is orthogonal for such a form.

12. (*Bialgebra structure on the quantum plane*) (a) Show that the formulas

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

equip the free algebra $k\{x, y\}$ and the quantum plane $k_q[x, y]$ with a bialgebra structure.

(b) Prove that an algebra R is a module-algebra over the bialgebra $k\{x, y\}$ [resp. over $k_q[x, y]$] if and only if R possesses an algebra endomorphism τ and a τ-derivation δ [resp. τ and δ such that the relation $\delta\tau = q\tau\delta$ holds].

(c) Find all $k_q[x, y]$-algebra structures on the polynomial algebra $k[z]$ (consider only the ones for which τ is an automorphism). In particular, show that, when τ is the algebra automorphism τ_q of $k[z]$ considered in IV.2, then δ is necessarily a scalar multiple of δ_q (see Exercise 4 in Chapter IV).

13. Show that any antilinear involution $*$ on a complex Lie algebra L such that $[x, y]^* = [y^*, x^*]$ for all $x, y \in L$ induces a Hopf $*$-algebra structure on $U(L)$.

14. Prove that there exists a unique Hopf $*$-algebra structure on $U(\mathfrak{sl}(2))$ such that $X^* = Y$, $Y^* = X$, and $H^* = -H$.

15. Find all Hopf $*$-algebra structures on $U(\mathfrak{sl}(2))$ up to equivalence, assuming that the ground field is the field of complex numbers.

V.9 Notes

There exist numerous textbooks on the theory of Lie algebras. See, for instance, [Bou60][Dix74][Hum72][Jac79][Ser65][Var74]. The content of this chapter is essentially taken from these sources. We found the proof of Theorem 4.6 in Serre's book [Ser65]. As for Definition 7.1, we took it from [Tak81]. Let us supplement the content of this chapter with the following remarks.

(*Free Lie algebras*) Let X be a set. Consider the smallest Lie subalgebra $\mathcal{L}(X)$ of the free algebra $k\{X\}$ containing X. Denote by i_X the injection of X into $\mathcal{L}(X)$. The free Lie algebra $\mathcal{L}(X)$ enjoys the following universal property: For any set-theoretic map f from X into a Lie algebra L, there exists a unique morphism of Lie algebras $\bar{f} : \mathcal{L}(X) \to L$ such that $f = \bar{f} \circ i_X$. It follows from this universal property, from Proposition I.2.1, and from Theorem 2.1 that there is an isomorphism of algebras

$$U(\mathcal{L}(X)) \cong k\{X\}.$$

A description of bases for $\mathcal{L}(X)$ may be found in [Bou60], Chap. 2. See also [Reu93].

(*Primitive elements of the enveloping bialgebra*) Any Lie algebra L is contained in the Lie algebra of primitive elements of its enveloping algebra. In characteristic zero, this embedding is an equality:

$$L = \mathrm{Prim}(U(L)).$$

When applied to free algebras, one gets $\mathcal{L}(X) \cong \mathrm{Prim}(k\{X\})$ (see [Bou60], Chap. 2).

(*Real forms*) A real form of a complex Lie algebra L is a real Lie subalgebra $L_{\mathbf{R}}$ of L such that the embedding of the complexification $L_{\mathbf{R}} \oplus iL_{\mathbf{R}}$ into L is an isomorphism of complex Lie algebras. Here i denotes a square root of -1. To any real form of L, one associates its conjugation, which is the antilinear involutive endomorphism of Lie algebras σ given by

$$\sigma(x + iy) = x - iy$$

for all $x, y \in L_{\mathbf{R}}$. Conversely, given any such involution of L, we obtain a real form by

$$L_{\mathbf{R}} = \{x \in L \mid \sigma(x) = x\}.$$

For any real form of L with conjugation σ, we define a Hopf $*$-algebra structure on the enveloping algebra $U(L)$ by $* = S \circ U(\sigma)$. In other words, we have $1^* = 1$ and

$$(x_1 \ldots x_n)^* = (-1)^n \sigma(x_n) \ldots \sigma(x_1)$$

for all $x_1, \ldots, x_n \in L$. Conversely, suppose we have a Hopf $*$-algebra structure on the enveloping algebra $U(L)$. Since $*$ is a coalgebra morphism, it preserves the Lie subalgebra of primitive elements, which is L (we are in characteristic zero). It is easy to check that the subspace of all elements x of L such that $x = -x^*$ is a real form of L. We thus see that the real forms on a complex Lie algebra L are in one-to-one correspondence with the Hopf $*$-algebra structures on $U(L)$.

For instance, the real Lie subalgebra $\mathfrak{su}(2)$ of 2×2-matrices M in $\mathfrak{sl}(2)$ such that $M = -{}^t\overline{M}$ is a real form of $\mathfrak{sl}(2)$. The vectors $A = \frac{1}{2}(X - Y)$, $B = \frac{i}{2}(X + Y)$, iH form a real basis of $\mathfrak{su}(2)$ such that

$$[A, B] = C, \quad [B, C] = A, \quad [C, A] = B.$$

This proves that $\mathfrak{su}(2)$ is isomorphic to the Lie algebra $\mathfrak{so}(3)$ of real antisymmetric 3×3-matrices.

(*Duality*) Theorem 7.6 asserts the existence of a Hopf algebra morphism from $SL(2)$ to $U(\mathfrak{sl}(2))^*$. This morphism is actually an isomorphism from $SL(2)$ to the restricted dual $U(\mathfrak{sl}(2))^o$. This holds, more generally, for any simply-connected algebraic group in characteristic zero (see [Abe80] [Hoc81] [JS91b] [Swe69]).

Chapter VI

The Quantum Enveloping Algebra of $\mathfrak{sl}(2)$

The aim of Chapters VI–VII is to construct a Hopf algebra $U_q = U_q(\mathfrak{sl}(2))$ which is a one-parameter deformation of the enveloping algebra of the Lie algebra $\mathfrak{sl}(2)$ investigated in Chapter V, and which is in duality with the Hopf algebra $SL_q(2)$ defined in Chapter IV. It will be our second main example of a quantum group. When the parameter q is not a root of unity, the algebra U_q has properties parallel to those of the enveloping algebra of $\mathfrak{sl}(2)$. In the present chapter we classify the simple finite-dimensional modules of U_q and determine its centre. We close the chapter with a few considerations on the case when q is a root of unity.

We assume throughout this chapter that the ground field k is the field of complex numbers.

VI.1 The Algebra $U_q(\mathfrak{sl}(2))$

Let us fix an invertible element q of k different from 1 and -1 so that the fraction $\frac{1}{q-q^{-1}}$ is well-defined. We introduce some notation.

For any integer n, set

$$[n] = \frac{q^n - q^{-n}}{q - q^{-1}} = q^{n-1} + q^{n-3} + \cdots + q^{-n+3} + q^{-n+1}. \tag{1.1}$$

These q-analogues are more symmetric than the ones defined in IV.2, as shown by the relations

$$[-n] = -[n] \quad \text{and} \quad [m + n] = q^n[m] + q^{-m}[n]. \tag{1.2}$$

Observe that, if q is not a root of unity, then $[n] \neq 0$ for any non-zero integer. This is not so when q is a root of unity. In that case, denote by d its order, i.e., the smallest integer > 1 such that $q^d = 1$. Since we assume $q^2 \neq 1$, we must have $d > 2$. Define also

$$e = \begin{cases} d & \text{if } d \text{ is odd} \\ d/2 & \text{when } d \text{ is even.} \end{cases} \tag{1.3}$$

Let us agree that $d = e = \infty$ when q is not a root of unity. Now it is easy to check that

$$[n] = 0 \Longleftrightarrow n \equiv 0 \text{ modulo } e. \tag{1.4}$$

We also have the following versions of factorials and binomial coefficients. For integers $0 \leq k \leq n$, set $[0]! = 1$,

$$[k]! = [1][2]\dots[k] \tag{1.5}$$

if $k > 0$, and

$$\left[\begin{array}{c} n \\ k \end{array} \right] = \frac{[n]!}{[k]![n-k]!}. \tag{1.6}$$

These q-analogues are related to those of IV.2 by

$$[n] = q^{-(n-1)}\,(n)_{q^2}, \quad [n]! = q^{-n(n-1)/2}(n)!_{q^2}, \tag{1.7}$$

and

$$\left[\begin{array}{c} n \\ k \end{array} \right] = q^{-k(n-k)} \left(\begin{array}{c} n \\ k \end{array} \right)_{q^2}. \tag{1.8}$$

With this new notation we can rewrite Proposition IV.2.2 as follows. If x and y are variables subject to the relation $yx = q^2xy$, then we have $(n > 0)$

$$(x+y)^n = \sum_{k=0}^{n} q^{k(n-k)} \left[\begin{array}{c} n \\ k \end{array} \right] x^k y^{n-k}. \tag{1.9}$$

Definition VI.1.1. *We define $U_q = U_q(\mathfrak{sl}(2))$ as the algebra generated by the four variables E, F, K, K^{-1} with the relations*

$$KK^{-1} = K^{-1}K = 1, \tag{1.10}$$

$$KEK^{-1} = q^2E, \quad KFK^{-1} = q^{-2}F, \tag{1.11}$$

and

$$[E,F] = \frac{K - K^{-1}}{q - q^{-1}}. \tag{1.12}$$

The rest of the section is devoted to a few elementary properties of U_q. The following lemma has an easy proof left to the reader.

Lemma VI.1.2. *There is a unique algebra automorphism of U_q such that*

$$\omega(E) = F, \quad \omega(F) = E, \quad \omega(K) = K^{-1}.$$

The automorphism ω is sometimes called the *Cartan automorphism.* We now state a q-analogue of Lemma V.3.1.

Lemma VI.1.3. *Let $m \geq 0$ and $n \in \mathbf{Z}$. The following relations hold in U_q:*

$$E^mK^n = q^{-2mn}\,K^nE^m, \quad F^mK^n = q^{2mn}\,K^nF^m,$$

$$\begin{aligned} [E,F^m] &= [m]\,F^{m-1}\frac{q^{-(m-1)}K - q^{m-1}K^{-1}}{q-q^{-1}} \\ &= [m]\,\frac{q^{m-1}K - q^{-(m-1)}K^{-1}}{q-q^{-1}}F^{m-1}, \end{aligned}$$

$$\begin{aligned} [E^m,F] &= [m]\,\frac{q^{-(m-1)}K - q^{m-1}K^{-1}}{q-q^{-1}}E^{m-1} \\ &= [m]\,E^{m-1}\frac{q^{m-1}K - q^{-(m-1)}K^{-1}}{q-q^{-1}}. \end{aligned}$$

PROOF. The first two relations result trivially from Relations (1.11). The third one is proved by induction on m using

$$[E,F^m] = [E,F^{m-1}]F + F^{m-1}[E,F] = [E,F^{m-1}]F + F^{m-1}\frac{K-K^{-1}}{q-q^{-1}}$$

as in the proof of Lemma V.3.1. Applying the automorphism ω to the third relation, one gets the fourth one. □

We now describe a basis of U_q by showing that U_q is an iterated Ore extension. We refer to I.7–8 for information concerning Ore extensions.

Proposition VI.1.4. *The algebra U_q is Noetherian and has no zero divisors. The set $\{E^iF^jK^\ell\}_{i,j\in\mathbf{N};\,\ell\in\mathbf{Z}}$ is a basis of U_q.*

PROOF. Define $A_0 = k[K,K^{-1}]$. We shall construct two Ore extensions $A_1 \subset A_2$ such that A_2 is isomorphic to U_q. First, observe that the algebra A_0 has no zero divisors and is Noetherian as a quotient of a (Noetherian) two-variable polynomial algebra. The family $\{K^\ell\}_{\ell\in\mathbf{Z}}$ is a basis of A_0.

Consider the automorphism α_1 of A_0 determined by $\alpha_1(K) = q^2K$ and the corresponding Ore extension $A_1 = A_0[F,\alpha_1,0]$: the latter has a basis consisting of the monomials $\{F^jK^\ell\}_{j\in\mathbf{N},\,\ell\in\mathbf{Z}}$. An argument analogous to the one used to prove Lemma IV.4.2 shows that A_1 is the algebra generated by F, K, K^{-1} and the relation $FK = q^2KF$.

We now build an Ore extension $A_2 = A_1[E, \alpha_1, \delta]$ from an automorphism α_1 and an α_1-derivation of A_1. The automorphism α_1 is defined by

$$\alpha_1(F^j K^\ell) = q^{-2\ell} F^j K^\ell. \tag{1.13}$$

Let us take as given for a moment that there exists an α_1-derivation δ such that

$$\delta(F) = \frac{K - K^{-1}}{q - q^{-1}} \quad \text{and} \quad \delta(K) = 0.$$

Then the following relations hold in A_2:

$$EK = \alpha_1(K)E + \delta(K) = q^{-2}KE$$

and

$$EF = \alpha_1(F)E + \delta(F) = FE + \frac{K - K^{-1}}{q - q^{-1}}.$$

From these one easily concludes that A_2 is isomorphic to U_q. It then results from Corollary I.7.2 and from Theorem I.8.3 that U_q has the required properties. □

It remains to prove the following technical lemma in order to complete the proof of Proposition 1.4.

Lemma VI.1.5. *Denote by $\delta(F)(K)$ the Laurent polynomial $\frac{K-K^{-1}}{q-q^{-1}}$, and set $\delta(K^\ell) = 0$ and*

$$\delta(F^j K^\ell) = \sum_{i=0}^{j-1} F^{j-1}\delta(F)(q^{-2i}K)K^\ell \tag{1.14}$$

when $j > 0$. Then δ extends to an α_1-derivation of A_1.

PROOF. We must check that, for all $j, m \in \mathbf{N}$ and all $\ell, n \in \mathbf{Z}$, we have

$$\delta(F^j K^\ell \cdot F^m K^n) = \alpha_1(F^j K^\ell)\delta(F^m K^n) + \delta(F^j K^\ell)F^m K^n. \tag{1.15}$$

Let us compute the right-hand side of (1.15) using (1.11), (1.13), and (1.14). We have

$$\begin{aligned}
&\alpha_1(F^j K^\ell)\delta(F^m K^n) + \delta(F^j K^\ell)F^m K^n \\
&= \sum_{i=0}^{m-1} q^{-2\ell}\, F^j K^\ell F^{m-1}\delta(F)(q^{-2i}K)K^n \\
&\qquad + \sum_{i=0}^{j-1} F^{j-1}\delta(F)(q^{-2i}K)K^\ell F^m K^n \\
&= \sum_{i=0}^{m-1} q^{-2\ell-2\ell(m-1)}\, F^{j+m-1}\delta(F)(q^{-2i}K)K^{\ell+n} \\
&\qquad + \sum_{i=0}^{j-1} q^{-2\ell m}\, F^{m+j-1}\delta(F)(q^{-2i-2m}K)K^{\ell+n} \\
&= \sum_{i=0}^{m-1} q^{-2\ell m}\, F^{m+j-1}\delta(F)(q^{-2i}K)K^{\ell+n} \\
&\qquad + \sum_{i=m}^{j+m-1} q^{-2\ell m}\, F^{m+j-1}\delta(F)(q^{-2i}K)K^{\ell+n} \\
&= q^{-2\ell m}\left(\sum_{i=0}^{j+m-1} F^{j+m-1}\delta(F)(q^{-2i}K)K^{\ell+n}\right) \\
&= q^{-2\ell m}\delta(F^{j+m}K^{\ell+n}) \\
&= \delta(F^j K^\ell \cdot F^m K^n).
\end{aligned}$$

□

VI.2 Relationship with the Enveloping Algebra of $\mathfrak{sl}(2)$

One expects to recover $U = U(\mathfrak{sl}(2))$ from U_q by setting $q = 1$. This is impossible with Definition 1.1. So we first have to give another presentation for U_q.

Proposition VI.2.1. *The algebra U_q is isomorphic to the algebra U'_q generated by the five variables E, F, K, K^{-1}, L and the relations*

$$KK^{-1} = K^{-1}K = 1, \tag{2.1}$$

$$KEK^{-1} = q^2E, \quad KFK^{-1} = q^{-2}F, \tag{2.2}$$

$$[E, F] = L, \quad (q - q^{-1})L = K - K^{-1}, \tag{2.3}$$

$$[L, E] = q(EK + K^{-1}E), \quad [L, F] = -q^{-1}(FK + K^{-1}F). \tag{2.4}$$

Observe that, contrary to U_q, the algebra U'_q is defined for all values of the parameter q, in particular for $q = 1$. In some sense, it would have been better to proceed through the whole theory of the quantum enveloping algebra of $\mathfrak{sl}(2)$ with U'_q rather than with U_q, but the simpler presentation given in Section 1 is sufficient for our purposes.

PROOF. Set

$$\varphi(E) = E, \quad \varphi(F) = F, \quad \varphi(K) = K$$

and

$$\psi(E) = E, \quad \psi(F) = F, \quad \psi(K) = K, \quad \psi(L) = [E, F].$$

It is clear that φ gives rise to a well-defined morphism of algebras from U_q to U'_q. Let us show that $\psi : U'_q \to U_q$ is well-defined too. It suffices to check that the images under ψ of the defining Relations (2.1) hold in the algebra U_q. This is clearly true for Relations (2.1–2.2) and for $[E, F] = L$. For the remaining relation in (2.3) we have

$$(q - q^{-1})\psi(L) = (q - q^{-1})[E, F] = K - K^{-1}.$$

For the first relation in (2.4) we get

$$\begin{aligned}[\psi(L), \psi(E)] = [[E, F], E] &= \frac{1}{q - q^{-1}}[K - K^{-1}, E] \\ &= \frac{(q^2 - 1)EK + (q^2 - 1)K^{-1}E}{q - q^{-1}} \\ &= q\,(EK + K^{-1}E).\end{aligned}$$

One derives the last relation in a similar fashion.

The reader may now verify that φ and ψ are reciprocal algebra morphisms by checking the necessary relations on the generators. □

The relationship with the enveloping algebra U is given in the following statement.

Proposition VI.2.2. *If $q = 1$, we have*

$$U'_1 \cong U[K]/(K^2 - 1) \quad \textit{and} \quad U \cong U'_1/(K - 1).$$

PROOF. It suffices to prove the first isomorphism. Now U'_1 has the following presentation: it is generated by E, F, K, K^{-1}, L and Relations (2.1–2.4) in which q has been replaced by 1, namely

$$KK^{-1} = K^{-1}K = 1, \tag{2.5}$$

$$KEK^{-1} = E, \quad KFK^{-1} = F, \tag{2.6}$$

$$[E, F] = L, \quad K - K^{-1} = 0, \tag{2.7}$$

$$[L, E] = (EK + K^{-1}E), \quad [L, F] = -(FK + K^{-1}F). \tag{2.8}$$

Relations (2.5–2.6) imply that K is central. Relation (2.7) yields $K^2 = 1$, which allows one to rewrite the Relations (2.8) as

$$[L, E] = 2EK, \quad [L, F] = -2FK. \tag{2.9}$$

We then get an isomorphism from U'_1 to $U[K]/(K^2 - 1)$ by sending E to XK, F to Y, K to K, and L to HK. □

In particular, the projection of U'_1 onto U is obtained by sending E to X, F to Y, K to 1, and L to H. One may use this projection to rederive certain relations in U (for instance, Lemma V.3.1) from their q-analogues in U'_q.

VI.3 Representations of U_q

We assume in this section that the complex parameter q is not a root of unity. Our aim is to determine all finite-dimensional simple U_q-modules under this assumption by closely following the methods of Section V.4.

For any U_q-module V and any scalar $\lambda \neq 0$, we denote by V^λ the subspace of all vectors v in V such that $Kv = \lambda v$. The scalar λ is called a *weight* of V if $V^\lambda \neq \{0\}$.

Lemma VI.3.1. *We have $EV^\lambda \subset V^{q^2\lambda}$ and $FV^\lambda \subset V^{q^{-2}\lambda}$.*

PROOF. For $v \in V^\lambda$ we have

$$K(Ev) = q^2E(Kv) = q^2\lambda Ev \quad \text{and} \quad K(Fv) = q^{-2}F(Kv) = q^{-2}\lambda Fv.$$

□

Definition VI.3.2. *Let V be a U_q-module and λ be a scalar. An element $v \neq 0$ of V is a highest weight vector of weight λ if $Ev = 0$ and if $Kv = \lambda v$. A U_q-module is a highest weight module of highest weight λ if it is generated by a highest weight vector of weight λ.*

Proposition VI.3.3. *Any non-zero finite-dimensional U_q-module V contains a highest weight vector. Moreover, the endomorphisms induced by E and F on V are nilpotent.*

PROOF. Since $k = \mathbf{C}$ is algebraically closed and V is finite-dimensional, there exists a non-zero vector w and a scalar α such that $Kw = \alpha w$. If $Ew = 0$, the vector w is a highest weight vector and we are done. If not, let us consider the sequence of vectors $E^n w$ where n runs over the non-negative integers. According to Lemma 3.1, it is a sequence of eigenvectors with distinct eigenvalues; consequently, there exists an integer n such that $E^n w \neq 0$ and $E^{n+1}w = 0$. The vector $E^n w$ is a highest weight vector.

In order to show that the action of E on V is nilpotent, it suffices to check that 0 is the only possible eigenvalue of E. Now, if v is a non-zero eigenvector for E with eigenvalue $\lambda \neq 0$, then so is $K^n v$ with eigenvalue $q^{-2n}\lambda$. The endomorphism E would then have infinitely many distinct eigenvalues, which is impossible. The same argument works for F. □

Lemma VI.3.4. *Let v be a highest weight vector of weight λ. Set $v_0 = v$ and $v_p = \frac{1}{[p]!}F^p v$ for $p > 0$. Then*

$$Kv_p = \lambda q^{-2p}\, v_p, \quad Ev_p = \frac{q^{-(p-1)}\lambda - q^{p-1}\lambda^{-1}}{q - q^{-1}}\, v_{p-1}, \quad Fv_{p-1} = [p]\, v_p.$$

PROOF. These relations result from Lemma 1.3. □

We now determine all finite-dimensional simple U_q-modules.

Theorem VI.3.5. (a) *Let V be a finite-dimensional U_q-module generated by a highest weight vector v of weight λ. Then*

(i) *The scalar λ is of the form $\lambda = \varepsilon q^n$ where $\varepsilon = \pm 1$ and n is the integer defined by $\dim(V) = n+1$.*

(ii) *Setting $v_p = F^p v/[p]!$, we have $v_p = 0$ for $p > n$ and, in addition, the set $\{v = v_0, v_1, \dots, v_n\}$ is a basis of V.*

(iii) *The operator K acting on V is diagonalizable with the $(n+1)$ distinct eigenvalues $\{\varepsilon q^n, \varepsilon q^{n-2}, \dots, \varepsilon q^{-n+2}, \varepsilon q^{-n}\}$.*

(iv) *Any other highest weight vector in V is a scalar multiple of v and is of weight λ.*

(v) *The module V is simple.*

(b) *Any simple finite-dimensional U_q-module is generated by a highest weight vector. Two finite-dimensional U-modules generated by highest weight vectors of the same weight are isomorphic.*

PROOF. (a) According to Lemma 3.4, the sequence $\{v_p\}_{p\geq 0}$ is a sequence of eigenvectors for K with distinct eigenvalues. Since V is finite-dimensional, there has to exist an integer n such that $v_n \neq 0$ and $v_{n+1} = 0$. The formulas of Lemma 3.4 then show that $v_m = 0$ for all $m > n$ and $v_m \neq 0$ for all $m \leq n$. By Lemma 3.4, we also have

$$0 = Ev_{n+1} = \frac{q^{-n}\lambda - q^n\lambda^{-1}}{q - q^{-1}} v_n.$$

Hence, $q^{-n}\lambda = q^n\lambda^{-1}$, which is equivalent to $\lambda = \pm q^n$. The rest of the proof of (i)–(iii) is as in the classical case (see Theorem V.4.4).

(iv) Let v' be another highest weight vector. It is an eigenvector for the action of K; hence, it is a scalar multiple of some vector v_i. But, again by Lemma 3.4, the vector v_i is killed by E if and only $i = 0$.

(v) Let V' be a non-zero U_q-submodule of V and let v' be a highest weight vector of V'. Then v' also is a highest weight vector for V. By (iv), v' has to be a non-zero scalar multiple of v. Therefore v is in V'. Since v generates V, we must have $V \subset V'$, which proves that V is simple.

(b) The proof is the same as for Theorem V.4.4 (b). □

Theorem 3.5 implies that, up to isomorphism, there exists a unique simple U_q-module of dimension $n+1$ and generated by a highest weight vector of weight εq^n. We denote this module by $V_{\varepsilon,n}$ and the corresponding morphism of algebras $U_q \to \mathrm{End}(V_{\varepsilon,n})$ by $\rho_{\varepsilon,n}$. Observe that the formulas of Lemma 3.4 may be rewritten as follows for $V_{\varepsilon,n}$:

$$Kv_p = \varepsilon\, q^{n-2p}\, v_p, \tag{3.1}$$

$$Ev_p = \varepsilon\, [n-p+1]\, v_{p-1}, \tag{3.2}$$

and

$$Fv_{p-1} = [p]\, v_p. \tag{3.3}$$

As a special case, we have $V_{\varepsilon,0} = k$. The morphism $\rho_{\varepsilon,0}$ is given by

$$\rho_{\varepsilon,0}(K) = \varepsilon, \quad \rho_{\varepsilon,0}(E) = \rho_{\varepsilon,0}(F) = 0.$$

We shall see in VII.1 that $\rho_{\varepsilon,0}$ may be identified with the counit of a Hopf algebra structure on U_q. It will imply that the module $V_{1,0}$ is trivial and that any trivial U_q-module is isomorphic to a direct sum of copies of $V_{1,0}$. On the other hand, the module $V_{-1,0}$ is not trivial.

On the $(n+1)$-dimensional module $V_{\varepsilon,n}$, the generators E, F and K act by operators that can be represented on the basis $\{v_0, v_1, \dots, v_n\}$ by the matrices

$$\rho_{\varepsilon,n}(E) = \varepsilon \begin{pmatrix} 0 & [n] & 0 & \cdots & 0 \\ 0 & 0 & [n-1] & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & \ddots & 1 \\ 0 & 0 & \cdots & 0 & 0 \end{pmatrix},$$

$$\rho_{\varepsilon,n}(F) = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & [2] & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & [n] & 0 \end{pmatrix},$$

and

$$\rho_{\varepsilon,n}(K) = \varepsilon \begin{pmatrix} q^n & 0 & \cdots & 0 & 0 \\ 0 & q^{n-2} & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & q^{-n+2} & 0 \\ 0 & 0 & \cdots & 0 & q^{-n} \end{pmatrix}.$$

So far, we have built U_q-modules generated by highest weight vectors whose weights λ had special values. Let us now show that there exist highest weight modules with arbitrary highest weights.

Let us fix a scalar $\lambda \neq 0$. Consider an infinite-dimensional vector space $V(\lambda)$ with denumerable basis $\{v_i\}_{i\in\mathbf{N}}$. For $p \geq 0$, set

$$Kv_p = \lambda q^{-2p}\, v_p, \quad K^{-1}v_p = \lambda^{-1} q^{2p}\, v_p, \tag{3.4}$$

$$Ev_{p+1} = \frac{q^{-p}\lambda - q^p\lambda^{-1}}{q - q^{-1}}\, v_p, \quad Fv_p = [p+1]\, v_{p+1} \tag{3.5}$$

and $Ev_0 = 0$.

Lemma VI.3.6. *Relations (3.4–3.5) define a U_q-module structure on $V(\lambda)$. The element v_0 generates $V(\lambda)$ as a U_q-module and is a highest weight vector of weight λ.*

PROOF. Immediate computations yield

$$\begin{aligned} KK^{-1}v_p &= v_p, & K^{-1}Kv_p &= v_p \\ KEK^{-1}v_p &= q^2Ev_p, & KFK^{-1}v_p &= q^{-2}Fv_p. \end{aligned}$$

We also have

$$\begin{aligned} [E,F]v_p &= \left([p+1]\,\frac{q^{-p}\lambda - q^p\lambda^{-1}}{q-q^{-1}} - [p]\,\frac{q^{-(p-1)}\lambda - q^{p-1}\lambda^{-1}}{q-q^{-1}}\right) v_p \\ &= \frac{q^{-2p}\lambda - q^{2p}\lambda^{-1}}{q-q^{-1}}\, v_p \\ &= \frac{K-K^{-1}}{q-q^{-1}} v_p. \end{aligned}$$

This proves that Relations (3.4–3.5) define a U_q-module structure on $V(\lambda)$.
Next, we have $Kv_0 = \lambda\, v_0$ and $Ev_0 = 0$, which means that v_0 is a highest weight vector of weight λ. Finally, (3.5) implies that $v_p = F^p v_0/[p]!$ for all p, which proves that $V(\lambda)$ is generated by v_0. □

By analogy with the classical case, the highest weight U_q-module $V(\lambda)$ is called the *Verma module* of highest weight λ. It enjoys the following universal property.

Proposition VI.3.7. *Any highest weight U_q-module V of highest weight λ is a quotient of the Verma module $V(\lambda)$.*

PROOF. Let v be a highest weight vector generating V. We define a linear map f from $V(\lambda)$ to V by $f(v_p) = 1/[p]!\,F^p v$. Lemma 3.4 implies that f is U_q-linear. Since $f(v_0) = v$ generates V, the map f is surjective. □

In particular, the simple finite-dimensional module $V_{\varepsilon,n}$ described above is a quotient of the Verma module $V(\varepsilon q^n)$. As a consequence, the module $V(\lambda)$ cannot be simple when λ is of the form $\pm q^n$ where n is a nonnegative integer.

VI.4 The Harish-Chandra Homomorphism and the Centre of U_q

Our next objective is to describe the centre Z_q of U_q in case q is not a root of unity. We assume this throughout this section.
We start by introducing a special central element of U_q. It is sometimes called the *quantum Casimir element.*

Proposition VI.4.1. *The element*

$$C_q = EF + \frac{q^{-1}K + qK^{-1}}{(q-q^{-1})^2} = FE + \frac{qK + q^{-1}K^{-1}}{(q-q^{-1})^2}$$

belongs to the centre of U_q.

PROOF. It suffices to check that C_q commutes with the generators K, E, F. The commutation with K is clear from $KEFK^{-1} = EF$. As for E, we have

$$EC_q = EFE + E\frac{qK + q^{-1}K^{-1}}{(q-q^{-1})^2} = EFE + \frac{q^{-1}K + qK^{-1}}{(q-q^{-1})^2}E = C_qE.$$

Similar argument gives the result for F. □

Let U_q^K be the subalgebra of U_q of all elements commuting with K.

Lemma VI.4.2. *An element of U_q belongs to U_q^K if and only if it is of the form*

$$\sum_{i\geq 0} F^i P_i E^i \tag{4.1}$$

where $P_0, P_1, \dots$ are elements of $k[K,K^{-1}]$.

PROOF. This is a consequence of the fact that $\{F^iK^\ell E^j\}_{i,j\in\mathbf{N};\,\ell\in\mathbf{Z}}$ is a basis of U_q and that $K(F^iK^\ell E^j)K^{-1} = q^{2(j-i)}\,F^iK^\ell E^j$. □

Let us consider the left ideal $I = U_qE \cap U_q^K$ of U_q^K.

Lemma VI.4.3. *We have $I = FU_q \cap U_q^K$ and $U_q^K = k[K,K^{-1}] \oplus I$.*

PROOF. Let $u = \sum_{i\geq 0} F^iP_iE^i$ be an element of U_q^K. If u also lies in U_qE, then $P_0 = 0$. Hence, u belongs to $FU_q \cap U_q^K$ and conversely. Since the form (4.1) is unique for any element of U_q^K, we get the desired direct sum. □

It results from $I = FU_q \cap U_q^K$ that I is a two-sided ideal and that the projection φ from U_q^K onto $k[K,K^{-1}]$ is a morphism of algebras. The map φ is called the *Harish-Chandra homomorphism.* It permits one to express the action of the centre Z_q on a highest weight module.

Proposition VI.4.4. *Let V be a highest weight U_q-module with highest weight λ. Then, for any central element z of U_q and any $v \in V$, we have*

$$zv = \varphi(z)(\lambda)v.$$

Recall that $\varphi(z)$ is a Laurent polynomial in K and that $\varphi(z)(\lambda)$ is its value at λ.

PROOF. Let v_0 be a highest weight vector generating V and z a central element of U_q. The element z can be written in the form

$$z = \varphi(z) + \sum_{i>0} F^i P_i E^i.$$

Since $Ev_0 = 0$ and $Kv_0 = \lambda v_0$, we get $zv_0 = \varphi(z)(\lambda)v_0$. If v is an arbitrary element of V, we have $v = xv_0$ for some x in U_q; hence,

$$zv = zxv_0 = xzv_0 = \varphi(z)(\lambda)xv_0 = \varphi(z)(\lambda)v.$$

□

Example 1. The definition of the central element C_q shows that

$$\varphi(C_q) = \frac{qK - q^{-1}K^{-1}}{(q-q^{-1})^2}. \tag{4.2}$$

Consequently, C_q acts on a highest weight module of highest weight λ as the multiplication by the scalar

$$\frac{q\lambda + q^{-1}\lambda^{-1}}{(q-q^{-1})^2}. \tag{4.3}$$

Let us now prove that the restriction of the Harish-Chandra homomorphism to the centre Z_q is injective.

Lemma VI.4.5. *Let $z \in Z_q$. If $\varphi(z) = 0$, then $z = 0$.*

PROOF. Let z be an element in the centre such that $\varphi(z) = 0$. Assume z non-zero; it can be written as $z = \sum_{i=k}^{\ell} F^i P_i E^i$ where $0 < k \leq \ell$ are integers and $P_k, \ldots, P_\ell$ are non-zero Laurent polynomials in K. Consider a Verma module $V(\lambda)$ whose highest weight is not a power of q. Then Relations (3.4–3.5) show that $Ev_p = 0$ if and only if $p = 0$. Let us apply z to the vector v_k of $V(\lambda)$. On the one hand, Proposition 4.4 implies that $zv_k = \varphi(z)(\lambda)v_k = 0$; on the other, we get

$$zv_k = F^k P_k E^k v_k = c\, P_k(\lambda)v_k,$$

where c is a non-zero constant. It follows that $P_k(\lambda) = 0$. As a consequence, we have a non-zero polynomial P_k with infinitely many roots; hence a contradiction. □

Verma modules will also allow us to prove a symmetry relation for the polynomials $\varphi(z)$. Before we state this, let us introduce the following notation. For any Laurent polynomial P in $k[K, K^{-1}]$, denote by $\widetilde{P}$ the polynomial defined by the change of variable

$$\widetilde{P}(\lambda) = P(q^{-1}\lambda).$$

Lemma VI.4.6. *For any element z in the centre Z_q, we have*

$$\widetilde{\varphi(z)}(\lambda) = \widetilde{\varphi(z)}(\lambda^{-1}).$$

PROOF. For any integer $n > 0$, consider the Verma module $V(q^{n-1})$. By (3.5) we have

$$Ev_n = \frac{q^{-(n-1)}q^{n-1} - q^{n-1}q^{-(n-1)}}{q - q^{-1}}\, v_n = 0.$$

Thus, v_n is a highest weight vector of weight $q^{n-1-2n} = q^{-n-1}$. By Proposition 4.4, a central element z acts on the module generated by v_n as the multiplication by the scalar $\varphi(z)(q^{-n-1})$; but, since v_n is in $V(q^{n-1})$, the element z also acts as the scalar $\varphi(z)(q^{n-1})$. In other words, we have

$$\widetilde{\varphi(z)}(q^n) = \widetilde{\varphi(z)}(q^{-n}).$$

One concludes by observing that the powers of q form an infinite sequence of distinct scalars. □

We pause to record the following lemma.

Lemma VI.4.7. *Any Laurent polynomial of $k[K, K^{-1}]$ satisfying the relation $P(\lambda) = P(\lambda^{-1})$ is a polynomial in $K + K^{-1}$.*

PROOF. We proceed by induction on the degree of the polynomial. If the degree is 0, the statement holds trivially. Let us suppose that the lemma is proved for all degrees $< n$ and let P be a Laurent polynomial of degree n such that $P(\lambda) = P(\lambda^{-1})$. Then we may write P in the form

$$P(K) = c\,(K^n + K^{-n}) + \text{ (terms of degree } < n).$$

Now,

$$K^n + K^{-n} = (K + K^{-1})^n + \text{ (terms of degree } < n).$$

One concludes by applying the induction hypothesis. □

We are ready to state the main theorem.

Theorem VI.4.8. *When q is not a root of unity, the centre Z_q of U_q is a polynomial algebra generated by the element C_q. The restriction of the Harish-Chandra homomorphism to Z_q is an isomorphism onto the subalgebra of $k[K, K^{-1}]$ generated by $qK + q^{-1}K^{-1}$.*

PROOF. We already know that the restriction of φ to the centre is injective. We are left with determining its image. By Lemmas 4.6 and 4.7, the latter is contained in the subalgebra of $k[K, K^{-1}]$ generated by $qK + q^{-1}K^{-1}$. Consider the central element C_q defined above. By (4.2) we know that

$$\varphi(C_q) = \frac{1}{(q-q^{-1})^2}(qK + q^{-1}K^{-1}),$$

Chapter VII

A Hopf Algebra Structure on $U_q(\mathfrak{sl}(2))$

We assume in this chapter that the field k is the field of complex numbers and that q is *not* a root of unity. We now equip the algebra $U_q = U_q(\mathfrak{sl}(2))$ defined in Chapter VI with a Hopf algebra structure. Then we prove that any finite-dimensional U_q-module is a direct sum of the simple modules described in VI.3. We show later that U_q acts naturally on the quantum plane of IV.1 and that it is in duality with the Hopf algebra $SL_q(2)$ of Chapter IV. We shall also build scalar products on the simple finite-dimensional U_q-modules. We describe the quantum Clebsch-Gordan formula and give the main properties of the quantum Clebsch-Gordan coefficients.

VII.1 Comultiplication

We resume the notation of the previous chapter. Set

$$\Delta(E) = 1 \otimes E + E \otimes K, \quad \Delta(F) = K^{-1} \otimes F + F \otimes 1, \tag{1.1}$$

$$\Delta(K) = K \otimes K, \quad \Delta(K^{-1}) = K^{-1} \otimes K^{-1}, \tag{1.2}$$

$$\varepsilon(E) = \varepsilon(F) = 0, \quad \varepsilon(K) = \varepsilon(K^{-1}) = 1, \tag{1.3}$$

and

$$S(E) = -EK^{-1}, \quad S(F) = -KF, \quad S(K) = K^{-1}, \quad S(K^{-1}) = K. \tag{1.4}$$

Proposition VII.1.1. *Relations* (1.1–1.4) *endow* U_q *with a Hopf algebra structure.*

PROOF. (a) We first show that Δ defines a morphism of algebras from U_q into $U_q \otimes U_q$. It is enough to check that

$$\Delta(K)\Delta(K^{-1}) = \Delta(K^{-1})\Delta(K) = 1, \tag{1.5}$$

$$\Delta(K)\Delta(E)\Delta(K^{-1}) = q^2\Delta(E), \tag{1.6}$$

$$\Delta(K)\Delta(F)\Delta(K^{-1}) = q^{-2}\Delta(F), \tag{1.7}$$

$$[\Delta(E), \Delta(F)] = \frac{\Delta(K) - \Delta(K^{-1})}{q - q^{-1}}. \tag{1.8}$$

Relations (1.5) are clear. As for (1.6), we have

$$\begin{aligned} \Delta(K)\Delta(E)\Delta(K^{-1}) &= (K \otimes K)(1 \otimes E + E \otimes K)(K^{-1} \otimes K^{-1}) \\ &= 1 \otimes KEK^{-1} + KEK^{-1} \otimes K \\ &= q^2(1 \otimes E + E \otimes K) \\ &= q^2\Delta(E). \end{aligned}$$

Relation (1.7) is proved in a similar way. Finally, for (1.8) we have

$$\begin{aligned} &[\Delta(E), \Delta(F)] \\ &= (1 \otimes E + E \otimes K)(K^{-1} \otimes F + F \otimes 1) \\ &\qquad - (K^{-1} \otimes F + F \otimes 1)(1 \otimes E + E \otimes K) \\ &= K^{-1} \otimes EF + F \otimes E + EK^{-1} \otimes KF + EF \otimes K \\ &\qquad - K^{-1} \otimes FE - K^{-1}E \otimes FK - F \otimes E - FE \otimes K \\ &= K^{-1} \otimes [E,F] + [E,F] \otimes K \\ &= \frac{K^{-1} \otimes (K - K^{-1}) + (K - K^{-1}) \otimes K}{q - q^{-1}} \\ &= \frac{\Delta(K) - \Delta(K^{-1})}{q - q^{-1}}. \end{aligned}$$

(b) Next, we check that Δ is coassociative. It suffices to do it on the four generators. We give a sample calculation for E. On the one hand, we have

$$(\Delta \otimes \mathrm{id})\Delta(E) = (\Delta \otimes \mathrm{id})(1 \otimes E + E \otimes K) = 1 \otimes 1 \otimes E + 1 \otimes E \otimes K + E \otimes K \otimes K.$$

On the other hand, we have

$$(\mathrm{id} \otimes \Delta)\Delta(E) = (\mathrm{id} \otimes \Delta)(1 \otimes E + E \otimes K) = 1 \otimes 1 \otimes E + 1 \otimes E \otimes K + E \otimes K \otimes K,$$

which is the same.

(c) It is easy to check that ε defines a morphism of algebras from U_q onto k and satisfies the counit axiom.

(d) It remains to see that S defines an antipode for U_q. We have first to check that S is a morphism of algebras from U_q into U_q^{op}, namely that the following four relations hold:

$$S(K^{-1})S(K) = S(K)S(K^{-1}) = 1, \tag{1.9}$$

$$S(K^{-1})S(E)S(K) = q^2 S(E), \tag{1.10}$$

$$S(K^{-1})S(F)S(K) = q^{-2} S(F), \tag{1.11}$$

$$[S(F), S(E)] = \frac{S(K) - S(K^{-1})}{q - q^{-1}}. \tag{1.12}$$

We give the computations for (1.10) and (1.12). We have

$$S(K^{-1})S(E)S(K) = -K(EK^{-1})K^{-1} = -q^2 EK^{-1} = q^2 S(E)$$

and

$$\begin{aligned} [S(F), S(E)] &= KFEK^{-1} - EK^{-1}KF = [F, E] \\ &= \frac{K^{-1} - K}{q - q^{-1}} = \frac{S(K) - S(K^{-1})}{q - q^{-1}}. \end{aligned}$$

To conclude that S is an antipode, we appeal to Lemma III.3.6. It suffices to check that the relations

$$\sum_{(x)} x' S(x'') = \sum_{(x)} S(x')x'' = \varepsilon(x)1$$

hold when x is any of the generators E, F, K, K^{-1}. This verification is left to the reader. □

We have thus defined a Hopf algebra that is *neither commutative nor cocommutative.* Observe also that the square of the antipode is not the identity (when $q^2 \neq 1$). Nevertheless, it is an inner automorphism, as expressed by the following statement.

Proposition VII.1.2. *We have $S^2(u) = KuK^{-1}$ for any $u \in U_q$.*

PROOF. In effect, we have

$$S^2(E) = q^2 E = KEK^{-1}, \quad S^2(F) = q^{-2} F = KFK^{-1},$$

and $S^2(K) = K$. □

We thus get, just as in Chapter IV, examples of Hopf algebras whose antipodes have a finite order $2N$ for any integer $N > 1$; it suffices to take any primitive $2N$-th root of unity as the parameter q.

The algebra U'_q of VI.2 can be endowed with a Hopf algebra structure such that the isomorphism $\varphi : U_q \to U'_q$ of Proposition VI.2.1 preserves the Hopf algebra structures. In addition to Relations (1.1–1.4), it suffices to set

$$\Delta(L) = K^{-1} \otimes L + L \otimes K, \quad \varepsilon(L) = 0, \quad S(L) = -L. \tag{1.13}$$

It follows easily that the isomorphism $U(\mathfrak{sl}(2)) \cong U'_1/(K-1)$ is an isomorphism of Hopf algebras. In other words, the Hopf algebra structure of U_q extends the Hopf algebra structure of the enveloping algebra $U(\mathfrak{sl}(2))$.

We end this section by expressing the comultiplication of U_q in the basis described in Proposition VI.1.4.

Proposition VII.1.3. *For all $i, j \in \mathbf{N}$ and $\ell \in \mathbf{Z}$ we have*

$$\begin{aligned} \Delta(E^i F^j K^\ell) &= \sum_{r=0}^{i} \sum_{s=0}^{j} q^{r(i-r)+s(j-s)-2(i-r)(j-s)} \begin{bmatrix} i \\ r \end{bmatrix} \begin{bmatrix} j \\ s \end{bmatrix} \\ &\qquad \times E^{i-r} F^s K^{\ell-(j-s)} \otimes E^r F^{j-s} K^{\ell+(i-r)}. \end{aligned}$$

PROOF. First observe that

$$\begin{aligned} \Delta(E^i F^j K^\ell) &= \Delta(E)^i \Delta(F)^j \Delta(K)^\ell \\ &= (1 \otimes E + E \otimes K)^i (K^{-1} \otimes F + F \otimes 1)^j (K^\ell \otimes K^\ell). \end{aligned}$$

Now,

$$(E \otimes K)(1 \otimes E) = q^2 (1 \otimes E)(E \otimes K)$$

and

$$(K^{-1} \otimes F)(F \otimes 1) = q^2 (F \otimes 1)(K^{-1} \otimes F).$$

Applying Relation (VI.1.9), we get

$$\Delta(E)^i = \sum_{r=0}^{i} q^{r(i-r)} \begin{bmatrix} i \\ r \end{bmatrix} E^{i-r} \otimes E^r K^{i-r}$$

and

$$\Delta(F)^j = \sum_{s=0}^{j} q^{s(j-s)} \begin{bmatrix} j \\ s \end{bmatrix} F^s K^{-(j-s)} \otimes F^{j-s}.$$

One concludes with (VI.1.11). □

VII.2 Semisimplicity

In this section we shall prove that any finite-dimensional U_q-module is the direct sum of simple U_q-modules when q is not a root of unity, which we assume in this chapter. Let us start with a technical lemma on the simple modules $V_{\varepsilon,n}$ of VI.3.

Lemma VII.2.1. *There exists an element C of the centre of U_q acting by 0 on $V_{\varepsilon,0}$ and by a non-zero scalar on $V_{\varepsilon',n}$ when n is an integer > 0 and $\varepsilon, \varepsilon' = \pm 1$.*

PROOF. Define

$$C = C_q - \varepsilon \frac{q+q^{-1}}{(q-q^{-1})^2}$$

where C_q is the central element introduced in VI.4. By (VI.4.3), C acts on $V_{\varepsilon,0}$ by

$$\varepsilon \frac{q+q^{-1}}{(q-q^{-1})^2} - \varepsilon \frac{q+q^{-1}}{(q-q^{-1})^2} = 0,$$

and on $V_{\varepsilon',n}$ by

$$\varepsilon' \frac{q^{n+1}+q^{-(n+1)}}{(q-q^{-1})^2} - \varepsilon \frac{q+q^{-1}}{(q-q^{-1})^2}.$$

We have to show that the latter is not 0. If it were, we would have

$$q^{2n+2} - \varepsilon\varepsilon' q^{n+2} - \varepsilon\varepsilon' q^n + 1 = 0,$$

or, equivalently,

$$(q^{n+2} - \varepsilon\varepsilon')(q^n - \varepsilon\varepsilon') = 0,$$

which would be contrary to the assumptions. □

We now state a quantum version of Theorem V.4.6.

Theorem VII.2.2. *When q is not a root of unity, any finite-dimensional U_q-module is semisimple.*

PROOF. We follow the proof of Theorem V.4.6 step by step. Recall that it is enough to prove that if V is any finite-dimensional U_q-module and V' is any submodule of V, then there exists another submodule V'' such that V is isomorphic to the direct sum $V' \oplus V''$ as a module.

1. We shall first prove the existence of such a submodule V'' in the case when V' is of codimension one in V. We proceed by induction on the dimension of V'.

If $\dim(V') = 0$, we may take $V'' = V$. If $\dim(V') = 1$, then necessarily V' and V/V' are simple one-dimensional modules of respective weights ε_1 and ε_2. If the weights ε_1 and ε_2 differ, there exists a basis $\{v_1, v_2\}$ of V in which K acts diagonally. Since Ev_i is an eigenvector for K with eigenvalue $\varepsilon_i q^2 \neq \varepsilon_j$, we must have $Ev_i = 0$ for $i = 1, 2$. Similarly, F acts trivially on V. Hence, the module V is the direct sum of the submodules $V' = kv_1$ and $V'' = kv_2$.

Otherwise, there exists a basis $\{v_1, v_2\}$ with $V' = kv_1$ such that we have $Kv_1 = \varepsilon v_1$ and $Kv_2 = \varepsilon v_2 + \alpha v_1$. Again, Ev_1 is an eigenvector for K with eigenvalue $\varepsilon q^2 \neq \varepsilon$, hence it is zero. Let us prove that Ev_2 is zero too. Indeed, writing $Ev_2 = \lambda v_1 + \mu v_2$, we have

$$\varepsilon\lambda v_1 + \mu(\varepsilon v_2 + \alpha v_1) = KEv_2 = q^2 EKv_2 = q^2 E(\varepsilon v_2 + \alpha v_1) = \varepsilon q^2(\lambda v_1 + \mu v_2),$$

which implies $\mu\varepsilon(q^2-1) = 0$ and $\lambda\varepsilon(q^2-1) = \mu\alpha$. Thus, $\lambda = \mu = 0$. One proves in a similar way that F acts as 0 on V. Since $[E, F]$ acts as 0, we have $K = K^{-1}$ on V. In particular, since $K^{-1}v_2 = \varepsilon v_2 - \alpha v_1$, we have $\alpha = -\alpha$, hence $\alpha = 0$. In this situation K is also diagonalizable and we reach the same conclusion as before.

We now assume that $\dim(V') = p > 1$ and that the assertion to be proved holds in dimension $< p$. There is the following alternative: either V' is simple, or it is not.

1.a. If V' is not simple, one uses the same argument as in Part 1.a of the proof of Theorem V.4.6.

1.b. Suppose now that the submodule V' is simple of dimension > 1. The one-dimensional quotient module V/V' has weight $\varepsilon = \pm 1$. Let us consider the operator C of Lemma 2.1; it acts by 0 on V/V'. Consequently, we have $CV \subset V'$. On the other hand, C acts on V' as multiplication by a scalar $\alpha \neq 0$. It follows that C/α is the identity on V'. Therefore the map C/α is a projector of V onto V'. This projector is U_q-linear since C is central. By Proposition I.1.3, the submodule $V'' = \mathrm{Ker}\,(C/\alpha)$ meets the requirements.

2. *General case.* We are now given finite-dimensional modules $V' \subset V$ without any restriction on the codimension. We shall reduce to the codimension-one case by considering vector spaces $W' \subset W$ defined as follows: W [resp. W'] is the subspace of all linear maps from V to V' whose restriction to V' is a homothety [resp. is zero]. It is clear that W' is of codimension one in W. In order to reduce to Part 1, we have to equip W and W' with U_q-module structures. We give $\mathrm{Hom}(V, V')$ the U_q-module structure defined in III.5. Let us check that W and W' are submodules of $\mathrm{Hom}(V, V')$. For $f \in W$, let α be the scalar such that $f(v) = \alpha v$ for all $v \in V'$; then for all $x \in U_q$ and $v \in V'$, we have

$$(xf)(v) = \sum_{(x)} x' f(S(x'')v) = \alpha\Big(\sum_{(x)} x' S(x'')\Big)v = \alpha\varepsilon(x)v.$$

A similar argument proves that W' is a submodule too. Applying Part 1, we get a one-dimensional submodule W'' such that $W \cong W' \oplus W''$. Let f be a generator of W''. By definition, it acts on V' as a scalar $\alpha \neq 0$. It follows that f/α is a projector of V onto V' and that $V'' = \mathrm{Ker}\,(f)$ is a supplementary subspace of V'. To conclude, it suffices to check that V'' is a U_q-submodule of V. Now, since W'' is a one-dimensional submodule, it is simple of weight ± 1. Therefore, for all $x \in U_q$ we have $xf = \pm\,\varepsilon(x)f$. In particular, if v belongs to V'', we have

$$K^{-1}f(Kv) = (K^{-1}f)(v) = \pm\varepsilon(K^{-1})f(v) = 0,$$

which implies $f(Kv) = 0$. This proves that $KV'' \subset V''$. Similarly, V'' is stable under K^{-1}. On the other hand, we have for v, hence for Kv in V'',

$$\begin{aligned} 0 &= \pm\varepsilon(E)f(Kv) = (Ef)(Kv \\ &= f(S(E)Kv) + Ef(K^{-1}Kv) = -f(Ev) + Ef(v). \end{aligned}$$

Consequently, $f(Ev) = 0$, which implies that V'' is stable under the action of E. A similar computation shows that $FV'' \subset V''$. The subspace V'' is therefore a submodule. □

VII.3 Action of $U_q(\mathfrak{sl}(2))$ on the Quantum Plane

This section is the quantum version of V.6. We start with a few generalities on skew-derivations of an algebra A. For $a \in A$, denote by a_ℓ [resp. a_r] the left [resp. right] multiplication by the element a. If σ is an automorphism of the algebra A, we have

$$\sigma a_\ell = \sigma(a)_\ell \sigma \quad \text{and} \quad \sigma a_r = \sigma(a)_r \sigma. \tag{3.1}$$

Given two automorphisms σ and τ of an algebra A, a linear endomorphism δ of A is called a (σ,τ)-*derivation* if

$$\delta(aa') = \sigma(a)\delta(a') + \delta(a)\tau(a') \tag{3.2}$$

for all a, a' in A. Relation (3.2) is equivalent to

$$\delta a_\ell = \sigma(a)_\ell \delta + \delta(a)_\ell \tau \tag{3.3}$$

or to

$$\delta a_r = \tau(a)_r \delta + \delta(a)_r \sigma. \tag{3.4}$$

It is well-known that, if δ is a derivation of a commutative algebra, then $a_\ell \delta$ is a derivation too. In a non-commutative situation, this is no longer the case. Nevertheless, the following assertion holds.

Lemma VII.3.1. *Let δ be a (σ,τ)-derivation of A and a be an element of A. If there exist algebra automorphisms σ' and τ' of A such that*

$$a_r \sigma' = a_\ell \sigma \quad \textit{and} \quad a_\ell \tau' = a_r \tau,$$

then the linear endomorphism $a_\ell\delta$ is a (σ',τ)-derivation and $a_r\delta$ is a (σ,τ')-derivation. □

PROOF. This follows from straightforward computations.

We now return to the quantum plane $A = k_q[x,y]$ of IV.1. Let us consider its algebra automorphisms σ_x and σ_y defined by

$$\sigma_x(x) = qx, \quad \sigma_x(y) = y, \quad \sigma_y(x) = x, \quad \sigma_y(y) = qy. \tag{3.5}$$

When $q = 1$, we have $\sigma_x = \sigma_y = \mathrm{id}$. We define q-analogues $\partial_q/\partial x$ and $\partial_q/\partial y$ of the classical partial derivatives by

$$\frac{\partial_q(x^m y^n)}{\partial x} = [m]\, x^{m-1}y^n \quad \text{and} \quad \frac{\partial_q(x^m y^n)}{\partial y} = [n]\, x^m y^{n-1} \tag{3.6}$$

for all $m, n \geq 0$. Let us describe all commutation relations between the endomorphisms x_ℓ, x_r, y_ℓ, y_r, σ_x, σ_y, $\partial_q/\partial x$, $\partial_q/\partial y$. We say that a commutation relation between two endomorphisms u and v is trivial if $uv = vu$.

Proposition VII.3.2. (a) *Within the algebra of linear endomorphisms of $k_q[x,y]$, all commutation relations between the above six endomorphisms are trivial, except the following ones:*

$$\begin{aligned} &y_\ell x_\ell = q x_\ell y_\ell, \qquad x_r y_r = q y_r x_r, \\ &\sigma_x x_{\ell,r} = q x_{\ell,r}\sigma_x, \qquad \sigma_y y_{\ell,r} = q y_{\ell,r}\sigma_y, \\ &\frac{\partial_q}{\partial x}\sigma_x = q\sigma_x \frac{\partial_q}{\partial x}, \qquad \frac{\partial_q}{\partial y}\sigma_y = q\sigma_y\frac{\partial_q}{\partial y}, \\ &\frac{\partial_q}{\partial x} y_\ell = q y_\ell \frac{\partial_q}{\partial x}, \qquad \frac{\partial_q}{\partial y} x_r = q x_r \frac{\partial_q}{\partial y}, \\ &\frac{\partial_q}{\partial x} x_\ell = q^{-1} x_\ell \frac{\partial_q}{\partial x} + \sigma_x = q x_\ell \frac{\partial_q}{\partial x} + \sigma_x^{-1}, \\ &\frac{\partial_q}{\partial y} y_r = q^{-1} y_r \frac{\partial_q}{\partial y} + \sigma_y = q y_r \frac{\partial_q}{\partial y} + \sigma_y^{-1}. \end{aligned}$$

We also have

$$x_\ell \frac{\partial_q}{\partial x} = \frac{\sigma_x - \sigma_x^{-1}}{q - q^{-1}} \quad \textit{and} \quad y_r \frac{\partial_q}{\partial y} = \frac{\sigma_y - \sigma_y^{-1}}{q - q^{-1}}.$$

(b) *The endomorphism $\frac{\partial_q}{\partial x}$ is a $(\sigma_x^{-1}\sigma_y, \sigma_x)$-derivation and, similarly, $\frac{\partial_q}{\partial y}$ is a $(\sigma_y, \sigma_x\sigma_y^{-1})$-derivation.*

PROOF. (a) This part results from easy, but fastidious computations.

(b) First observe that, if Relation (3.3) holds for two elements a, a' of A, then it holds for their product aa'. Indeed, we have

$$\begin{aligned} \delta(aa')_\ell &= \delta a_\ell a'_\ell \\ &= \sigma(a)_\ell \delta a'_\ell + \delta(a)_\ell \tau a'_\ell \\ &= \sigma(a)_\ell \sigma(a')_\ell \delta + \sigma(a)_\ell \delta(a')_\ell \tau + \delta(a)_\ell \tau(a')_\ell \tau \\ &= \sigma(aa')_\ell \delta + \delta(aa')_\ell \tau. \end{aligned}$$

We are reduced to checking Relation (3.3) for $\partial_q/\partial x$ and $\partial_q/\partial y$ in the case when $a = x$ and $a = y$. For $\partial_q/\partial x$ we have

$$(\sigma_x^{-1}\sigma_y)(x)_\ell \frac{\partial_q}{\partial x} + \left(\frac{\partial_q x}{\partial x}\right)_\ell \sigma_x = q^{-1}x_\ell\frac{\partial_q}{\partial x} + \sigma_x = \frac{\partial_q}{\partial x}x_\ell$$

by Proposition 3.2(a). We also have

$$(\sigma_x^{-1}\sigma_y)(y)_\ell \frac{\partial_q}{\partial x} + \left(\frac{\partial_q y}{\partial x}\right)_\ell \sigma_x = qy_\ell\frac{\partial_q}{\partial x} = \frac{\partial_q}{\partial x}y_\ell.$$

Similar computations can be carried out for $\partial_q/\partial y$. □

We now show how the "quantum partial derivatives" $\frac{\partial_q}{\partial x}$ and $\frac{\partial_q}{\partial y}$ endow the quantum plane with the structure of a module-algebra (as defined in V.6.1) over the Hopf algebra U_q.

Theorem VII.3.3. *For any $P \in k_q[x,y]$, set*

$$EP = x\frac{\partial_q P}{\partial y}, \quad FP = \frac{\partial_q P}{\partial x}y,$$

$$KP = (\sigma_x\sigma_y^{-1})(P), \quad K^{-1}P = (\sigma_y\sigma_x^{-1})(P). \tag{3.7}$$

(a) *Formulas* (3.7) *define the structure of a U_q-module-algebra on $k_q[x,y]$.*

(b) *The subspace $k_q[x,y]_n$ of homogeneous elements of degree n is a U_q-submodule of the quantum plane. It is generated by the highest weight vector x^n and is isomorphic to the simple module $V_{1,n}$.*

Theorem 3.3 is the quantum version of Theorem V.6.4. It shows that the quantum plane contains all finite-dimensional simple U_q-modules.

PROOF. (a) We first show that the formulas (3.7) equip $k_q[x,y]$ with a U_q-module structure. In other words, we have to check Relations (VI.1.10–1.12). We use Proposition 3.2.

Relation (1.10) is trivially verified. For Relation (1.11) we have

$$\begin{aligned} KEK^{-1} &= \sigma_x\sigma_y^{-1}x_\ell\frac{\partial_q}{\partial y}\sigma_y\sigma_x^{-1} \\ &= qx_\ell\sigma_y^{-1}\frac{\partial_q}{\partial y}\sigma_y \\ &= q^2x_\ell\frac{\partial_q}{\partial y} = q^2E. \end{aligned}$$

One proves $KFK^{-1} = q^{-2}F$ in a similar fashion. As for (1.12), we have

$$\begin{aligned} [E,F] &= x_\ell\frac{\partial_q}{\partial y}y_r\frac{\partial_q}{\partial x} - y_r\frac{\partial_q}{\partial x}x_\ell\frac{\partial_q}{\partial y} \\ &= q^{-1}x_\ell y_r\frac{\partial_q}{\partial y}\frac{\partial_q}{\partial x} + x_\ell\sigma_y\frac{\partial_q}{\partial x} - q^{-1}y_r x_\ell\frac{\partial_q}{\partial x}\frac{\partial_q}{\partial y} - y_r\sigma_x\frac{\partial_q}{\partial y} \\ &= x_\ell\sigma_y\frac{\partial_q}{\partial x} - y_r\sigma_x\frac{\partial_q}{\partial y} \\ &= \frac{\sigma_y(\sigma_x - \sigma_x^{-1}) - \sigma_x(\sigma_y - \sigma_y^{-1})}{q-q^{-1}} \\ &= \frac{\sigma_x\sigma_y^{-1} - \sigma_y\sigma_x^{-1}}{q-q^{-1}} \\ &= \frac{K-K^{-1}}{q-q^{-1}}. \end{aligned}$$

We now prove that the quantum plane is a U_q-algebra. By Lemma V.6.2, it is enough to check that for any $u \in U_q$, we have

$$u1 = \varepsilon(u)1, \tag{3.8}$$

and

$$K(PQ) = K(P)K(Q), \tag{3.9}$$

$$E(PQ) = PE(Q) + E(P)K(Q), \tag{3.10}$$

$$F(PQ) = K^{-1}(P)F(Q) + F(P)Q, \tag{3.11}$$

for any pair (P,Q) of elements of the quantum plane. Relation (3.8) follows easily from (3.5–3.7) and Relation (3.9) from the fact that K acts as an algebra automorphism. By Lemma 3.1 and by Proposition 3.2(b), the endomorphism $x_\ell\frac{\partial_q}{\partial y}$ is a $(\mathrm{id}, \sigma_x\sigma_y^{-1})$-derivation and $y_r\frac{\partial_q}{\partial x}$ is a $(\sigma_x^{-1}\sigma_y, \mathrm{id})$-derivation, which implies Relations (3.10–3.11).

(b) We have $Ex^n = 0$, $Kx^n = q^nx^n$, and

$$\frac{1}{[p]!}F^p(x^n) = q^{-p}\frac{[n]!}{[p]![n-p]!}x^{n-p}y^p.$$

Consequently, x^n is a highest weight vector of weight q^n and generates the submodule $k_q[x,y]_n$. □

Observe that $[E,F]$ acts on the quantum plane as the operator

$$x_\ell\sigma_y\frac{\partial_q}{\partial x} - y_r\sigma_x\frac{\partial_q}{\partial y}.$$

Its "limit when q tends to 1" is the operator $x\partial/\partial x - y\partial/\partial y$ by which the element H of $\mathfrak{sl}(2)$ acts on the affine plane (see Theorem V.6.4).

VII.4 Duality between the Hopf Algebras $U_q(\mathfrak{sl}(2))$ and $SL_q(2)$

We now relate this chapter to Chapter IV by showing that U_q is in duality with the Hopf algebra $SL_q(2)$ defined in IV.6. We use the concept of duality introduced in V.7.

As in V.7, our first task is to construct an algebra morphism ψ from the algebra $M_q(2)$ (defined in IV.3) into the dual algebra U_q^*. We shall deduce a bilinear form on $U_q \times M_q(2)$ defined by $< u, x > = \psi(x)(u)$ and satisfying Relations (V.7.2) and (V.7.4). Giving the morphism ψ is equivalent to giving four elements A, B, C, D in U_q^* satisfying the six defining relations of $M_q(2)$ (see IV.3).

The definitions of A, B, C, D use the simple U_q-module $V_{1,1}$ of highest weight q and with basis $\{v_0, v_1\}$. The matrix representations of the generators E, F and K in this basis have been given in VI.3. Setting $\rho = \rho_{1,1}$, we have

$$\rho(E) = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \rho(F) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad \rho(K) = \begin{pmatrix} q & 0 \\ 0 & q^{-1} \end{pmatrix}. \tag{4.1}$$

More generally, for any element u of U_q, define

$$\rho(u) = \begin{pmatrix} A(u) & B(u) \\ C(u) & D(u) \end{pmatrix}. \tag{4.2}$$

We thus get four linear forms on U_q, hence four elements A, B, C, D of U_q^*.

Lemma VII.4.1. *The quadruple (A, B, C, D) is a U_q^*-point of $M_q(2)$.*

PROOF. This is done by a direct, but laborious checking. First, one has to compute in U_q^* the twelve products AB, BA, AC, $CA, \ldots$ formed by all pairs of distinct elements of the set $\{A, B, C, D\}$. Recall that the product of any two elements x, y of U_q^* is given by

$$(xy)(u) = \sum_{(u)} x(u')y(u''). \tag{4.3}$$

It suffices to evaluate $(xy)(u)$ on the basis $\{E^iF^jK^\ell\}$ of U_q. Let us set $u = E^iF^jK^\ell$. When $i > 2$ or when $j > 2$, we see from Proposition 1.3 that in the sum $\sum_{(u)} u' \otimes u''$, either u' or u'' contains powers of E or of F with exponents > 1. Now, by (4.1), $\rho(E^iF^jK^\ell) = \rho(E)^i\rho(F)^j\rho(K)^\ell$ vanishes when $i > 1$ or $j > 1$. Consequently, if $x, y \in \{A, B, C, D\}$, we have

$$(xy)(E^iF^jK^\ell) = 0$$

whenever $i > 2$ or $j > 2$. It therefore remains to evaluate the products on the elements $E^iF^jK^\ell$ where $0 \leq i \leq 2$ and $0 \leq j \leq 2$.

(i) If $u = K^\ell$, we have $\Delta(K^\ell) = K^\ell \otimes K^\ell$ and all products evaluated on u vanish, except that

$$(AD)(u) = (DA)(u) = 1. \tag{4.4}$$

(ii) If $u = FK^\ell$, we have $\Delta(FK^\ell) = K^{\ell-1} \otimes FK^\ell + FK^\ell \otimes K^\ell$ and all products evaluated on u vanish, except that

$$(CA)(u) = q\,(AC)(u) = q^{2\ell} \quad \text{and} \quad (DC)(u) = q\,(CD)(u) = q. \tag{4.5}$$

(iii) If $u = F^2K^\ell$, we have

$$\Delta(F^2K^\ell) = \alpha_1\, FK^{\ell-1} \otimes FK^\ell + (\text{terms of degree } > 2 \text{ in } F)$$

and all products evaluated on u vanish.

(iv) If $u = EK^\ell$, we have $\Delta(EK^\ell) = EK^\ell \otimes K^{\ell+1} + K^\ell \otimes EK^\ell$ and all products evaluated on u vanish, except that

$$(BA)(u) = q\,(AB)(u) = q \quad \text{and} \quad (DB)(u) = q\,(BD)(u) = q^{-2\ell}. \tag{4.6}$$

(v) If $u = EFK^\ell$, we have

$$\begin{aligned} \Delta(EFK^\ell) &= K^{\ell-1} \otimes EFK^\ell + EFK^\ell \otimes K^{\ell+1} \\ &\quad + FK^\ell \otimes EK^\ell + q^{-2}\, EK^{\ell-1} \otimes FK^{\ell+1} \end{aligned}$$

and all products evaluated on u vanish, except that

$$(BC)(u) = (CB)(u) = 1, \quad (DA)(u) = q, \quad \text{and} \quad (AD)(u) = q^{-1}. \tag{4.7}$$

(vi) If $u = EF^2K^\ell$, we have

$$\begin{aligned} \Delta(EF^2K^\ell) &= \alpha_2\,(FK^{\ell-1} \otimes EFK^\ell + q^{-2}\, EFK^{\ell-1} \otimes FK^{\ell+1}) \\ &\quad + (\text{terms of degree } > 2 \text{ in } F) \end{aligned}$$

and all products evaluated on u vanish, except

$$(CA)(u) = q\,(AC)(u) = \alpha_2\, q^{2\ell-1}. \tag{4.8}$$

(vii) If $u = E^2K^\ell$, we have

$$\Delta(E^2K^\ell) = \alpha_3\, EK^\ell \otimes EK^{\ell+1} + (\text{terms of degree } > 2 \text{ in } E)$$

and all products evaluated on u vanish.

(viii) If $u = E^2FK^\ell$, we have

$$\begin{aligned} \Delta(E^2FK^\ell) &= \alpha_4\,(EFK^\ell \otimes EK^{\ell+1} + q^{-2}\, EK^{\ell-1} \otimes EFK^{\ell+1}) \\ &\quad + (\text{terms of degree } > 2 \text{ in } E) \end{aligned}$$

and all products evaluated on u vanish, except

$$(BA)(u) = q\,(AB)(u) = \alpha_4. \tag{4.9}$$

(ix) If $u = E^2F^2K^\ell$, we have

$$\Delta(E^2F^2K^\ell) = \alpha_5\, EFK^{\ell-1} \otimes EFK^{\ell+1} + (\text{terms of degree } > 2 \text{ in } E \text{ and } F)$$

and all products evaluated on u vanish.

In Cases (iii) and (vi–ix) we denoted by α_1, α_2, α_3, α_4, and α_5 scalars that are well-defined, but about which we need not be explicit. From this case-by-case analysis, it is easy to check that A, B, C, D satisfy the six defining relations of $M_q(2)$. As a sample calculation, we check the most involved relation, namely

$$DA - AD = (q - q^{-1})\,BC.$$

From the above observations, we see that it is enough to perform the checking for $u = K^\ell$, which is trivial, and for $u = EFK^\ell$. In the latter case, (4.7) implies

$$(DA - AD)(u) = q - q^{-1} = (q - q^{-1})\,(BC)(u).$$

□

As a consequence of Lemma 4.1 and of IV.3, there exists a unique morphism of algebras ψ from $M_q(2)$ into U_q^* such that

$$\psi(a) = A, \quad \psi(b) = B, \quad \psi(c) = C, \quad \psi(d) = D.$$

Proposition VII.4.2. *The bilinear form* $< u, x > = \psi(x)(u)$ *realizes a duality between the bialgebras* U_q *and* $M_q(2)$.

PROOF. The comultiplication and the counit of $M_q(2)$ being the same as those of $M(2)$, the proof follows along the same lines as in the proof of Proposition V.7.3. □

The duality between $M_q(2)$ and U_q is not perfect, just as in the classical case.

Lemma VII.4.3. *For the quantum determinant* $\det_q = da - qbc$ *of* $M_q(2)$, *we have* $\psi(\det_q) = 1$.

Equivalently, $< u, \det_q > = \varepsilon(u)$ for all elements u of U_q.

PROOF. By Theorem IV.5.1, the element $\det_q$ is grouplike, i.e., we have $\Delta(\det_q) = \det_q \otimes \det_q$. It results that the map $u \mapsto < u, \det_q >$ is a morphism of algebras from U_q to k. To show that this morphism coincides with the counit ε, it suffices to check that both maps take the same values

on the generators E, F, K and K^{-1}. Using (V.7.2–7.3) and (1.1), we get for E:

$$\begin{aligned} &< E, \det_q > \\ &= \; < E, da > -q < E, bc > \\ &= \; \varepsilon(d) < E, a > + < E, d >< K, a > \\ &\qquad\qquad -q\varepsilon(b) < E, c > -q < E, b >< K, c > \\ &= \; 0 = \varepsilon(E). \end{aligned}$$

For K we have

$$\begin{aligned} < K, \det_q > &= \; < K, da > -q < K, bc > \\ &= \; < K, d >< K, a > -q < K, b >< K, c > \\ &= \; q^{-1}q = 1 = \varepsilon(K). \end{aligned}$$

Similar computations can be carried out for F and K^{-1}. □

As a consequence of Lemma 4.3, the algebra morphism ψ from $M_q(2)$ to U_q^* factors through $SL_q(2) = M_q(2)/(\det_q - 1)$. We still denote by ψ the induced morphism of algebras from $SL_q(2)$ into U_q^* and by $< \, , \, >$ the corresponding bilinear form.

Theorem VII.4.4. *The bilinear form* $< u, x > = \psi(x)(u)$ *realizes a duality between the Hopf algebras* U_q *and* $SL_q(2)$.

PROOF. We use the same argument as in the proof of Theorem V.7.6. The only difference lies with the antipodes. We first check Relation (V.7.5) for the generators. Using the condensed matrix form, we have

$$\begin{aligned} < S(E), \begin{pmatrix} a & b \\ c & d \end{pmatrix} > &= \rho(S(E)) = -\rho(E)\rho(K^{-1}) = \begin{pmatrix} 0 & -q \\ 0 & 0 \end{pmatrix} \\ &= < E, \begin{pmatrix} d & -qb \\ -q^{-1}c & a \end{pmatrix} > = < E, \begin{pmatrix} S(a) & S(b) \\ S(c) & S(d) \end{pmatrix} >. \end{aligned}$$

For F we have

$$\begin{aligned} < S(F), \begin{pmatrix} a & b \\ c & d \end{pmatrix} > &= \rho(S(F)) = -\rho(K)\rho(F) = \begin{pmatrix} 0 & 0 \\ -q^{-1} & 0 \end{pmatrix} \\ &= < F, \begin{pmatrix} d & -qb \\ -q^{-1}c & a \end{pmatrix} > = < F, \begin{pmatrix} S(a) & S(b) \\ S(c) & S(d) \end{pmatrix} >. \end{aligned}$$

One proceeds with K and K^{-1} similarly. To conclude, one appeals to Lemma V.7.7. □

VII.5 Duality between $U_q(\mathfrak{sl}(2))$-Modules and $SL_q(2)$-Comodules

Exactly as in the classical case considered in V.7, there is a duality between U_q-modules and $SL_q(2)$-comodules. We have seen in IV.7 that the vector space $k_q[x,y]_n$ of homogeneous elements of degree n of the quantum plane has a natural structure as an $SL_q(2)$-comodule. By duality, the dual vector space $k_q[x,y]_n^*$ has a module structure over the algebra $SL_q(2)^*$, hence over the algebra U_q via the morphism $\varphi : U_q \to SL_q(2)^*$. The following statement gives the structure of $k_q[x,y]_n^*$ as a U_q-module.

Theorem VII.5.1. *The U_q-module $k_q[x,y]_n^*$ is isomorphic to the simple module $V_{1,n}$ of highest weight q^n.*

Thus, the $SL_q(2)$-comodule $k_q[x,y]_n$ corresponds by duality to the U_q-module $V_{1,n}$.

PROOF. We shall show that the linear form on $k_q[x,y]_n$ defined by

$$f(x^i y^{n-i}) = \delta_{ni}$$

is a highest weight vector, with weight q^n, of the U_q-module $k_q[x,y]_n^*$, which implies that $k_q[x,y]_n^*$ contains a submodule isomorphic to the simple module $V_{1,n}$. Since

$$\dim(V_{1,n}) = n+1 = \dim(k_q[x,y]_n^*),$$

we get $k_q[x,y]_n^* \cong V_{1,n}$.

In order to prove that f is a highest weight vector, we need the relation

$$(uf)(x^i y^{n-i}) = < u, a^i c^{n-i} > \tag{5.1}$$

for all $u \in U_q$ and for all i such that $0 \le i \le n$. But this is so since, by definition of f, by III.6, Example 2, by Lemma IV.7.2, and using the abbreviation

$$C_{r,s} = q^{(i-r)s} \begin{pmatrix} i \\ r \end{pmatrix}_{q^2} \begin{pmatrix} n-i \\ s \end{pmatrix}_{q^2}$$

to shorten the formulas, we have

$$\begin{aligned} (uf)(x^i y^{n-i}) &= (u \otimes f)(\Delta_A(x^i y^{n-i})) \\ &= \sum_{r=0}^{i} \sum_{s=0}^{n-i} C_{r,s} < u, a^r b^{i-r} c^s d^{n-i-s} > f(x^{r+s} y^{n-r-s}) \\ &= \sum_{r=0}^{i} \sum_{s=0}^{n-i} C_{r,s} < u, a^r b^{i-r} c^s d^{n-i-s} > \delta_{n,r+s} \\ &= \sum_{r=0}^{i} \sum_{s=0}^{n-i} C_{r,s} < u, a^r b^{i-r} c^s d^{n-i-s} > \delta_{i,r} \delta_{n-i,s} \\ &= < u, a^i c^{n-i} > . \end{aligned}$$

Let us apply Relation (5.1) to K. A straightforward computation yields

$$< K, a^i c^j > = < K, a >^i < K, c >^j = \delta_{j0}\, q^i .$$

Consequently, we have $(Kf)(x^i y^{n-i}) = \delta_{ni}\, q^i = \delta_{ni}\, q^n$, which implies that $Kf = q^n f$.

It remains to prove that $Ef = 0$. This is a consequence of Relation (5.1) applied to E and of the fact that $< E, a^i c^j > = 0$ for all i and j. Let us prove the latter. First, we have $< E, 1 > = \varepsilon(E) = 0$. Next, if $i > 0$ we have by (V.7.2–7.3)

$$\begin{aligned} < E, a^i > &= \varepsilon(a) < E, a^{i-1} > + < E, a >< K, a^{i-1} > \\ &= < E, a^{i-1} > = \ldots = < E, a > = 0. \end{aligned}$$

Similarly, if $j > 0$ we get

$$< E, c^j > = \varepsilon(c) < E, c^{j-1} > + < E, c >< K, c^{j-1} > = 0.$$

Consequently,

$$< E, a^i c^j > = \varepsilon(a)^i < E, c^j > + < E, a^i >< K, c^j > = 0.$$

□

VII.6 Scalar Products on $U_q(\mathfrak{sl}(2))$-Modules

In this section, given any finite-dimensional U_q-module V, we construct a *scalar product*, i.e., a non-degenerate symmetric bilinear form (,) on V such that

$$(xv, v') = (v, T(x)v') \tag{6.1}$$

for all $x \in U_q$ and $v, v' \in V$. The linear map T is the algebra antiautomorphism of U_q defined as follows.

Proposition VII.6.1. *There exists a unique algebra antiautomorphism T of U_q such that $T(E) = KF$, $T(F) = EK^{-1}$, and $T(K) = K$. The automorphism T is also a morphism of coalgebras.*

PROOF. Left to the reader. □

By Theorem 2.2, it is enough to construct a scalar product on any simple U_q-module of the form $V_{\varepsilon,n}$. This is done in the following theorem.

Theorem VII.6.2. *On the simple U_q-module $V_{\varepsilon,n}$ generated by the highest weight vector v, there exists a unique scalar product such that $(v,v) = 1$. If we define the vectors v_i for all $i \ge 0$ by $v_i = F^i v/[i]!$, then they are pairwise orthogonal and we have*

$$(v_i, v_i) = q^{-(n-i-1)i} \begin{bmatrix} n \\ i \end{bmatrix} .$$

PROOF. Let us first assume that there exists a scalar product on $V_{\varepsilon,n}$ such that $(v,v)=1$. Let us show that (v_i,v_j) is necessarily of the prescribed form. By definition and by (6.1) we have

$$(v_i,v_j)=\frac{1}{[i]!}(F^i v,v_j)=\frac{1}{[i]!}(v,T(F)^i v_j)=\frac{1}{[i]!}(v,(EK^{-1})^i v_j).$$

An easy induction on i shows that $(EK^{-1})^i=q^{i(i+1)}K^{-i}E^i$ for any $i>0$. Consequently, the vector $T(F)^i v_j$ is a scalar multiple of $E^i v_j$ which vanishes as soon as $i>j$. Therefore $(v_i,v_j)=0$ if $i>j$. By symmetry, we also have $(v_i,v_j)=0$ if $i<j$.

We need the formula

$$E^i v_j=\varepsilon^i\frac{[n-j+i]!}{[n-j]!}v_{j-i}$$

to compute (v_i,v_i). We have

$$\begin{aligned}(v_i,v_i) &= \frac{1}{[i]!}q^{i(i+1)}(v,K^{-i}E^i v_i)\\ &= \varepsilon^i q^{i(i+1)}\frac{[n]!}{[i]![n-i]!}(v,K^{-i}v)\\ &= q^{i(i+1)-ni}\begin{bmatrix} n\\ i\end{bmatrix}(v,v).\end{aligned}$$

This proves the uniqueness of the scalar product. Let us now prove its existence.

Clearly, there exists a non-degenerate symmetric bilinear form such that

$$(v_i,v_j)=q^{-(n-i-1)i}\begin{bmatrix} n\\ i\end{bmatrix}\delta_{ij}. \tag{6.2}$$

We have to check that it satisfies Relation (6.1). It is enough to check this for $x=E$, F, K and K^{-1}. We shall do this for $x=E$ leaving all other computations to the reader. On the one hand, we have

$$(Ev_i,v_j)=\varepsilon[n-i+1](v_{i-1},v_j)=\varepsilon\delta_{i-1,j}\,q^{-(n-i)(i-1)}\frac{[n]!}{[i-1]![n-i]!}.$$

On the other hand, by (VI.3.1–3.3) and by (6.2), we have

$$\begin{aligned}(v_i,T(E)v_j) &= (v_i,KFv_j)\\ &= \varepsilon q^{n-2(j+1)}[j+1]\,(v_i,v_{j+1})\\ &= \varepsilon\delta_{i,j+1}\,q^{-(n-i-1)i+n-2(j+1)}\,[j+1]\frac{[n]!}{[i]![n-i]!}\\ &= \varepsilon\delta_{i,j+1}\,q^{-(n-i)(i-1)}\frac{[n]!}{[i-1]![n-i]!}=(Ev_i,v_j).\end{aligned}$$

□

VII.7 Quantum Clebsch-Gordan

We now prove a quantum Clebsch-Gordan formula for the finite-dimensional simple U_q-modules. Since

$$V_{\varepsilon,n}\cong V_{\varepsilon,0}\otimes V_{1,n}\cong V_{1,n}\otimes V_{\varepsilon,0}, \tag{7.1}$$

we need give this formula only for the modules $V_{1,n}$, henceforth denoted for simplicity by V_n.

Theorem VII.7.1. *Let $n\geq m$ be two nonnegative integers. There exists an isomorphism of U_q-modules*

$$V_n\otimes V_m\cong V_{n+m}\oplus V_{n+m-2}\oplus\cdots\oplus V_{n-m}.$$

One proves Theorem 7.1 in the same way as Proposition V.5.1. It suffices to check that the module $V_n\otimes V_m$ contains a highest weight vector of weight q^{n+m-2p} for any integer p such that $0\leq p\leq m$.

Lemma VII.7.2. *Let $v^{(n)}$ be a highest weight vector of weight q^n in V_n and $v^{(m)}$ be a highest weight vector of weight q^m in V_m. Let us define $v_p^{(n)}=\frac{1}{[p]!}F^p v^{(n)}$ and $v_p^{(m)}=\frac{1}{[p]!}F^p v^{(m)}$ for all $p\geq 0$. Then,*

$$v^{(n+m-2p)}=\sum_{i=0}^{p}(-1)^i\frac{[m-p+i]![n-i]!}{[m-p]![n]!}q^{-i(m-2p+i+1)}\,v_i^{(n)}\otimes v_{p-i}^{(m)}$$

is a highest weight vector of weight q^{n+m-2p} in $V_n\otimes V_m$.

PROOF. It is clear that $v_i^{(n)}\otimes v_{p-i}^{(m)}$ has weight $q^{n-2i+m-2(p-i)}=q^{n+m-2p}$. Let us prove that $Ev^{(n+m-2p)}=0$. Recall that $\Delta(E)=1\otimes E+E\otimes K$. It follows that

$$\begin{aligned}&Ev^{(n+m-2p)}\\ &= \sum_{i=0}^{p}(-1)^i\frac{[m-p+i]![n-i]!}{[m-p]![n]!}q^{-i(m-2p+i+1)}\,v_i^{(n)}\otimes Ev_{p-i}^{(m)}\\ &\quad+\sum_{i=0}^{p}(-1)^i\frac{[m-p+i]![n-i]!}{[m-p]![n]!}q^{-i(m-2p+i+1)}\,Ev_i^{(n)}\otimes Kv_{p-i}^{(m)}\\ &= \sum_{i=0}^{p}(-1)^i[m-p+i+1]\frac{[m-p+i]![n-i]!}{[m-p]![n]!}q^{-i(m-2p+i+1)}\\ &\qquad\times v_i^{(n)}\otimes v_{p-i-1}^{(m)}\\ &\quad+\sum_{i=0}^{p}(-1)^i[n-i+1]\frac{[m-p+i]![n-i]!}{[m-p]![n]!}q^{-i(m-2p+i+1)+(m-2p+2i)}\end{aligned}$$

$$\begin{aligned}
&\times v_{i-1}^{(n)} \otimes v_{p-i}^{(m)} \\
= & \sum_{i=0}^{p} (-1)^i \Big(\frac{[m-p+i]![n-i+1]!}{[m-p]![n]!} q^{-(i-1)(m-2p+i)} \\
& - \frac{[m-p+i]![n-i+1]!}{[m-p]![n]!} q^{-(i-1)(m-2p+i)} \Big) v_{i-1}^{(n)} \otimes v_{p-i}^{(m)} \\
= & \ 0.
\end{aligned}$$

□

This concludes the proof of Theorem 7.1. We wish to go one step further and address the following problem. We now have two bases of $V_n \otimes V_m$ at our disposal. They are of different natures: the first one, adapted to the tensor product, is the set

$$\{v_i^{(n)} \otimes v_j^{(m)}\}_{0\le i\le n,\, 0\le j\le m} \ ;$$

the second one, formed by the vectors

$$v_k^{(n+m-2p)} = \frac{1}{[k]!} F^k v^{(n+m-2p)}$$

with $0 \le p \le m$ and $0 \le k \le n+m-2p$, is better adapted to the U_q-module structure. Comparing both bases leads us to the so-called *quantum Clebsch-Gordan coefficients*

$$\begin{bmatrix} n & m & n+m-2p \\ i & j & k \end{bmatrix}$$

defined for $0 \le p \le m$ and $0 \le k \le n+m-2p$ by

$$v_k^{(n+m-2p)} = \sum_{0\le i\le n,\, 0\le j\le m} \begin{bmatrix} n & m & n+m-2p \\ i & j & k \end{bmatrix} v_i^{(n)} \otimes v_j^{(m)}. \tag{7.2}$$

The remainder of this section is devoted to a few properties of these coefficients, also called *quantum* $3j$*-symbols* in the physics literature.

Lemma VII.7.3. *Fix p and k. The vector $v_k^{(n+m-2p)}$ is a linear combination of vectors of the form $v_i^{(n)} \otimes v_{p-i+k}^{(m)}$. Therefore, we have*

$$\begin{bmatrix} n & m & n+m-2p \\ i & j & k \end{bmatrix} = 0 \tag{7.3}$$

when $i+j \neq p+k$. We also have the induction relation

$$\begin{bmatrix} n & m & n+m-2p \\ i & j+1 & k+1 \end{bmatrix} = \frac{[j+1]q^{-(n-2i)} + [i]}{[k+1]} \begin{bmatrix} n & m & n+m-2p \\ i & j & k \end{bmatrix}. \tag{7.4}$$

PROOF. This goes by induction on k. The assertion holds for $k = 0$ thanks to Lemma 7.2. Supposing

$$v_k^{(n+m-2p)} = \sum_i \alpha_i\, v_i^{(n)} \otimes v_{p-i+k}^{(m)},$$

we get

$$\begin{aligned}
[k+1]v_{k+1}^{(n+m-2p)} &= F v_k^{(n+m-2p)} \\
&= \sum_i \alpha_i \left(K^{-1} v_i^{(n)} \otimes F v_{p-i+k}^{(m)} + F v_i^{(n)} \otimes v_{p-i+k}^{(m)} \right) \\
&= \sum_i \alpha_i \Big([p-i+k+1] q^{-(n-2i)} v_i^{(n)} \otimes v_{p-i+k+1}^{(m)} \\
&\qquad + [i+1] v_{i+1}^{(n)} \otimes v_{p-i+k}^{(m)} \Big) \\
&= \sum_i \alpha_i \left([p-i+k+1] q^{-(n-2i)} + [i] \right) v_i^{(n)} \otimes v_{p-i+k+1}^{(m)}.
\end{aligned}$$

The rest follows easily. □

We now prove some orthogonality relations for the quantum Clebsch-Gordan coefficients, which will allow us to express the basis $\{v_i^{(n)} \otimes v_j^{(m)}\}_{i,j}$ in terms of the basis $\{v_k^{(n+m-2p)}\}_{p,k}$. Let us equip V_n and V_m with the scalar product $(\ ,\ )$ defined in Section 6. Consider the symmetric bilinear form on $V_n \otimes V_m$ given by

$$(v_1 \otimes v_1', v_2 \otimes v_2') = (v_1, v_2)(v_1', v_2') \tag{7.5}$$

where $v_1, v_2 \in V_n$ and $v_1', v_2' \in V_m$.

Lemma VII.7.4. *The symmetric bilinear form (7.5) is non-degenerate and the basis $\{v_i^{(n)} \otimes v_j^{(m)}\}_{i,j}$ is orthogonal. Furthermore, for all $x \in U_q$ and all $w_1, w_2 \in V_n \otimes V_m$, we have*

$$(xw_1, w_2) = (w_1, T(x)w_2).$$

PROOF. The first two assertions are clear. Let us prove the last one. If $w_1 = v_1 \otimes v_1'$ and $w_2 = v_2 \otimes v_2'$, we have

$$\begin{aligned}
(xw_1, w_2) &= (\Delta(x)(v_1 \otimes v_1'), v_2 \otimes v_2') \\
&= \sum_{(x)} (x'v_1, v_2)(x''v_1', v_2') \\
&= \sum_{(x)} (v_1, T(x')v_2)(v_1', T(x'')v_2') \\
&= \sum_{(T(x))} (v_1, T(x)'v_2)(v_1', T(x)''v_2') \\
&= (w_1, T(x)w_2),
\end{aligned}$$

using the fact that T is an automorphism of coalgebras (see Proposition 6.1). □

The second basis of $V_n \otimes V_m$ is orthogonal too.

Proposition VII.7.5. (a) *The basis* $\{v_k^{(n+m-2p)}\}_{0\leq p\leq m,\, 0\leq k\leq n+m-2p}$ *is orthogonal.*

(b) *Fix integers p, q, k, ℓ. We have the following orthogonality relations:*

$$0 = \sum_{i,j} q^{-i(n-i-1)-j(m-j-1)} \begin{bmatrix} n \\ i \end{bmatrix} \begin{bmatrix} m \\ j \end{bmatrix} \times \begin{bmatrix} n & m & n+m-2p \\ i & j & k \end{bmatrix} \begin{bmatrix} n & m & n+m-2q \\ i & j & \ell \end{bmatrix}$$

when $p \neq q$ or $k \neq \ell$, and

$$\sum_{i,j} q^{-i(n-i-1)-j(m-j-1)} \begin{bmatrix} n \\ i \end{bmatrix} \begin{bmatrix} m \\ j \end{bmatrix} \begin{bmatrix} n & m & n+m-2p \\ i & j & k \end{bmatrix}^2 = q^{-k(n+m-2p-k-1)} \begin{bmatrix} n+m-2p \\ k \end{bmatrix}.$$

(c) *Given i and j, we have*

$$v_i^{(n)} \otimes v_j^{(m)} = q^{-i(n-i-1)-j(m-j-1)} \begin{bmatrix} n \\ i \end{bmatrix} \begin{bmatrix} m \\ j \end{bmatrix} \times \sum_{p=0}^{m} \sum_{k=0}^{n+m-2p} q^{k(n+m-2p-k-1)} \frac{\begin{bmatrix} n & m & n+m-2p \\ i & j & k \end{bmatrix}}{\begin{bmatrix} n+m-2p \\ k \end{bmatrix}} v_k^{(n+m-2p)}.$$

PROOF. (a) Arguing as in the proof of Theorem 6.2, one shows that

$$(v_k^{(n+m-2p)}, v_\ell^{(n+m-2p)}) = 0$$

whenever $k \neq \ell$. Let us examine the case when $p \neq q$. Let us first show that the highest weight vectors $v^{(n+m-2p)}$ and $v^{(n+m-2q)}$ are orthogonal. In fact, Lemma 7.2 implies that $(v^{(n+m-2p)}, v^{(n+m-2q)})$ can be written

$$\begin{aligned}(v^{(n+m-2p)}, v^{(n+m-2q)}) &= \sum_{i,j} \alpha_i\beta_j (v_i^{(n)}, v_j^{(n)})(v_{p-i}^{(m)}, v_{q-j}^{(m)}) \\ &= \sum_{i} \alpha_i\beta_i (v_i^{(n)}, v_i^{(n)})(v_{p-i}^{(m)}, v_{q-i}^{(m)}),\end{aligned}$$

which is zero because $p - i \neq q - i$. It remains to show that

$$(v_k^{(n+m-2p)}, v_\ell^{(n+m-2q)}) = 0$$

when $k, \ell > 0$.

By symmetry, it is enough to consider the case $k \geq \ell$. We have

$$\begin{aligned}(v_k^{(n+m-2p)}, v_\ell^{(n+m-2q)}) &= \gamma\,(F^k v^{(n+m-2p)}, v_\ell^{(n+m-2q)}) \\ &= \gamma'\,(v^{(n+m-2p)}, E^k v_\ell^{(n+m-2q)})\end{aligned}$$

for some scalars γ and γ'. Now, if $k \geq \ell$, the vector $E^k v_\ell^{(n+m-2q)}$ is zero or is a scalar multiple of the highest weight vector $v^{(n+m-2q)}$, which brings us back to a previous case.

(b) Let us compute $(v_k^{(n+m-2p)}, v_\ell^{(n+m-2q)})$. It is equal to

$$\begin{aligned}&\sum_{i+j=p+k}\ \sum_{r+s=q+\ell} \begin{bmatrix} n & m & n+m-2p \\ i & j & k \end{bmatrix} \begin{bmatrix} n & m & n+m-2q \\ r & s & \ell \end{bmatrix} \times (v_i^{(n)}, v_r^{(n)})(v_j^{(m)}, v_s^{(m)}) \\ &= \sum_{i+j=p+k} \begin{bmatrix} n & m & n+m-2p \\ i & j & k \end{bmatrix} \begin{bmatrix} n & m & n+m-2q \\ i & j & \ell \end{bmatrix} \times (v_i^{(n)}, v_i^{(n)})(v_j^{(m)}, v_j^{(m)}) \\ &= \sum_{i+j=p+k} q^{-i(n-i-1)-j(m-j-1)} \begin{bmatrix} n \\ i \end{bmatrix} \begin{bmatrix} m \\ j \end{bmatrix} \begin{bmatrix} n & m & n+m-2p \\ i & j & k \end{bmatrix} \times \begin{bmatrix} n & m & n+m-2q \\ i & j & \ell \end{bmatrix}.\end{aligned}$$

On the other hand, we have

$$(v_k^{(n+m-2p)}, v_\ell^{(n+m-2q)}) = \delta_{pq}\delta_{k\ell}\, q^{-k(n+m-2p-k-1)} \begin{bmatrix} n+m-2p \\ k \end{bmatrix}.$$

(c) We have $v_i^{(n)} \otimes v_j^{(m)} = \sum_{p=0}^{m} \sum_{k=0}^{n+m-2p} \gamma_{pk}\, v_k^{(n+m-2p)}$ for some coefficients γ_{pk}. Therefore,

$$\begin{aligned}\gamma_{pk}(v_k^{(n+m-2p)}, v_k^{(n+m-2p)}) &= (v_i^{(n)} \otimes v_j^{(m)}, v_k^{(n+m-2p)}) \\ &= \begin{bmatrix} n & m & n+m-2p \\ i & j & k \end{bmatrix} (v_i^{(n)}, v_i^{(n)})(v_j^{(m)}, v_j^{(m)}).\end{aligned}$$

Applying (6.2), one gets the desired explicit expression for γ_{pk}. □

For more details on the quantum Clebsch-Gordan coefficients, see [KR89] [KK89] [Vak89] where they are expressed in terms of *q-Hahn polynomials*, i.e., of certain orthogonal q-hypergeometric series (see also [GR90], Chap. 7). Koelink-Koornwinder and Vaksman showed that the orthogonality relations of the q-Hahn polynomials were equivalent to the orthogonality relations of the quantum Clebsch-Gordan coefficients. The corresponding property for the classical Clebsch-Gordan coefficients was known already (see [Koo90]).

VII.8 Exercises

1. Compute $S(E^iF^jK^\ell)$ in U_q.

2. Let x be an element of U_q. Prove successively that

   (a) x is grouplike if and only if x is of the form $x = K^n$;

   (b) if $\Delta(x) = 1 \otimes x + x \otimes K$ and $\varepsilon(x) = 0$, then x is a linear combination of E and of KF;

   (c) if $\Delta(x) = K^{-1} \otimes x + x \otimes 1$ and $\varepsilon(x) = 0$, then x is a linear combination of F and of EK^{-1};

   (d) if $\Delta(x) = 1 \otimes x + x \otimes K^{-1}$, then $x = 0$.

3. Use Exercise 2 to show that there exists an isomorphism of Hopf algebras from U_q onto $U_{q'}$ if and only if $q' = \pm q^{\pm 1}$, and that any Hopf algebra automorphism φ of U_q is of the form

$$\varphi(E) = \alpha E, \quad \varphi(F) = \alpha^{-1}F, \quad \varphi(K) = K$$

   where α is a non-zero scalar.

4. (*Hopf $*$-algebra structures on U_q*) We use the concepts introduced in IV.8.

   (a) Prove that U_q is a Hopf $*$-algebra if and only if q^2 is a real number or q is a complex number of modulus 1.

   (b) Check that the following formulas determine five Hopf $*$-algebra structures on U_q:

   (i) $E^* = E$, $F^* = F$, and $K^* = K$ if $|q| = 1$;

   (ii) $E^* = KF$, $F^* = EK^{-1}$, and $K^* = K$ if q is real > 0;

   (iii) $E^* = -KF$, $F^* = -EK^{-1}$, and $K^* = K$ if q is real < 0;

   (iv) $E^* = iKF$, $F^* = iEK^{-1}$, and $K^* = K$ if $q = \lambda i$ with λ real > 0;

   (v) $E^* = -iKF$, $F^* = -iEK^{-1}$, and $K^* = K$ if $q = \lambda i$ with λ real < 0.

   (c) Show that any Hopf $*$-algebra structure on U_q is equivalent to one of the previous five ones (Hint: use Exercise 2).

5. Given a Hopf $*$-algebra structure on U_q and a U_q-module V, define a Hermitian scalar product as a definite positive Hermitian form $(\ ,\ )$ such that $(xv, v') = (v, x^*v')$ for all $x \in U_q$ and $v, v' \in V$. Determine all Hermitian scalar products on the simple module $V_{\varepsilon,n}$.

6. Prove that there exists a U_q-linear isomorphism between the simple module $V_{\varepsilon,n}$ and its dual module.

VII.9 Notes

The Hopf algebra structure of $U_q(\mathfrak{sl}(2))$ is due to Sklyanin [Skl85]. The Drinfeld-Jimbo algebras $U_q(\mathfrak{g})$ also have a non-commutative, non-cocommutative Hopf algebra structure. In the cases A, D, E considered in VI.7, it is given on the generators $(E_i, F_i, K_i)_{1\leq i\leq \ell}$ by

$$\Delta(E_i) = 1 \otimes E_i + E \otimes K_i, \quad \Delta(F_i) = K_i^{-1} \otimes F_i + F_i \otimes 1, \quad \Delta(K_i) = K_i \otimes K_i,$$

$$\varepsilon(E_i) = \varepsilon(F_i) = 0, \quad \varepsilon(K_i) = 1,$$

and

$$S(E_i) = -E_iK_i^{-1}, \quad S(F_i) = -K_iF_i, \quad S(K_i) = K_i^{-1}.$$

In this chapter we adopted the conventions of Takeuchi [Tak92c] rather than those of Drinfeld and Jimbo. In the special case $\mathfrak{g} = \mathfrak{sl}(2)$, Takeuchi's conventions allow U_q to act on the quantum plane of Chapter IV. Following Drinfeld [Dri87], Takeuchi [Tak92c] [Tak92b] also showed the existence of a duality between $U_q(\mathfrak{sl}(n))$ and the Hopf algebra $SL_q(n)$ of IV.9, embedding the latter into the restricted dual of $U_q(\mathfrak{sl}(n))$.

The semisimplicity of the finite-dimensional U_q-modules is due to Rosso [Ros88]. We followed his proof closely.

For more details on quantum Clebsch-Gordan coefficients, read [KR89] [KK89] [Koo90] [Vak89]. For the Hopf $*$-algebra structures on U_q (determined in Exercise 4), see [MMN$^+$90].

Chapter X

Knots, Links, Tangles, and Braids

We now embark into a topological digression which will lead us into the world of knots. The reason for the presence of this chapter in a book devoted to quantum groups is the close relationship between the newly discovered invariants of links (such as the celebrated Jones polynomial) and R-matrices. This relationship will become more precise in Chapter XII. In this one we proceed to describe several classes of one-dimensional submanifolds of the three-dimensional space $\mathbf{R}^3$, such as knots, links, tangles, and braids. Since there are excellent textbooks on knot theory, we shall not prove all assertions that can be found elsewhere. Nevertheless, all results pertaining to the matter of this book, namely those connecting topological problems with the algebra of quantum groups, will be proved in detail.

After defining knots and links in $\mathbf{R}^3$, we recall the classical problem of their classification up to isotopy. Traditionally, one approaches this problem by constructing algebraic isotopy invariants. One major step in this direction was undertaken in the 1920's by Alexander, who associated a polynomial to each isotopy class of oriented links. The Alexander polynomial was used to distinguish many links and has been a powerful tool in knot theory since.

In the summer of 1984 Vaughan Jones found a different one-variable polynomial which distinguished knots that the Alexander polynomial could not distinguish [Jon85]. Shortly after, a new invariant appeared, the so-called Jones-Conway polynomial, which is a two-variable generalization of both the Alexander and the Jones polynomials. Another aim of this chapter is to establish the existence and the main properties of the Jones-Conway polynomial.

X.1 Knots and Links

Let us start with some vocabulary from general topology. The only topological spaces considered here are the real Euclidean vector spaces $\mathbf{R}^n$ with their standard topology as well as their subsets and quotients with the induced topologies.

A continuous map f from a subset U of $\mathbf{R}^m$ to a subset X of $\mathbf{R}^n$ is *piecewise-linear* if there exists a finite partition $(U_i)_i$ of U such that the n components of the restriction of f to any U_i are maps of the form $(z_1, \ldots, z_m) \mapsto a_0 + a_1 z_1 + \cdots a_m z_m$ where $a_0, a_1, \ldots, a_m$ are real numbers.

Let X be a convex topological subspace of the Euclidean space $\mathbf{R}^3$. In the sequel, X will be either $\mathbf{R}^3$, $\mathbf{R}^2$, $\mathbf{R}^2 \times [0,1]$, or $\mathbf{R} \times [0,1]$. Given a finite sequence $(M_1, \ldots, M_n)$ of points in X, we denote by $[M_1, \ldots, M_n]$ [resp. $]M_1, \ldots, M_n[$] their closed [resp. open] convex envelope, i.e., the set of all points of the form $\lambda_1 M_1 + \cdots + \lambda_n M_n$ where $(\lambda_1, \ldots, \lambda_n)$ is a sequence of real numbers ≥ 0 [resp. > 0] such that $\lambda_1 + \cdots + \lambda_n = 1$.

Definition X.1.1. *A polygonal arc L in X is the union*

$$L = \bigcup_{i=1}^{n-1} [M_i, M_{i+1}]$$

of a finite number of segments such that $]M_i, M_{i+1}[\cap]M_j, M_{j+1}[= \emptyset$ if $i \neq j$. The points $M_1, \ldots, M_n$ are called the vertices of the polygonal arc and the segments $[M_i, M_{i+1}]$ are its edges. We say that the polygonal arc is simple if the points $M_1, \ldots, M_{n-1}$ are all distinct. The polygonal arc L is closed if $M_1 = M_n$; in this case, we say that the boundary ∂L is empty. If $M_1 \neq M_n$, we set $\partial L = \{M_1, M_n\}$; the point M_1 is the origin of the simple polygonal arc L and M_n is its endpoint.

By ordering the vertices of L we define an orientation on L. It will be materialized in the figures by arrows on the edges such that on the edge $[M_i, M_{i+1}]$ the arrow points to M_{i+1}.

Definition X.1.2. *A link L in X is the union of a finite number m of pairwise disjoint simple closed polygonal arcs in X. The closed arcs are called the connected components of L. The integer m is called the order of the link. A knot is a link of order 1.*

A link is oriented by giving an orientation to each of its connected components. In the sequel we consider only oriented links. Following Reidemeister [Rei32], we define a combinatorial operation Δ on links. We assume X to be $\mathbf{R}^3$ until the end of this section.

Definition X.1.3. (a) *Let L be a link in X and M_i, M_{i+1} two consecutive vertices in a connected component of L. Given a point N in X such that $N \notin L$, $M_i \notin [N, M_{i+1}]$, $M_{i+1} \notin [M_i, N]$, and*

$$[M_i, N, M_{i+1}] \cap L = [M_i, M_{i+1}],$$

we denote by L' the link

$$L' = (L \setminus [M_i, M_{i+1}]) \cup [M_i, N] \cup [N, M_{i+1}].$$

We say that L' is obtained from L by a Δ-operation.

(b) *Two links L and L' are combinatorially equivalent — we write this $L \sim_c L'$ — if there exist links $L = L_0, L_1, \ldots, L_k = L'$ such that for all i, one of the two links L_i, L_{i+1} is obtained from the other one by a Δ-operation.*

The relation $\sim_c$ is an equivalence relation: it is the equivalence relation generated by the Δ-operations.

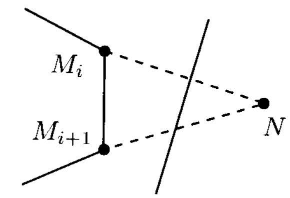

Figure 1.1. A Δ-operation

It is also possible to deform links continuously. This leads us to the concept of isotopy.

Definition X.1.4. (a) *An isotopy of X is a piecewise-linear map h from $[0,1] \times X$ to X such that, for any $t \in I$, the mapping $h(t, -)$ is a homeomorphism of X, and $h(0, -)$ is the identity of X.*

(b) *Two links L and L' are isotopic — we write $L \sim_i L'$ — if there exists an orientation-preserving isotopy h of X such that $h(1, L) = L'$.*

Lemma X.1.5. *Isotopy is an equivalence relation for links.*

Proof. Let L, L', and L'' be links. (a) Set $h(t, -) = \mathrm{id}_X$ for all $t \in I$. It is clear that h is an isotopy between L and itself: $L \sim_i L$.

(b) Let us suppose that $L \sim_i L'$ via an isotopy h. Let $h'(t, -) = h(t, -)^{-1}$ be the inverse homeomorphism. It is an isotopy between L' and L. Hence $L' \sim_i L$.

(c) If, moreover, $L' \sim_i L''$ via an isotopy h', then

$$h''(t, -) = \begin{cases} h(2t, -) & \text{if} \quad 0 \leq t \leq 1/2 \\ h'(2t - 1, -) \circ h(1, -) & \text{if} \quad 1/2 \leq t \leq 1 \end{cases}$$

defines an isotopy between L and L''. In other words, the relation $\sim_i$ is transitive. □

We now have two equivalence relations on links. The following proposition identifies them with each other.

Proposition X.1.6. *Let L and L' be links in $\mathbf{R}^3$. Then*

$$L \sim_c L' \iff L \sim_i L'.$$

The reader will find a proof of this result in [BZ85], Prop. 1.10. As a consequence, we shall suppress the subscripts i and c from the symbols $\sim_i$ and $\sim_c$ and henceforth speak of isotopic or equivalent links.

We end this section with a definition of a trivial link.

Definition X.1.7. *A link of order m in $\mathbf{R}^3$ is trivial if it is isotopic to the union of m disjoint triangles in a plane. A trivial knot is a trivial link of order* 1.

We denote a trivial link of order m by

$$O^{\otimes m} = OO \cdots O \qquad (m \text{ times}).$$

Trivial links of the same order, but with different orientations, are always isotopic. Therefore we need not specify the orientation of a trivial link.

X.2 Classification of Links up to Isotopy

The fundamental problem in knot theory is to classify all links in $\mathbf{R}^3$ up to isotopy. In particular, one would like to have convenient criteria for two links to be isotopic or for a link to be trivial. This is a difficult problem.

A classical way of approching this problem is to assign to each link L an algebraic object I_L such that $I_L = I_{L'}$ whenever L and L' are equivalent. Such a function I is called an *isotopy invariant* for links. Let us give some examples.

(a) (*The order*) It is clear that the number of connected components of a link is preserved by an isotopy or a Δ-operation. Therefore the order of a link, i.e., the number of its connected components, is an isotopy invariant. However, this invariant is weak since it is clearly insensitive to how much a link is "knotted". Indeed all knots have the same order and nevertheless there exists non-trivial knots such as the right-handed trefoil knot drawn in Figure 2.1.

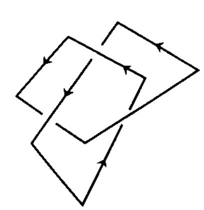

Figure 2.1. A right-handed trefoil knot

(b) (*The linking number*) This is a more refined invariant which dates back to Gauss. Let us consider two connected components L_1 and L_2 of a link L. Consider a diagram of L (to be defined in Section 3). It shows crossings of L_1 and of L_2. We associate to each crossing P an integer $\varepsilon(P) = \pm 1$ defined as in Figure 2.2.

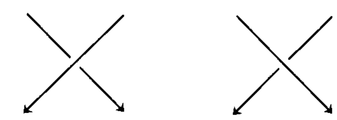

Figure 2.2. The linking number

Then the linking number of the components L_1 and L_2 is the integer

$$\mathrm{lk}(L_1, L_2) = \frac{1}{2} \sum_P \varepsilon(P)$$

where P runs over all crossings of L_1 and L_2. This number does not depend on the projection and is an isotopy invariant for links of order 2. For instance, we have $\mathrm{lk}(OO) = 0$ for the trivial link with two components, and $\mathrm{lk}(H) = 1$ for the Hopf link H drawn in Figure 2.3. It follows that the Hopf link is not trivial.

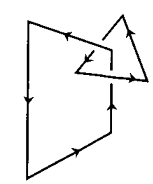

Figure 2.3. The Hopf link

(c) (*The fundamental group of a link*) Define $\pi(L) = \pi_1(\mathbf{R}^3 \setminus L)$ as the ndamental group of the complement of the link in $\mathbf{R}^3$ (the definition f the fundamental group is given in the Appendix to this chapter). For e trivial knot, the group $\pi(O)$ is isomorphic to $\mathbf{Z}$. More generally, the oup of the trivial link of order m is isomorphic to the free group F_m on generators. By the very definition of isotopy, the fundamental group of link is an isotopy invariant. It is a very powerful invariant as one can e from a theorem of Dehn's which asserts that a link L of order m is ivial if and only if $\pi(L) = F_m$. In general, the group of a link is non-elian. Though it is possible to give a presentation of $\pi(L)$ by generators d relations from a plane projection of L, it is very difficult to use this presentation, for instance, to decide whether L is isotopic to another given link. For more details, see [Bir74][BZ85].

(d) (*Alexander and Conway polynomials*) In 1928 Alexander [Ale28] constructed for each link L a polynomial $\Delta_L \in \mathbf{Z}[t, t^{-1}]$ defined only up to $\pm$ a power of t, which he proved to be an isotopy invariant. This invariant was a very efficient tool for distinguishing links that were not equivalent. In 1970 Conway [Con70] showed that a suitable normalization of the Alexander polynomial was of the form $\Delta_L(t) = \nabla_L(t - t^{-1})$ where $\nabla_L(z)$ is a polynomial, now called the *Conway polynomial*, in $\mathbf{Z}[z]$. Moreover, the Conway polynomial has a simple characterization in terms of the skein relations that will be described in Section 4.

X.3 Link Diagrams

The simplest way to describe a link in $\mathbf{R}^3$ is to represent it by a planar diagram. We have already used this technique for the figures of Sections 1–2. We now give a definition of what we mean by a link diagram. We first need the notion of a regular projection.

Definition X.3.1. (a) *A link projection* Π *is the union of a finite number of closed polygonal arcs in* $\mathbf{R}^2$ *such that no vertex lies in the interior of any edge. A crossing point of* Π *is a point of the link projection lying in the interior of at least two edges. The order of a crossing point* P *is the number of distinct edges in the interior of which* P *lies.*

(b) *A link projection is regular if each crossing point is of order exactly* 2.

It is not difficult to see that a crossing point cannot be a vertex, and that a link projection has only finitely many crossing points. The ordering of each component will be represented by arrows on the edges of the projection of the link following the rule given in Section 1.

Let Π be a *regular* link projection in the plane. Given a crossing point P we may consider the set E_P consisting of the two edges on which P lies. A priori, the set E_P is unordered. This brings us to the following definition.

Definition X.3.2. *A link diagram is a regular link projection in* $\mathbf{R}^2$ *for which all sets* E_P *(indexed by the crossing points* P*) are ordered. Given a crossing point* P*, the first edge of the set* E_P *with respect to the ordering is called the overcrossing edge whereas the other edge is called the undercrossing edge.*

Observe that an overcrossing edge for a crossing point may be undercrossing for another crossing point. Changing the ordering in some sets E_P will be called a change of crossings. If a regular link projection has m crossing points, then clearly there are 2^m link diagrams with the same underlying link projection.

We represent a link diagram by a drawing of the regular link projection in which the undercrossing edges are interrupted in the neighbourhood of the crossings (as in Figures 2.1 and 2.3). From such a picture we observe that any link diagram defines a link in $\mathbf{R}^3$ by letting any undercrossing edge pass under the corresponding overcrossing edge in the neighbourhood of the crossing point. This link is defined only up to isotopy. There is no reason — and in general it is false — why two link diagrams differing by a change of crossings should define equivalent links. Nevertheless, the following should be noted.

Lemma X.3.3. *Any link diagram may be turned after appropriate changes of crossings into a link diagram representing a trivial link in* $\mathbf{R}^3$.

PROOF. Consider a link diagram. Pick a vertex and start moving along the link, leaving a trail of red paint on the edges. At each crossing point, make the red edge into an overcrossing edge unless the other edge is already red, in which case the first edge is made into an undercrossing one. Apply this procedure to each connected component. The resulting link diagram (obtained from the original ones by a series of changes of crossings) represents a trivial link. □

The obvious question is now: Can any link in $\mathbf{R}^3$ be represented by a link diagram, at least up to isotopy? The answer is yes and provided by the following proposition where we fix a linear projection π_0 of the space $\mathbf{R}^3$ on the plane $\mathbf{R}^2$.

Proposition X.3.4. *Any link in* $\mathbf{R}^3$ *is equivalent to a link* L *whose image* $\pi_0(L)$ *is a regular link projection.*

PROOF. We sketch the proof. For details, see [BZ85]. Let L be a link in $\mathbf{R}^3$. Consider the set S of all possible linear projections of $\mathbf{R}^3$ onto a fixed plane. Given a projection π of S, there exists a homeomorphism h of $\mathbf{R}^3$ such that $\pi_0(h(L)) = \pi(L)$. It is therefore enough to show that the subset S_{reg} of those projections π of S such that $\pi(L)$ is a regular link projection is not empty. Now S is in bijection with $\mathbf{R}^2$. Therefore we can transport the topology of $\mathbf{R}^2$ onto S. What we shall actually prove, is that S_{reg} is dense in S for this topology.

Let π be an element of $S \setminus S_{reg}$. Then in the projection $\pi(L)$ we may have the following singularities: some crossing point may be of order ≥ 3 or some vertex may sit in the interior of some edge. This happens when the direction of the projection π passes through three edges or when it passes through a vertex and an edge. In the first case, the direction sweeps over a portion of a quadric; this projects to a part of a conic. In the second case, it determines by projection a segment of the plane. Identifying S with $\mathbf{R}^2$, we see that $S \setminus S_{reg}$ is contained in a finite number of straight lines and conics of the plane. Therefore S_{reg} is dense in S. □

Having expressed the problem of classification of links in $\mathbf{R}^3$ in purely two-dimensional terms, we now ask: When do two link diagrams represent isotopic links? Before we answer this important question, let us again follow Reidemeister by introducing the four transformations on link diagrams shown in Figures 3.1–3.4. These transformations are also called *Reidemeister moves*.

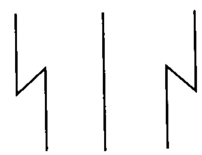

Figure 3.1. Reidemeister move (0)

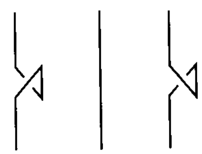

Figure 3.2. Reidemeister move (I)

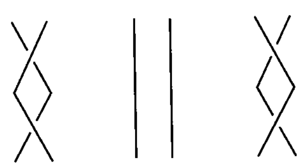

Figure 3.3. Reidemeister move (II)

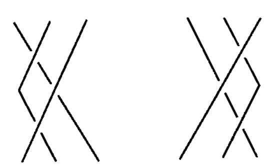

Figure 3.4. Reidemeister move (III)

Applying Transformation (0) to a link diagram means that one modifies it locally by substituting one of the drawings of the figure of Transformation (0) by another one without touching the rest of the link diagram. Similarly for the other Transformations. Figures 3.5–3.8 show that Transformations (0), (I), (II), and (III) are obtained by projection of Δ-operations. Consequently, applying these transformations to link diagrams does not change the isotopy class of the link in $\mathbf{R}^3$.

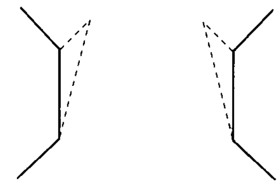

Figure 3.5. (0 projected)

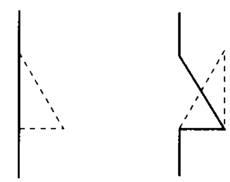

Figure 3.6. (I projected)

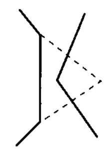

Figure 3.7. (II projected)

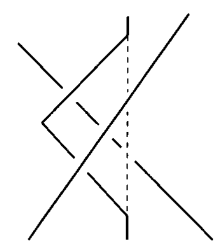

Figure 3.8. (III projected)

Reidemeister Transformations are sufficient in a sense we shall make recise below after we defined the following additional concepts. Two link iagrams Π, Π' are *isotopic* if there exists an isotopy h of $\mathbf{R}^2$ (see Defiition 1.4) such that $h(1, \Pi) = \Pi'$. By this we mean that the underlying rojections are isotopic in the plane and that the orders of the sets E_P are reserved in the course of the isotopy. Two isotopic link diagrams represent otopic links in $\mathbf{R}^3$.

Introducing the *height* as the second projection of $\mathbf{R}^2$ onto $\mathbf{R}$, we define a *neric link diagram* to be a link diagram for which any two distinct vertices have different heights. In particular, a generic link diagram cannot have a horizontal edge, i.e., an edge parallel to $\mathbf{R} \times \{0\}$. A *generic isotopy* between two generic link diagrams Π, Π' is an isotopy of $\mathbf{R}^2$ such that $h(1, \Pi) = \Pi'$ and such that $h(t, \Pi)$ is a generic diagram for all $t \in [0,1]$. The following statement is a criterion for generic diagrams to be isotopic as diagrams.

Lemma X.3.5. *Two generic diagrams are isotopic if and only if they are obtained from one another by a finite number of operations belonging to the following set:*

(A) *a generic isotopy,*

(B) *an isotopy interchanging the order of the vertices with respect to the height,*

(C) *a Reidemeister Transformation* (0), *and*

(D) *an isotopy in the neighbourhood of a local maximum as depicted in Figure* 3.9 *and its images under reflection in the plane of the page, in a horizontal line and in a vertical line.*

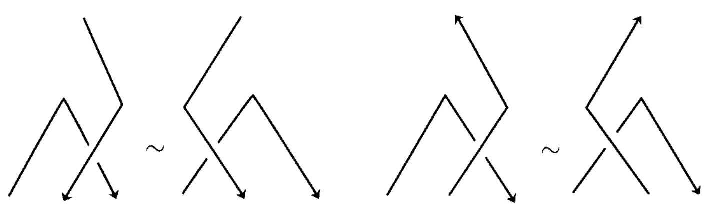

Figure 3.9. An isotopy in the neighbourhood of a local maximum

We replace Transformation (D) of the previous lemma by another set of operations that will turn out to be more adequate in Chapter XII.

Lemma X.3.6. *Two generic diagrams are isotopic if and only if they are obtained from one another by a finite number of the following operations:*

(A) *a generic isotopy,*

(B) *an isotopy interchanging the order of the vertices with respect to the height,*

(C) *a Reidemeister Transformation* (0), *and*

(E) *an isotopy in the neighbourhood of a crossing point as shown in Figure* 3.10 *and its images under reflection in the plane of the page.*

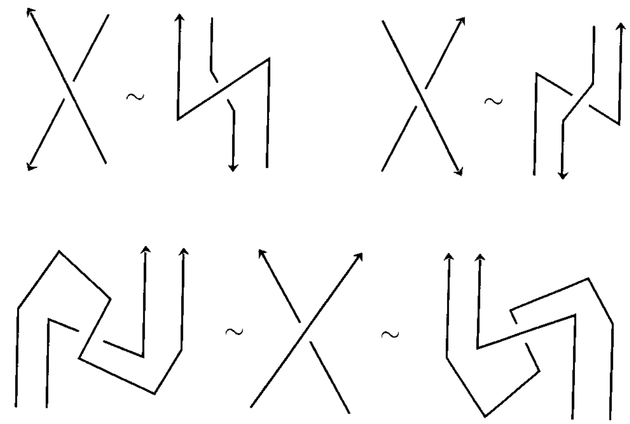

Figure 3.10. An isotopy in the neighbourhood of a crossing point

PROOF. It is clear that the operations in (E) are obtained by isotopies of diagrams. By Lemma 3.5 they follow from (A), (B), (C), and (D).

It remains to prove that Transformation (D) is a consequence of Transformations (A), (B), (C), and (E). Figures 3.11–3.12 below give a proof of this fact for the two operations represented in Figure 3.9.

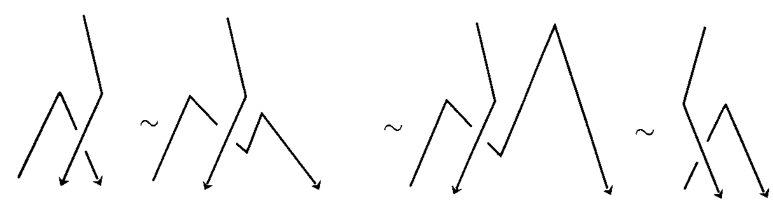

Figure 3.11.

In Figure 3.11 the first operation is of type (C), the second one of type (A) and (B) while the third one is of type (E).

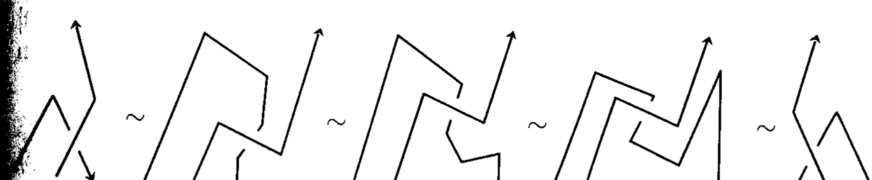

Figure 3.12.

In Figure 3.12 the first and fourth operations are of type (E), the second one of type (C), and the third one of type (A) and (B). Reflecting the previous transformations with respect to the plane of the paper or with respect to a vertical line takes care of their images under these reflections. As for the reflections with respect to a horizontal line (they involve local minima), our assertion follows from the set of operations of Figure 3.13 where the first and last ones are Transformations (C), the middle one is authorized by Figure 3.11, and the remaining ones are of type (A) and (B). □

Figure 3.13.

We return to the problem of representing links in $\mathbf{R}^3$ by (generic) link diagrams. Since moving vertices up and down locally allows us to turn any link diagram into a generic one, we see that Proposition 3.4 implies that any link in $\mathbf{R}^3$ is equivalent to a link L whose projection $\pi_0(L)$ is a generic diagram.

Reidemeister [Rei32] proved the following important theorem which expresses isotopy classes of links in $\mathbf{R}^3$ in terms of purely two-dimensional link diagrams.

Theorem X.3.7. *Two generic link diagrams represent equivalent links in* $\mathbf{R}^3$ *if and only if one is obtained from the other by a finite sequence of Reidemeister Transformations* (I), (II), (III), *and of isotopies of diagrams.*

X.4 The Jones-Conway Polynomial

We now construct the Jones-Conway polynomial. This is an isotopy invariant of oriented links satisfying what knot theorists call "skein relations". In order to formulate these relations, we introduce the concept of a Conway triple. This concept already appears in [Ale28] p. 301, but Conway [Con70] was the first one to observe that it could characterize knot invariants such as the Alexander or the Conway polynomials.

Definition X.4.1. *A triple* (L_+, L_-, L_0) *of oriented links in* $\mathbf{R}^3$ *is a Conway triple if they can be represented by link diagrams* D_+, D_-, D_0 *which coincide outside a disk in* $\mathbf{R}^2$ *and which are respectively isotopic to* X_+, X_- *and* $\downarrow\downarrow$ *inside the disk.*

The diagrams X_+ and X_- are represented in Figure 4.1.

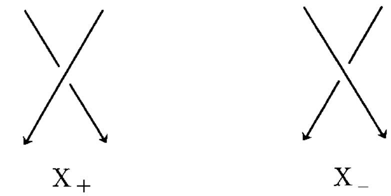

Figure 4.1.

We now state the main theorem of this chapter.

Theorem X.4.2. *There exists a unique map* $L \mapsto P_L$ *from the set of all oriented links in* $\mathbf{R}^3$ *to the ring* $\mathbf{Z}[x, x^{-1}, y, y^{-1}]$ *of two-variable Laurent polynomials such that*
(i) *if* $L \sim L'$, *then* $P_L = P_{L'}$,
(ii) *the value of* P *on the trivial knot is* 1, *and*
(iii) *whenever* (L_+, L_-, L_0) *is a Conway triple, we have*

$$xP_{L_+} - x^{-1}P_{L_-} = yP_{L_0}. \tag{4.1}$$

The invariant P_L is called the *Jones-Conway polynomial*, or the *two-variable Jones polynomial*, or the *Homfly polynomial* (after the initials of the six authors of [FYH+85]) of the link L. Relations (4.1) are called *skein relations*. The polynomial $\nabla_L \in \mathbf{Z}[z]$ that Conway [Con70] devised as a variant of the Alexander polynomial is characterized by Properties (i)–(ii) of Theorem 4.2 along with the skein relation

$$\nabla_{L_+} - \nabla_{L_-} = z\nabla_{L_0}. \tag{4.2}$$

Similarly, the polynomial $V_L \in \mathbf{Z}[t^{1/2}, t^{-1/2}]$ which was discovered in 1984 by Vaughan Jones [Jon85][Jon87] is characterized by Properties (i)–(ii) and by the skein relation

$$t^{-1}V_{L_+} - tV_{L_-} = \left(\sqrt{t} - \frac{1}{\sqrt{t}}\right)V_{L_0}. \tag{4.3}$$

As a consequence of Theorem 4.2, the Conway polynomial and the Jones polynomial exist, and they are related to the two-variable Jones-Conway polynomial by

$$\nabla_L(z) = P_L(1, z) \quad \text{and} \quad V_L(t) = P_L(t^{-1}, t^{1/2} - t^{-1/2}).$$

The Jones-Conway polynomial can help distinguish a link L from its mirror image $\tilde{L}$, i.e., its image under a reflection with respect to a plane in $\mathbf{R}^3$. Theorem 4.2 has the following corollary.

Corollary X.4.3. *We have* $P_{\tilde{L}}(x, y) = P_L(x^{-1}, -y)$.

PROOF. The mirror image of the Conway triple (L_+, L_-, L_0) is the triple $(\widetilde{L}_-, \widetilde{L}_+, \widetilde{L}_0)$. Consequently, we have

$$x^{-1}P_{\widetilde{L}_-} - xP_{\widetilde{L}_+} = -yP_{\widetilde{L}_0}.$$

One conclude by appealing to the characteristic properties of P. □

Let us prove Theorem 4.2. Consider the ring $\Lambda = \mathbf{Z}[x, x^{-1}, y, y^{-1}]$, the set $\mathcal{K}$ of equivalence classes of all oriented links in $\mathbf{R}^3$, and $\Lambda[\mathcal{K}]$ the free Λ-module generated by $\mathcal{K}$. We denote by Υ the quotient of $\Lambda[\mathcal{K}]$ by the Λ-submodule generated by

$$x[L_+] - x^{-1}[L_-] - y[L_0] \tag{4.4}$$

where (L_+, L_-, L_0) runs over all Conway triples of $\mathcal{K}$. The Λ-module Υ is called the *skein module* of $\mathbf{R}^3$.

Proposition X.4.4. *Let $Q : \Lambda \to \Upsilon$ be the Λ-linear map sending 1 on the class $[O]$ of the trivial knot. Then Q is an isomorphism.*

Consequently, the skein module Υ is a free Λ-module of rank one generated by $[O]$. Proposition 4.4 implies Theorem 4.2. Indeed, let L be an oriented link and $[L]$ its class in Υ. Set

$$P_L = Q^{-1}([L]) \in \mathbf{Z}[x, x^{-1}, y, y^{-1}].$$

It is clear that P satisfies all three conditions of Theorem 4.2. It remains to establish Proposition 4.4. The proof of the latter divides into two parts consisting in proving successively that the map Q is surjective, then injective.

Surjectivity of Q. This is purely topological and is essentially independent of the nature of the ring Λ. It is enough to check that the Λ-module Υ is generated by the class $[O]$ of the trivial knot. This will be shown in two steps.

Lemma X.4.5. *The Λ-module Υ is generated by the family $\{[O^{\otimes n}]\}_{n>0}$ of isotopy classes of all trivial links.*

PROOF. Let Υ_m be the Λ-submodule generated by the isotopy classes of links representable by link diagrams with $\leq m$ crossing points. Clearly, Υ_m maps to Υ_{m+1} and Υ is the union of all Υ_m. It is therefore enough to prove Lemma 4.5 for each Υ_m. This is done by induction on m. The case $m = 0$ holds by definition of trivial links. Suppose the assertion is proved for all integers $< m$. Let $[L]$ be the class of a link L in Υ_m. It may be represented by a link diagram with m crossing points. Consider one of them. Then there exists a Conway triple (L_+, L_-, L_0) such that $L = L_+$ or $L = L_-$ and the diagram L_0 has less than m crossing points. It follows from (4.4) that $[L_+] \equiv x^{-2}[L_-]$ modulo Υ_{m-1}. In other words, a change of crossings changes the class of L modulo Υ_{m-1} by multiplication by an invertible element of Λ. By Lemma 3.3 this implies that the class of L belongs to the submodule generated by the trivial links and Υ_{m-1}. The latter is also generated by trivial links in view of the induction hypothesis. □

The second step in the proof of the surjectivity of Q is the following lemma which, incidentally, shows the necessity for y to be invertible (unless $x = \pm 1$ as in the case of the Conway polynomial).

Lemma X.4.6. *For any integer $n > 1$, we have*

$$[O^{\otimes n}] = \left(\frac{x - x^{-1}}{y}\right)^{n-1} [O].$$

PROOF. Figure 4.2 implies that $(O^{\otimes n}, O^{\otimes n}, O^{\otimes n+1})$ is a Conway triple for all $n \geq 1$. By definition of Υ we get

$$[O^{\otimes n+1}] = \frac{x - x^{-1}}{y} [O^{\otimes n}].$$

One concludes by induction on n. □

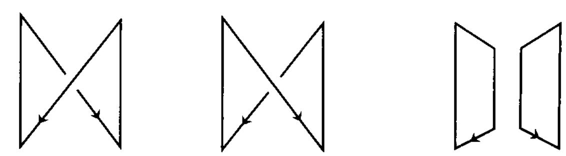

Figure 4.2. A Conway triple

Injectivity of Q. This part of the proof is algebraic in contrast with the surjectivity part. We use the following proposition whose proof will be given in Chapter XII.

Proposition X.4.7. *Let $q \neq 0$ be a complex number that is not a root of unity and let m be an integer > 1. There exists a unique map $\Phi_{m,q}$ from the set of all oriented links in $\mathbf{R}^3$ to the field $\mathbf{C}$ of complex numbers such that*

(i) *if $L \sim L'$, then $\Phi_{m,q}(L) = \Phi_{m,q}(L')$,*
(ii) *the value of $\Phi_{m,q}$ on the trivial knot is*

$$\Phi_{m,q}(O) = \frac{q^m - q^{-m}}{q - q^{-1}} \neq 0,$$

(iii) *and, whenever (L_+, L_-, L_0) is a Conway triple, we have*

$$q^m\Phi_{m,q}(L_+) - q^{-m}\Phi_{m,q}(L_-) = (q - q^{-1})\Phi_{m,q}(L_0).$$

Assuming Proposition 4.7 and using the ring map $\zeta_{q,m} : \Lambda \to \mathbf{C}$ defined by $\zeta_{q,m}(x) = q^m$ and $\zeta_{q,m}(y) = q - q^{-1}$, which furnishes $\mathbf{C}$ with a Λ-module structure, we see that $\Phi_{m,q}$ extends by linearity to a unique Λ-linear map $\Phi'_{m,q}$ from $\Lambda[\mathcal{K}]$ to $\mathbf{C}$. Now for any Conway triple (L_+, L_-, L_0), we have

$$\begin{aligned}
&\Phi'_{m,q}\Big(x[L_+] - x^{-1}[L_-] - y[L_0]\Big)\\
&= \zeta_{q,m}(x)\Phi_{m,q}(L_+) - \zeta_{q,m}(x^{-1})\Phi_{m,q}(L_-) - \zeta_{q,m}(y)\Phi_{m,q}(L_0)\\
&= q^m\Phi_{m,q}(L_+) - q^{-m}\Phi_{m,q}(L_-) - (q - q^{-1})\Phi_{m,q}(L_0)\\
&= 0
\end{aligned}$$

by Proposition 4.7. Consequently, $\Phi'_{m,q}$ factors through a unique Λ-linear map, denoted $\Phi''_{m,q}$, from Υ into $\mathbf{C}$ such that $\Phi''_{m,q}([L]) = \Phi_{m,q}(L)$ for any oriented link L.

We are now ready to prove the injectivity of the map Q from Λ into Υ, which will complete the proof of Proposition 4.4, hence of Theorem 4.2.

Let $f(x,y) \in \Lambda$ be a two-variable Laurent polynomial chosen such that $Q(f(x,y)) = f(x,y)[O]$ vanishes in Υ. Then, using the above-defined map $\Phi''_{m,q} : \Upsilon \to \mathbf{C}$, we have

$$0 = \Phi''_{m,q}\Big(f(x,y)[O]\Big) = f(q^m, q - q^{-1})\Phi_{m,q}(O)$$

for any integer $m > 1$ and any complex number q that is not a root of unity. Since $\Phi_{m,q}(O) \neq 0$, we have $f(q^m, q - q^{-1}) = 0$. Since this is true for an infinite number of distinct powers of q, the polynomial f is divisible by the polynomial $y - (q - q^{-1})$. The latter assertion holds for infinitely many complex numbers q, which is possible only if the polynomial f is zero. This proves the injectivity of Q. □

Application 4.8. We end this section with the computation of the Jones-Conway polynomial of the right-handed trefoil knot K and of the Hopf link H. Figures 4.3–4.4 show that (H, OO, O) and (K, O, H) are Conway triples.

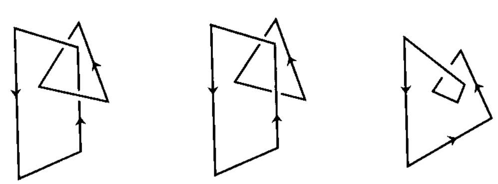

Figure 4.3.

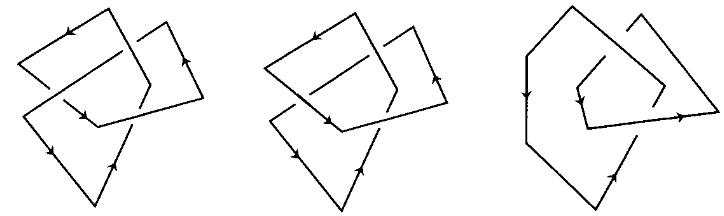

Figure 4.4.

By (4.1) we have

$$xP_H = x^{-1}P_{OO} + yP_O = x^{-1}\frac{x - x^{-1}}{y} + y.$$

Hence,

$$P_H = (x^{-1} - x^{-3})y^{-1} + x^{-1}y.$$

A similar computation yields

$$P_K = 2x^{-2} - x^{-4} + x^{-2}y^2$$

for the right-handed trefoil knot. By Corollary 4.3, we see that the Jones-Conway polynomial of the mirror image $\widetilde{K}$ is given by

$$P_{\widetilde{K}} = 2x^2 - x^4 + x^2y^2 \neq P_K.$$

This proves that the trefoil knot is not isotopic to its mirror image, a fact already observed by Dehn [Deh14] in 1914.

X.5 Tangles

This section is devoted to the concept of tangles which generalizes the notion of links. Tangles will be used extensively in Chapter XII, in particular for the proof of Proposition 4.7.

For any integer $n > 0$, we set $[n] = \{1, 2, \ldots, n\}$. When $n = 0$, we agree that $[0]$ is the empty set. We denote by I the closed interval $[0,1]$ and by $\mathbf{R}^2$ the real plane.

Definition X.5.1. *Let k and ℓ be nonnegative integers. A tangle L of type (k,ℓ) is the union of a finite number of pairwise disjoint simple oriented polygonal arcs in $X = \mathbf{R}^2 \times I$ such that the boundary ∂L of L satisfies the condition*

$$\partial L = L \cap (\mathbf{R}^2 \times \{0,1\}) = ([k] \times \{0\} \times \{0\}) \cup ([\ell] \times \{0\} \times \{1\}).$$

The boundary condition in Definition 5.1 means that the tangle intersects the two boundary planes of $\mathbf{R}^2 \times I$ transversally. Observe that a link in $\mathbf{R}^2 \times I$ is a tangle of type $(0,0)$. Figure 5.1 shows an example of a tangle that is not a link.

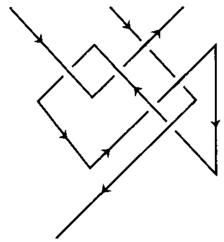

Figure 5.1. A tangle

Given a tangle L of type (k,ℓ), we define two finite sequences $s(L)$ and $b(L)$ consisting of $+$ and $-$ signs. If $k=0$, then $s(L)=\emptyset$ is the empty set by convention. Similarly if $\ell = 0$, we set $b(L)=\emptyset$. In the general case, we define

$$s(L) = (\varepsilon_1, \dots, \varepsilon_k) \quad \text{and} \quad b(L) = (\eta_1, \dots, \eta_\ell)$$

where $\varepsilon_i = +$ [resp. $\eta_i = +$] if the point $(i,0,0)$ [resp. the point $(i,0,1)$] is an endpoint [resp. an origin] of L. We have $\varepsilon_i = -$ and $\eta_i = -$ in the remaining cases.

Let us give a few examples of tangles that shall be used in the sequel.

1. We denote the polygonal arcs $[(1,0,1),(1,0,0)]$ and $[(1,0,0),(1,0,1)]$ by $\downarrow$ and $\uparrow$ respectively. We have $s(\downarrow) = (+)$, $b(\downarrow) = (+)$, $s(\uparrow) = (-)$, and $b(\uparrow) = (-)$.

2. The tangles X_+ and X_- of Figure 4.1 can be defined by

$$X_\pm = [M_1, M_2^\pm] \cup [M_2^\pm, M_3] \cup [N_1, N_2^\pm] \cup [N_2^\pm, N_3] \tag{5.1}$$

where $M_1, M_2^\pm, M_3, N_1, N_2^\pm, N_3$ are the points whose coordinates in $\mathbf{R}^2 \times I$ are

$$\begin{array}{lll} M_1 & = & (2,0,1), \\ M_2^\pm & = & (3/2, \mp 1, 1/2), \\ M_3 & = & (1,0,0), \end{array} \qquad \begin{array}{lll} N_1 & = & (1,0,1), \\ N_2^\pm & = & (3/2, \pm 1, 1/2), \\ N_3 & = & (2,0,0). \end{array}$$

We have $s(X_\pm) = b(X_\pm) = (+,+)$.

3. The tangles $\cap$ and $\overleftarrow{\cap}$ of type $(2,0)$ are defined by

$$\cap = [(1,0,0),(3/2,0,1/2)] \cup [(3/2,0,1/2),(2,0,0)] \tag{5.2}$$

and

$$\overleftarrow{\cap} = [(2,0,0),(3/2,0,1/2)] \cup [(3/2,0,1/2),(1,0,0)]. \tag{5.3}$$

We have $s(\cap) = (-,+)$, $b(\cap) = \emptyset$, $s(\overleftarrow{\cap}) = (+,-)$, and $b(\overleftarrow{\cap}) = \emptyset$ (see Figure 5.2).

Figure 5.2. The tangles $\cap$ and $\overleftarrow{\cap}$

4. Similarly, we define tangles $\cup$ and $\overleftarrow{\cup}$ of type $(0,2)$ by

$$\cup = [(1,0,1),(3/2,0,1/2)] \cup [(3/2,0,1/2),(2,0,1)] \tag{5.4}$$

and

$$\overleftarrow{\cup} = [(2,0,1),(3/2,0,1/2)] \cup [(3/2,0,1/2),(1,0,1)]. \tag{5.5}$$

We have $s(\cup) = \emptyset$, $b(\cup) = (+,-)$, $s(\overleftarrow{\cup}) = \emptyset$, and $b(\overleftarrow{\cup}) = (-,+)$ (see Figure 5.3).

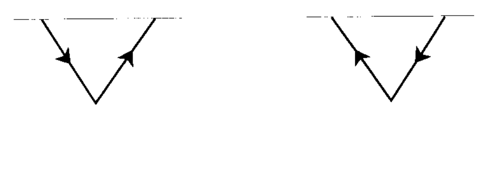

Figure 5.3. The tangles $\cup$ and $\overleftarrow{\cup}$

We have the same equivalence relations for tangles as for links. Let us adapt their definition to the case of tangles. We start with the combinatorial relation $\sim_c$.

Definition X.5.2. (a) *Let L be a tangle in X and M_i, M_{i+1} be two consecutive vertices of L. We are also given a point N in $\mathbf{R}^2 \times]0,1[$ such that $N \notin L$, $M_i \notin [N, M_{i+1}]$, $M_{i+1} \notin [M_i, N]$, and*

$$[M_i, N, M_{i+1}] \cap L = [M_i, M_{i+1}].$$

We define L' as the tangle

$$L' = (L \setminus [M_i, M_{i+1}]) \cup [M_i, N] \cup [N, M_{i+1}].$$

We say that L' is obtained from L by a Δ-operation.

(b) *Two tangles L and L' are combinatorially equivalent – we write this $L \sim_c L'$ – if there exist tangles $L = L_0, L_1, \dots, L_k = L'$ such that for all i, one of the tangles L_i, L_{i+1} is obtained from the other one by a Δ-operation.*

Clearly, if L and L' are combinatorially equivalent, they have the same boundaries and are of the same type. Isotopies are defined as follows.

Definition X.5.3. (a) *An isotopy of* $X = \mathbf{R}^2 \times I$ *is a piecewise-linear map* $h : I \times X \to X$ *such that for all* $t \in I$, *the mapping* $h(t, -)$ *is a homeomorphism of* X *restricting to the identity map on the boundary* $\partial X = \mathbf{R}^2 \times \{0,1\}$ *and such that* $h(0,-)$ *is the identity of* X.

(b) *Two tangles* L *and* L' *are isotopic – we write* $L \sim_i L'$ *– if there exists an isotopy* h *of* X *such that* $h(1, L) = L'$.

Again if L and L' are isotopic, they have the same boundaries and are of the same type. The isotopy is shown to be an equivalence relation for tangles in the same way as it was for links (see Lemma 1.5). We have the following counterpart of Proposition 1.6.

Proposition X.5.4. *Let* L *and* L' *be two tangles. Then*

$$L \sim_c L' \iff L \sim_i L'.$$

As for links, we shall suppress the subscripts i and c from the symbols $\sim_i$ and $\sim_c$ and we shall henceforth speak of isotopic or equivalent tangles.

Tangles can also be represented by planar diagrams. We adapt the following concepts and results from Section 3 without bothering to give unnecessary details.

Definition X.5.5. (a) *A tangle projection* Π *is the union of a finite number of (not necessarily closed) polygonal arcs in* $\mathbf{R}^2$ *such that no vertex sits in the interior of any edge and such that the boundary* $\partial\Pi$ *of* Π *satisfies the condition*

$$\partial\Pi = \Pi \cap (\mathbf{R} \times \{0,1\}) = ([k] \times \{0\}) \cup ([\ell] \times \{1\}).$$

A crossing point of Π *is a point of the tangle projection sitting in the interior of at least two edges. The order of a crossing point* P *is the number of distinct edges in the interior of which* P *sits.*

(b) *A tangle projection is regular if each crossing point is of order exactly* 2.

Let Π be a regular tangle projection in the plane. Given a crossing point P we may again consider the unordered set E_P consisting of the two edges on which P sits.

Definition X.5.6. *A tangle diagram is a regular tangle projection in* $\mathbf{R} \times I$ *for which all the sets* E_P *(indexed by the crossing points* P*) are ordered. Given a crossing point* P, *the first edge of the set* E_P *with respect to the ordering is called the overcrossing edge whereas the other edge is called the undercrossing edge.*

Replacing $\mathbf{R}^2$ by $\mathbf{R} \times [0,1]$, one defines the concepts of isotopy of tangle diagrams, of generic tangle diagrams, and of generic isotopy as for links. Similar results hold. We record here the counterpart of Lemma 3.6.

Lemma X.5.7. *Two generic tangle diagrams are isotopic if and only if they are obtained from one another by a finite number among the following operations:*

(A) *a generic isotopy,*

(B) *an isotopy interchanging the order of the vertices with respect to the height,*

(C) *a Reidemeister Transformation (0), and*

(E) *an isotopy in the neighbourhood of a crossing point as shown in Figure* 3.10 *and their images under reflection in the plane of the page.*

As in the case of links, any (generic) tangle diagram defines a tangle in $\mathbf{R}^2 \times I$ which is unique up to isotopy. Fix a linear projection π_0 of the space $\mathbf{R}^2 \times I$ on the strip $\mathbf{R} \times I$.

Proposition X.5.8. *Any tangle in* $\mathbf{R}^2 \times I$ *is equivalent to a tangle* L *whose projection* $\pi_0(L)$ *is a generic tangle diagram.*

When do two tangle diagrams represent isotopic tangles? The answer to this question is the same as in the case of links. It uses the Reidemeister moves already defined in Section 3.

Theorem X.5.9. *Two generic tangle diagrams represent equivalent tangles in* $\mathbf{R}^2 \times I$ *if and only if one is obtained from the other by a finite sequence of Reidemeister Transformations* (I), (II), (III), *and of isotopies of diagrams.*

We close this section by defining a partial binary operation on tangles. Consider the piecewise-linear mappings a_1, a_2 from the topological space $\mathbf{R}^2 \times I$ into itself defined by

$$a_1(p,z) = (p, z/2) \quad \text{and} \quad a_2(p,z) = (p, (z+1)/2)$$

where $p \in \mathbf{R}^2$ and $z \in I$. When L and L' are oriented tangles such that $b(L) = s(L')$, then

$$L' \circ L = a_1(L) \cup a_2(L')$$

is an oriented tangle with

$$s(L' \circ L) = s(L) \quad \text{and} \quad b(L' \circ L) = b(L').$$

The tangle $L' \circ L$ is called the *composition* of L and L'. It is obtained by placing L' on top of L, by glueing their middle ends together and by squeezing the whole into $\mathbf{R}^2 \times [0,1]$. Let us prove that composition is compatible with the equivalence of tangles.

Lemma X.5.10. *Let L_1, L_2, L_3, L_4 be oriented tangles with $b(L_1) = s(L_2)$ and $b(L_3) = s(L_4)$.*

(a) *If $L_1 \sim L_3$ and $L_2 \sim L_4$, then $L_2 \circ L_1 \sim L_4 \circ L_3$.*

(b) *If, furthermore, $b(L_2) = s(L_3)$, then $(L_3 \circ L_2) \circ L_1 \sim L_3 \circ (L_2 \circ L_1)$.*

PROOF. (a) Use Reidemeister Transformations.

(b) The tangles $(L_3 \circ L_2) \circ L_1$ and $L_3 \circ (L_2 \circ L_1)$ are isotopic through the isotopy $h(t, p, z) = (p, \varphi_t(z))$ where $p \in \mathbf{R}^2$, $t, z \in [0, 1]$ and φ is the continuous mapping from $I \times I$ into I defined by

$$\varphi_t(z) = \begin{cases} z(1 - \frac{t}{2}) & \text{if} \quad 0 \leq z \leq 1/2, \\ z - \frac{t}{4} & \text{if} \quad 1/2 \leq z \leq 3/4, \\ (1 + t)z - t & \text{if} \quad 3/4 \leq z \leq 1. \end{cases}$$

□

The composition has partial left and right units up to isotopy. Indeed, for any finite sequence ε of $\pm$ signs of length n, define the tangle id_ε as the union of the n intervals $\{1, \ldots, n\} \times \{0\} \times [0, 1]$, their origins and endpoints being uniquely determined by the requirement $s(\mathrm{id}_\varepsilon) = b(\mathrm{id}_\varepsilon) = \varepsilon$. If the sequence ε is empty, take $\mathrm{id}_\emptyset$ to be the empty tangle. An immediate application of Δ-operations proves the following lemma.

Lemma X.5.11. *For any tangle L, we have*

$$\mathrm{id}_{b(L)} \circ L \sim L \sim L \circ \mathrm{id}_{s(L)}.$$

X.6 Braids

We now consider a special class of tangles, called braids. Fix an integer $n \geq 1$.

Definition X.6.1. *A braid L with n strands is a tangle of type (n, n) such that*

(i) $s(L) = b(L) = (+, +, \cdots, +)$,

(ii) *L contains no closed arc, and*

(iii) *for all $z \in I$, the intersection of L with theplane $\mathbf{R}^2 \times \{z\}$ consists of exactly n distinct points.*

In other words, a braid with n strands is the union of n pairwise disjoint simple polygonal arcs, relating the set $[n] \times \{0\} \times \{1\}$ to the set $[n] \times \{0\} \times \{0\}$ and having no local maximum or minimum with respect to the "height" projection $\mathbf{R}^2 \times I \to I$. Figure 6.1 shows a braid with 5 strands.

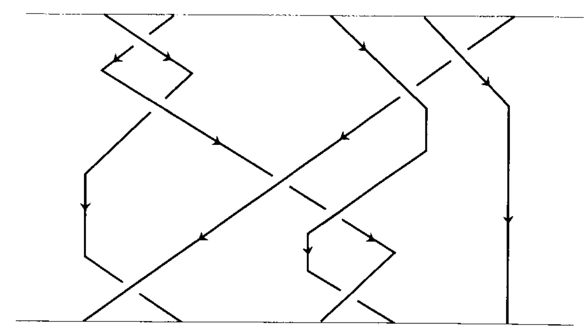

Figure 6.1. A braid

By definition, two braids are equivalent if they can be obtained from each other by a finite sequence of Δ-operations performed within the set of braids. Up to equivalence, a braid with n strands can be represented by what may be called a *braid diagram*, i.e., a tangle diagram such that for all $z \in I$ the intersection of the diagram with $\mathbf{R} \times \{z\}$ consists of exactly n distinct points. There is also a notion of isotopy of braid diagrams which is the restriction to braid diagrams of the corresponding notion for tangle diagrams. Braid diagrams are isotopic if and only if they are obtained from each other by moving vertices up and down. Concerning Reidemeister moves, Transformations (0) and (I) are clearly forbidden for braid diagrams. Only Transformations (II) and (III) may occur. They are sufficient to generate the braid equivalence, as witnessed by the following proposition whose proof is similar to (and simpler than) the proof of the corresponding Theorem 5.9 for tangles.

Proposition X.6.2. *Two braid diagrams represent equivalent braids if and only if they are obtained from each other by a finite sequence of Reidemeister Transformations* (II), (III), *and of isotopies of braid diagrams.*

X.6.1 The braid group B_n

In Section 5 we defined the composition $L' \circ L$ for tangles L, L' such that $b(L) = s(L')$. We see from the definitions that the composition of two braids with n strands is still a braid with n strands. A special braid with n strands is id_ε (as defined at the end of Section 5) where ε is the sequence consisting of n signs $+$. We denote its equivalence class by 1_n. Given a braid L we define the *inverse braid* L^{-1} as the image of L under the reflection through the plane $\mathbf{R}^2 \times \{1/2\}$.

Denote the set of equivalence classes of braids with n strands by B_n. The set B_0 has one single element, namely the empty braid. Restricted to braids, Lemma 5.10 implies that the composition of braids is compatible with braid equivalence. Therefore the composition induces a product on B_n. As a matter of fact, we have the following result.

Proposition X.6.3. *The composition of braids induces a group structure on B_n with 1_n as a unit.*

PROOF. Associativity of the product follows from Lemma 5.10 (b) whereas Lemma 5.11 implies that 1_n is a left and right unit for the product on B_n. Repeated use of Reidemeister Transformation (II) shows that

$$L^{-1} \circ L \sim 1_n \sim L \circ L^{-1},$$

which implies that the equivalence class of L^{-1} is an inverse for the equivalence class of L. □

The group B_n was introduced by E. Artin [Art25]. It is called the *braid group* (on n strands). The groups $B_0 = B_1$ are isomorphic to the trivial group $\{1\}$.

We now give a presentation by generators and relations of B_n. First, we define special elements $\sigma_1, \sigma_2, \dots, \sigma_{n-1}$ in B_n. A braid diagram of the braid σ_i is shown in Figure 6.2.

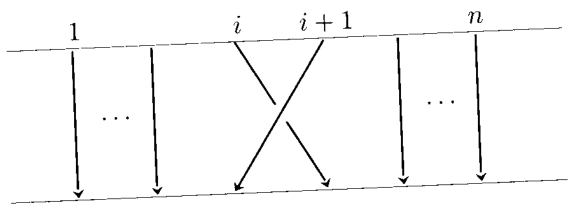

Figure 6.2. The braid σ_i

Using the tangle X_+ of Section 5, we see that σ_i is equivalent to the braid

$$\downarrow \cdots \downarrow X_+ \downarrow \cdots \downarrow$$

exchanging the i-th and the $(i+1)$-st strands and leaving the other ones untouched. Its inverse σ_i^{-1} is equivalent to the braid

$$\downarrow \cdots \downarrow X_- \downarrow \cdots \downarrow$$

with the opposite crossing (see Figure 6.3).

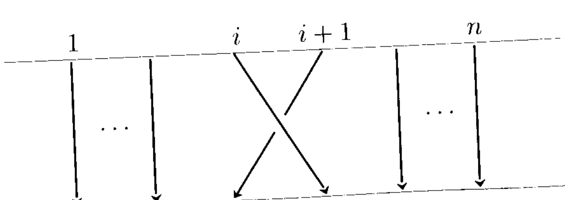

Figure 6.3. The braid σ_i^{-1}

Lemma X.6.4. (a) *The group B_n is generated by $\sigma_1, \dots, \sigma_{n-1}$.*

(b) *When $n \geq 3$ and $1 \leq i, j \leq n-1$, we have the following relations in the braid group B_n:*

$$\sigma_i \sigma_j = \sigma_j \sigma_i \tag{6.1}$$

if $|i-j| > 1$ and

$$\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}. \tag{6.2}$$

Relations (6.1–6.2) are called the *braid group relations* .

PROOF. (a) Represent a braid by a braid diagram. Move crossing points up or down so that one can find $0 < t_1 < \dots < t_r < 1$ such that for all i there is only one crossing point in $\mathbf{R} \times [t_i, t_{i+1}]$. This means that the braid is equivalent to a braid whose restriction to $\mathbf{R} \times [t_i, t_{i+1}]$ is equivalent to some σ_k or its inverse. Using the definition of the product in the braid group, we see that the given braid can be expressed in B_n as the product of the elements σ_k and their inverses.

(b) If $|i-j| > 1$, then clearly $\sigma_i \sigma_j$ and $\sigma_j \sigma_i$ are equivalent (draw a picture). Both sides of Relation (6.2) are represented in Figure 3.4. One passes from one diagram to the other by Reidemeister Transformation (III). □

We now state an important theorem due to E. Artin [Art25] [Art47].

Theorem X.6.5. *Given a group G and elements $c_1, \dots, c_{n-1}$ $(n > 2)$ such that for all i, j we have $c_i c_j = c_j c_i$ if $|i-j| > 1$ and*

$$c_i c_{i+1} c_i = c_{i+1} c_i c_{i+1},$$

then there exists a unique group morphism from B_n to G mapping σ_i to c_i.

Corollary X.6.6. *The group B_n is isomorphic to the group generated by $\sigma_1, \sigma_2, \dots, \sigma_{n-1}$ and the braid group relations (6.1–6.2).*

PROOF. Let G be the latter group. By Theorem 6.5, there exists a unique group morphism $\rho : B_n \to G$ such that $\rho(\sigma_i) = \sigma_i$ for all i. Now by definition of a group given by generators and relations, there exists a unique group morphism $\rho' : G \to B_n$ sending σ_i onto σ_i for all i. Then ρ' is inverse to ρ. □

oof of Theorem 6.5. The uniqueness of the group morphism follows from e fact proven in Lemma 6.4 (a) that $\sigma_1, \dots, \sigma_{n-1}$ generate B_n.

Now, let us establish the existence of a group morphism $\rho : B_n \to G$ such at $\rho(\sigma_i) = c_i$ for $i = 1, \dots, n-1$. We sketch a geometric proof. Consider a id L represented by a generic diagram as in the proof of Lemma 6.4 (a), mely for which two different crossing points have different heights. To h a diagram we can assign a unique braid word w in the generators σ_i their inverses as in the proof of Lemma 6.4 (a). Define $\rho(w)$ to be the element of G obtained by replacing σ_i by c_i and σ_i^{-1} by c_i^{-1} in the word w. Let us show that $\rho(w)$ depends only on the initial braid.

According to Proposition 6.2, we have to check that $\rho(w)$ does not change when we perform an isotopy of diagram or Reidemeister Transformations of type (II) and (III). In the first case, moving crossing points up and down amounts to changing the braid word by products of commutators of the form $\sigma_i\sigma_j\sigma_i^{-1}\sigma_j^{-1}$ for $|i-j|>1$. This leaves $\rho(w)$ unchanged because $c_ic_jc_i^{-1}c_j^{-1} = 1$ for $|i-j|>1$. Under a Reidemeister Transformation (II), braid words differ by $\sigma_i\sigma_i^{-1}$ or by $\sigma_i^{-1}\sigma_i$ whose images under ρ is 1. Under a Reidemeister Transformation (III), braid words differ by $\sigma_i\sigma_{i+1}\sigma_i\sigma_{i+1}^{-1}\sigma_i^{-1}\sigma_{i+1}^{-1}$ or its inverse. Their images under ρ again is 1 because of the relation $c_ic_{i+1}c_i = c_{i+1}c_ic_{i+1}$. □

We still have to investigate the case of braids with two strands. An adaptation of the proofs of Lemma 6.4 and Theorem 6.5 proves the following.

Proposition X.6.7. *The group B_2 is generated by σ_1 and is isomorphic to the group $\mathbf{Z}$ of integers.*

X.6.2 Braid group representations from R-matrices

We show how Theorem 6.5 allows us to construct braid group representations from any solution of the Yang-Baxter equation.

Let V be a vector space, c a linear automorphism of $V\otimes V$, and $n>1$ an integer. Then for $1\le i\le n-1$, define a linear automorphism c_i of $V^{\otimes n}$ by

$$c_i = \begin{cases} c\otimes \mathrm{id}_{V^{\otimes(n-2)}} & \text{if} \quad i=1,\\ \mathrm{id}_{V^{\otimes(i-1)}}\otimes c\otimes \mathrm{id}_{V^{\otimes(n-i-1)}} & \text{if} \quad 1<i<n-1,\\ \mathrm{id}_{V^{\otimes(n-2)}}\otimes c & \text{if} \quad i=n-1.\end{cases} \tag{6.3}$$

Clearly $c_ic_j = c_jc_i$ if $|i-j|>1$. It is easy to check the following lemma.

Lemma X.6.8. *Under the previous hypothesis, we have*

$$c_ic_{i+1}c_i = c_{i+1}c_ic_{i+1}$$

for all i if and only c is a solution of the Yang-Baxter equation.

The Yang-Baxter equation of VIII.1 can be expressed with the present notation as the equation $c_1c_2c_1 = c_2c_1c_2$ holding in $\mathrm{Aut}(V\otimes V\otimes V)$. The following is a consequence of Theorem 6.5 and Lemma 6.8.

Corollary X.6.9. *Let $c\in \mathrm{Aut}(V\otimes V)$ be a solution of the Yang-Baxter equation. Then, for any $n>0$, there exists a unique group morphism $\rho_n^c : B_n \to \mathrm{Aut}(V^{\otimes n})$ such that $\rho_n^c(\sigma_i) = c_i$ for $i=1,\dots,n-1$.*

Consequently, by this procedure, any linear automorphism c of $V\otimes V$ that is a solution of the Yang-Baxter gives rise to a representation of the braid group B_n on the tensor power $V^{\otimes n}$ where n is any integer ≥ 2.

X.6.3 Relation with the symmetric group S_n

Given a braid L, there exists a unique permutation $\sigma(L)$ of the set $\{1,\dots,n\}$ such that for all $k\in\{1,\dots,n\}$ the endpoint $(k,0,0)$ lies in the same connected component as the origin $(\sigma(k),0,1)$. The permutation $\sigma(L)$ is called the *permutation of the braid L*.

Lemma X.6.10. *The map $f\mapsto \sigma(f)$ induces a surjective morphism of groups from the braid group B_n onto the symmetric group S_n.*

PROOF. First it is clear that equivalent braids have the same permutation. Thus the map factors through B_n. It is a morphism of groups because we have $\sigma(L'\circ L) = \sigma(L')\circ\sigma(L)$, $\sigma(1_n) = \mathrm{id}$, and $\sigma(L^{-1}) = \sigma(L)^{-1}$. The permutation of the braid σ_i is the transposition $(i,i+1)$. The surjectivity of the map follows from the fact that such transpositions generate the symmetric group S_n. □

This lemma is not surprising in view of Moore's theorem which gives the following presentation in terms of generators and relations for the symmetric group S_n: it is generated by the $n-1$ transpositions $s_i = (i,i+1)$ and by Relations (6.1–6.2) where σ_i has been replaced by s_i, as well as by the additional relations $s_i^2 = 1$ for $i=1,\dots,n-1$.

One big difference between symmetric groups and braid groups is that the former are finite groups while the latter are infinite groups when $n>1$. Moreover, the group B_n has no torsion, that is to say, all elements $\ne 1_n$ have infinite order.

X.6.4 Representing braids as loops

We end this section by giving a function-theoretic definition of braids. Let n be an integer ≥ 1. Consider the set

$$Y_n = \{(z_1,\dots,z_n)\in \mathbf{C}^n \mid i\ne j \Rightarrow z_i\ne z_j\}$$

endowed with the subset topology of $\mathbf{C}^n$. The symmetric group S_n acts on Y_n by permutation of the coordinates. Let $X_n = Y_n/S_n$ be the quotient space with the quotient topology. The space X_n is the *configuration space* of n distinct points in $\mathbf{C}$. Consider the following set $p=\{1,2,\dots,n\}$ of n distinct points in X_n.

Definition X.6.11. *A loop in X_n is a piecewise linear map*

$$f = (f_1,f_2,\dots,f_n) : I=[0,1]\to \mathbf{C}^n$$

such that for all $t \in I$ *we have* $f_i(t) \neq f_j(t)$ *whenever* $i \neq j$ *and*

$$f(0) = (1, 2, \dots, n) \quad \text{and} \quad \{f_1(1), f_2(1), \dots, f_n(1)\} = \{1, 2, \dots, n\}.$$

Loops in X_n and braids with n strands in $\mathbf{R}^2 \times [0,1]$ are equivalent notions after we have identified $\mathbf{C}$ with $\mathbf{R}^2$. Indeed, given a loop $f = (f_1, f_2, \dots, f_n)$ in X_n, the union of the graphs of the maps f_i is a braid with n strands. Conversely, for any braid L with n strands, we define $f_i(z)$ to be the projection onto $\mathbf{R}^2 = \mathbf{C}$ of the intersection of the plane $\mathbf{R}^2 \times \{z\}$ with the connected component of L ending at the point $(i, 0, 0)$. This defines a loop $f = (f_1, f_2, \dots, f_n)$ in X_n.

For any loop $f = (f_1, \dots, f_n)$ in X_n, define the permutation $\sigma(f)$ of the set $\{1, \dots, n\}$ by $\sigma(f)(k) = f_k(1)$ for all k. Check that, if f is the loop corresponding to a braid L, then $\sigma(f) = \sigma(L)$.

The equivalence of braids can be expressed on loops in X_n as follows. Two loops $f = (f_1, f_2, \dots, f_n)$ and $g = (g_1, g_2, \dots, g_n)$ in X_n are homotopic in X_n — we write $f \sim g$ — if there exists a piecewise linear map, called an *isotopy*,

$$H = (H_1, H_2, \dots, H_n) : I \times I \to \mathbf{C}^n$$

such that for all $(s,t) \in I \times I$ and $i \neq j$ we have $H_i(s,t) \neq H_j(s,t)$, for all $s \in I$ and k with $1 \leq k \leq n$ we have

$$H_k(s,0) = f_k(0) = g_k(0) \quad \text{and} \quad H_k(s,1) = f_k(1) = g_k(1),$$

for all $t \in I$ and $1 \leq k \leq n$ we have

$$H_k(0,t) = f_k(t) \quad \text{and} \quad H_k(1,t) = g_k(t).$$

Proposition X.6.12. *Two braids with n strands are equivalent if and only if the corresponding loops are isotopic in* X_n.

We can transpose the composition of tangles on the level of loops. Let f [resp. f'] be the loop in X_n corresponding to a braid L [resp. L']. It is easy to see that the loop $ff' = \big((ff')_1, \dots, (ff')_n\big)$ corresponding to the braid $L' \circ Lx$, composed in the sense of tangles, (see Section 5) is given for all i by

$$(ff')_i(t) = \begin{cases} f_i(2t) & \text{if} \quad 0 \leq t \leq 1/2, \\ f'_{\sigma(i)}(2t-1) & \text{if} \quad 1/2 \leq t \leq 1 \end{cases}$$

where $\sigma = \sigma(f)$ is the permutation of f. The loop ff' is called the *product* of the loops f, and f'. We have $\sigma(ff') = \sigma(f') \circ \sigma(f)$.

Given a loop $f = (f_1, \dots, f_n)$ corresponding to a braid L, the loop f^{-1} defined by

$$f_i^{-1}(z) = f_{\sigma^{-1}(i)}(1-z),$$

where again $\sigma = \sigma(f)$, corresponds to the inverse braid L^{-1}. The loop corresponding to the braid 1_n is the constant map $z \mapsto (1, 2, \dots, n)$.

We have the following lemma which is the counterpart for loops of Lemmas 5.10–5.11.

Lemma X.6.13. *Given loops* f, f', f'', g, g' *in* X_n,
(a) *if* $f \sim g$ *and* $f' \sim g'$, *then* $ff' \sim gg'$,
(b) $(ff')f'' \sim f(f'f'')$,
(c) $1_n f \sim f \sim f 1_n$, *and*
(d) $ff^{-1} \sim 1_n \sim f^{-1}f$.

PROOF. See the Appendix to this chapter. □

We have the following important result as a consequence of the presentation of braids by loops and of the definitions of the Appendix.

Proposition X.6.14. *The braid group* B_n *is isomorphic to the fundamental group of the configuration space* X_n *of* n *distinct points in* $\mathbf{C}$:

$$B_n \cong \pi_1(X_n, p)$$

where p *is the set* $\{1, \dots, n\}$.

X.7 Exercises

1. (*Centre of the braid group*) Let n be an integer > 2. Show that the centre of the braid group B_n is generated by the element $(\sigma_1 \dots \sigma_{n-1})^n$.

2. For an integer $n > 1$ let F_n be the free group generated by $x_1, \dots, x_n$. Define automorphisms $X_1, \dots, X_{n-1}$ of F_n by

$$X_i(x_j) = \begin{cases} x_i x_{i+1} x_i^{-1} & \text{if} \quad j = i, \\ x_i & \text{if} \quad j = i+1, \\ x_j & \text{if} \quad j \neq i, i+1. \end{cases}$$

Prove that there exists a morphism X of the braid group B_n into the group of automorphisms of F_n such that $X(\sigma_i) = X_i$ for all i.

3. (*Burau representations*) (a) Let $n > 1$ be an integer and $\{v_1, \dots, v_n\}$ be a basis of a free $\mathbf{Z}[t, t^{-1}]$-module V_n of rank n. For any i such that $1 \leq i \leq n-1$ define an automorphism β_i of V_n by $\beta_i(v_k) = v_k$ if $k \neq i, i+1$, and

$$\beta_i(v_i) = (1-t)v_i + v_{i+1} \quad \text{and} \quad \beta_i(v_{i+1}) = tv_i.$$

Show that there exists a unique morphism β of the braid group B_n into the group of automorphisms of V_n such that $\beta(\sigma_i) = \beta_i$ for all i.

(b) Let $\{e_1, \dots, e_{n-1}\}$ be a basis of a free $\mathbf{Z}[t, t^{-1}]$-module V_{n-1} of rank $n-1$. For any i such that $1 < i < n-1$ define an automorphism

$\widetilde{\beta}_i$ of V_{n-1} by $\widetilde{\beta}_i(e_k) = e_k$ if $k \neq i$ and $\widetilde{\beta}_i(e_i) = te_{i-1} - te_i + e_{i+1}$ with the convention $e_0 = e_n = 0$. Show that there exists a unique morphism $\widetilde{\beta}$ of the braid group B_n into the group of automorphisms of V_{n-1} such that $\widetilde{\beta}(\sigma_i) = \widetilde{\beta}_i$ for all i. Prove that

$$\widetilde{\beta}\Big((\sigma_1 \cdots \sigma_{n-1})^n\Big) = t^n \,\mathrm{id}_{V_{n-1}}.$$

(c) When $n = 3$ and $t = -1$, prove that $\widetilde{\beta}$ induces a surjection of groups from B_3 onto the group $SL_2(\mathbf{Z})$ of integral 2×2-matrices with determinant one.

4. Define the pure braid group P_n as the kernel of the map $f \mapsto \sigma(f)$ from the braid group B_n to the symmetric group S_n. Show that P_n is isomorphic to the fundamental group of the space Y_n defined in 6.4.

5. (*Kauffman's bracket*) Show that the Kauffman bracket as defined in Section 8 is invariant under Reidemeister Transformations (0), (I'), (II) and (III) (Transformation (I') is the variant of Transformation (I) defined in Section 8).

X.8 Notes

Classical references on knot theory are [Bir74][BZ85][Kau87a][Rei32][Rol76]. The Jones polynomial V_L was defined in [Jon85] [Jon87]. Its two-variable extension P_L appeared in a number of papers written almost simultaneously [FYH+85] [Hos86] [LM87] [PT87] (see also [HKW86] [Kau91]). For Theorem 4.2 we followed the proof given by Turaev in [Tur89].

(*Smooth tangles*) There is a version of tangles and isotopies where piece-wise-linear maps are replaced by C^∞ maps and the boundary condition of Definition 5.1 is replaced by a transversality condition. Such smooth tangles project to smooth tangle diagrams. It may be shown that smooth isotopy classes of smooth tangles are in bijection with isotopy classes of tangles as defined in Section 5 (see [BZ85]).

(*Framed tangles*) Let us define a *normal vector field* on a smooth tangle L as a C^∞ vector field on L that is nowhere tangent to L and that is given by the vector $(0, -1, 0)$ at all points of the boundary ∂L. One may suggestively think of a tangle with a normal vector field as a tangled ribbon defined as follows: one edge of the ribbon is the tangle itself whereas the other one is obtained from the first one by a small translation along the vector field. A *framing* of the tangle L is a homotopy class of normal vector fields on L where two normal vector fields are said to be homotopic if they can be deformed into one another within the class of normal vector fields. One can extend the concept of isotopy from tangles to tangles with framings. Isotopy classes of tangles with framings are called *framed tangles* or *ribbons*. We

shall see in Chapter XIV that ribbons give rise to an interesting categorical structure, the so-called ribbon categories.

Framed tangles can be represented by tangle diagrams in the sense of Section 5 just as ordinary tangles are. Take a tangle diagram. By definition, it represents the following framed tangle: the underlying tangle is the tangle represented by the diagram and the framing is determined by the constant normal vector field $(0, -1, 0)$ that is perpendicular to the plane of the diagram and points to the reader. Any framed tangled may be represented by a planar diagram in such a way. We already know this for the underlying unframed tangle. To represent a general framed tangle with a vector field whirling around it, it is enough to know how to represent a vertical tangle around which the vector field turns by an angle of 2π or of -2π. The corresponding ribbons appear in Figure 8.1 and may be represented by the diagrams of Figure 8.2.

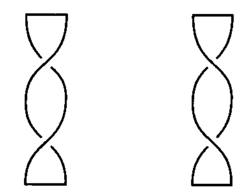

Figure 8.1.

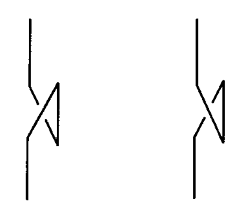

Figure 8.2.

There is an analogue of Reidemeister theorem for framed tangles. For this we need a variant (I') of Reidemeister Transformation (I). It is depicted in Figure 8.3. Two tangle diagrams represent isotopic *framed* tangles if and only if they can be obtained from one another by a finite sequence of Reidemeister Transformations (I'), (II), (III), and of isotopies of diagrams.

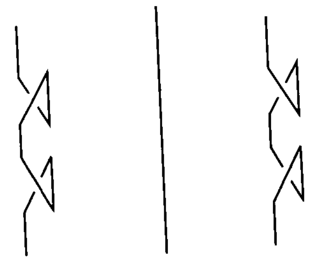

Figure 8.3. Reidemeister move (I')

(*Kauffman's bracket*) Shortly after Vaughan Jones's discovery of the link polynomial V_L, Louis Kauffman [Kau87b] found an isotopy invariant, now called the *Kauffman bracket*, for framed links. It is with values in the ring $\mathbf{Z}[x, x^{-1}]$ of Laurent polynomials. The Kauffman bracket $< L >$ can be characterized as follows. Take any diagram representing the framed link L. Single out a crossing. Define L_0 [resp. L_∞] to be the diagram where the crossing has been replaced by $||$ [resp. by $\substack{\cup \\ \cap}$]. Then the bracket is determined by the rules

$$< L >= x < L_0 > + x^{-1} < L_\infty >$$

and $< O^{\otimes n} >= (-1)^{n-1}(x^2 + x^{-2})^{n-1}$. The Jones polynomial can be recovered from the Kauffman bracket (see [Kau87b]).

(*Braid groups*) The braid groups were defined by E. Artin in [Art25]. Their presentation, as in Corollary 6.6, is also due to him [Art25][Art47]. The representations described in Exercise 3 were found by Burau in 1936 [Bur36]. The Burau representation is faithful for the braid group B_3. It has long been conjectured that the general Burau representation was faithful too. This was disproven recently by J.A. Moody [Moo91]. It is still an open question whether the braid groups B_n (for n large) have faithful finite-dimensional representations at all.

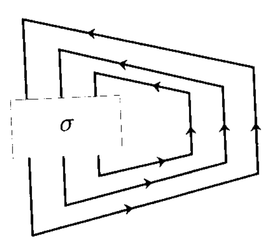

Figure 8.4. Closure of a braid

(*Closure of a braid*) For any braid $\sigma \in B_n$ define a link $\tilde{\sigma}$ by

$$\tilde{\sigma} = \sigma \cup \bigcup_{k=1}^{n} \Big([(k,0,0),(k,1,1/2)] \cup [(k,1,1/2)],(k,0,1)] \Big).$$

The link $\tilde{\sigma}$, called the closure of σ, is isotopic to the one represented in Figure 8.4. Alexander [Ale23] showed that any link in $\mathbf{R}^3$ was equivalent to the closure of some braid. Non-equivalent braids may have equivalent closures. Define an equivalence relation $\approx$ on the set of all braids by: $\sigma \approx \sigma'$ if σ and σ' have equivalent closures. Then Markov's theorem ([Mar36]; for a proof, see [Bir74]) states that $\approx$ is the equivalence relation generated by conjugation in the braid groups and by relations of the form $\sigma \approx i_n(\sigma)\sigma_n^{\pm 1}$ where $\sigma \in B_n$ and i_n is the morphism of B_n to B_{n+1} defined by $i_n(\sigma_i) = \sigma_i$ for $i = 1, \ldots, n-1$. As a consequence, any family $(f_n : B_n \to C)_{n>0}$ of set-theoretic maps with values in a set C such that for all n and all $\sigma, \tau \in B_n$

$$f_n(\tau\sigma\tau^{-1}) = f_n(\sigma) \quad \text{and} \quad f_n(\sigma) = f_{n+1}(i_n(\sigma)\sigma_n^{\pm 1}),$$

gives rise to a unique C-valued isotopy invariant f of links in $\mathbf{R}^3$ defined by $f(L) = f_n(\sigma)$ when L is equivalent to the closure of the braid $\sigma \in B_n$. This approach was used by V. Jones to construct the polynomial V_L in [Jon85] [Jon87]. It is to be observed that the approach using Markov's theorem is less elementary than the one by Reidemeister moves.

X.9 Appendix. The Fundamental Group

We briefly recall the definition of the fundamental group of a topological space. Set $I = [0,1]$.

Let X be a topological space with a distinguished point $\star$. A *loop* in X at the point $\star$ is a continuous map $f : I \to X$ such that $f(0) = f(1) = \star$. Denote the set of such maps by $\mathcal{L}_\star X$. Given elements f, g in $\mathcal{L}_\star X$ we define their *product* fg by

$$(fg)(t) = \begin{cases} f(2t) & \text{if} \quad 0 \le t \le 1/2, \\ g(2t-1) & \text{if} \quad 1/2 \le t \le 1. \end{cases}$$

The *constant loop* e is given by $e(t) = \star$. The *inverse* f^{-1} of f is defined by $f^{-1}(t) = f(1-t)$ for $t \in I$.

A *homotopy* from f to g is a continuous map $h : I \times I \to X$ such that

$$h(0,-) = f, \quad h(1,-) = g, \quad h(s,0) = h(s,1) = \star$$

for all $s \in I$. If such a homotopy exists, we write $f \sim g$. Homotopy is an equivalence relation. Indeed, it is

(a) reflexive because $(s,t) \mapsto f(t)$ is a homotopy from f to itself;

(b) symmetric: if h is a homotopy from f to g, then $h(1-s,-)$ is a homotopy from g to f;

(c) transitive: if h_1 and h_2 are homotopies from f_1 to f_2 and from f_2 to f_3 respectively, then

$$h(s,-) = \begin{cases} h_1(2s,-) & \text{if } 0 \le s \le 1/2, \\ h_2(2s-1,-) & \text{if } 1/2 \le s \le 1 \end{cases}$$

is a homotopy from f_1 to f_2.

We define $\pi_1(X,\star)$ as the set of homotopy classes in $\mathcal{L}_\star X$. We have the following lemma.

Lemma X.9.1. *Let f, f', f'', g, g' be elements of $\mathcal{L}_\star X$. Then*
(a) *$f \sim g$ and $f' \sim g'$ imply $ff' \sim gg'$,*
(b) *$(ff')f'' \sim f(f'f'')$,*
(c) *$fe \sim f \sim ef$, and*
(d) *$ff^{-1} \sim e \sim f^{-1}f$.*

PROOF. (a) If h [resp. h'] is a homotopy from f to g [resp. from f' to g'], then $(s,t) \mapsto (h(s,-)h'(s,-))(t)$ is a homotopy from ff' to gg'.

(b) A homotopy from $(ff')f''$ to $f(f'f'')$ is given by

$$h(s,t) = \begin{cases} f(\frac{4t}{s+1}) & \text{if } 0 \le t \le \frac{s+1}{4}, \\ f'(4t-s-1) & \text{if } \frac{s+1}{4} \le t \le \frac{s+2}{4}, \\ f''(\frac{4t-s-2}{2-s}) & \text{if } \frac{s+2}{4} \le t \le 1. \end{cases}$$

(c) The map

$$h(s,t) = \begin{cases} f(\frac{2t}{s+1}) & \text{if } 0 \le t \le \frac{s+1}{2}, \\ \star & \text{if } \frac{s+1}{2} \le t \le 1 \end{cases}$$

is a homotopy from fe to f. One can also exhibit a homotopy from ef to f.

(d) A homotopy from e to ff^{-1} is given by

$$h(s,t) = \begin{cases} f(2t) & \text{if } 0 \le 2t \le s, \\ f(s) & \text{if } s \le 2t \le 2-s, \\ f^{-1}(2t-1) & \text{if } 2-s \le 2t \le 2. \end{cases}$$

Exchange f and f^{-1} to get an homotopy from e to $f^{-1}f$. □

As a consequence, we see that the product of loops equips $\pi_1(X,\star)$ with the structure of a group in which the unit is the homotopy class of the constant loop e. This group is called the *fundamental group* of the topological space X at the point $\star$.

In the above definitions one may replace continuous maps by piecewise-linear or by C^∞ maps when X is an open subset of $\mathbf{R}^3$ or a quotient space of it. One gets a piecewise-linear or a smooth version of the fundamental group. These variants are isomorphic to the fundamental group defined above.

Chapter XI
Tensor Categories

This is our first chapter on tensor categories. As will become apparent in the sequel, tensor categories form the right framework for representations of Hopf algebras as well as for the topological objects of Chapter X. They provide a bridge between quantum groups and knot theory.

XI.1 The Language of Categories and Functors

We start with a few elementary definitions from category theory.

XI.1.1 Categories

Definition XI.1.1. *A category $\mathcal{C}$ consists*
(1) *of a class $\mathrm{Ob}(\mathcal{C})$ whose elements are called the objects of the category,*
(2) *of a class $\mathrm{Hom}(\mathcal{C})$ whose elements are called the morphisms of the category, and*
(3) *of maps*

$$\begin{array}{rcl} \textit{identity} & \mathrm{id} : & \mathrm{Ob}(\mathcal{C}) \to \mathrm{Hom}(\mathcal{C}), \\ \textit{source} & s : & \mathrm{Hom}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{C}), \\ \textit{target} & b : & \mathrm{Hom}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{C}), \\ \textit{composition} & \circ : & \mathrm{Hom}(\mathcal{C}) \times_{\mathrm{Ob}(\mathcal{C})} \mathrm{Hom}(\mathcal{C}) \to \mathrm{Ob}(\mathcal{C}), \end{array}$$

h that