A primer of Hopf algebras

Pierre Cartier

Institut Mathématique de Jussieu/CNRS, 175 rue du Chevaleret, F-75013 Paris
cartier@ihes.fr

Summary. In this paper, we review a number of basic results about so-called Hopf algebras. We begin by giving a historical account of the results obtained in the 1930's and 1940's about the topology of Lie groups and compact symmetric spaces. The climax is provided by the structure theorems due to Hopf, Samelson, Leray and Borel. The main part of this paper is a thorough analysis of the relations between Hopf algebras and Lie groups (or algebraic groups). We emphasize especially the category of unipotent (and prounipotent) algebraic groups, in connection with Milnor-Moore's theorem. These methods are a powerful tool to show that some algebras are free polynomial rings. The last part is an introduction to the combinatorial aspects of polylogarithm functions and the corresponding multiple zeta values.

1 Introduction

1.1. After the pioneer work of Connes and Kreimer[1], Hopf algebras have become an established tool in perturbative quantum field theory. The notion of Hopf algebra emerged slowly from the work of the topologists in the 1940's dealing with the cohomology of compact Lie groups and their homogeneous spaces. To fit the needs of topology, severe restrictions were put on these Hopf algebras, namely existence of a grading, (graded) commutativity, etc... The theory culminated with the structure theorems of Hopf, Samelson, Borel obtained between 1940 and 1950. The first part of this paper is devoted to a description of these results in a historical perspective.

1.2. In 1955, prompted by the work of J. Dieudonné on formal Lie groups [34], I extended the notion of Hopf algebra, by removing the previous restrictions[2]. Lie theory has just been extended by C. Chevalley [25] to the case of algebraic groups, but the correspondence between Lie groups and Lie algebras is invalid in the algebraic geometry of characteristic $p \neq 0$. In order to bypass this difficulty, Hopf algebras were introduced in algebraic geometry by Cartier, Gabriel, Manin, Lazard, Grothendieck and Demazure, ... with great success[3]. Here Hopf algebras play a dual role: first the (left) invariant differential operators on an algebraic group form a cocommutative Hopf algebra, which coincides with the enveloping algebra of the Lie algebra in characteristic 0, but not in characteristic p. Second: the regular functions on an affine algebraic group, under ordinary multiplication, form a commutative Hopf algebra. Our second part will be devoted to an analysis of the relations between groups and Hopf algebras.

1.3. The previous situation is typical of a general phenomenon of *duality between algebras*. In the simplest case, let G be a finite group. If k is any field, let kG be the group algebra of G: it is a vector space over k, with G as a

[1] See [26] in this volume.
[2] See my seminar [16], where the notions of coalgebra and comodule are introduced.
[3] The theory of Dieudonné modules is still today an active field of research, together with formal groups and p-divisible groups (work of Fontaine, Messing, Zink...).

basis, and the multiplication in G is extended to kG by linearity. Let also k^G be the set of all maps from G to k; with the pointwise operations of addition and multiplication k^G is a commutative algebra, while kG is commutative if, and only if, G is a commutative group. Moreover, there is a natural duality between the vector spaces kG and k^G given by

$$\left\langle \sum_{g \in G} a_g \cdot g, f \right\rangle = \sum_{g \in G} a_g \, f(g)$$

for $\sum a_g \cdot g$ in kG and f in k^G. Other instances involve the homology $H_\bullet(G; \mathbb{Q})$ of a compact Lie group G, with the Pontrjagin product, in duality with the cohomology $H^\bullet(G; \mathbb{Q})$ with the cup-product[4]. More examples:

- a locally compact group G, where the algebra $L^1(G)$ of integrable functions with the convolution product is in duality with the algebra $L^\infty(G)$ of bounded measurable functions, with pointwise multiplication;
- when G is a Lie group, one can replace $L^1(G)$ by the convolution algebra $C_c^{-\infty}(G)$ of distributions with compact support, and $L^\infty(G)$ by the algebra $C^\infty(G)$ of smooth functions.

Notice that, in all these examples, at least one of the two algebras in duality is (graded) commutative. A long series of structure theorems is summarized in the theorem of Cartier-Gabriel on the one hand, and the theorems of Milnor-Moore and Quillen on the other hand[5]. Until the advent of *quantum groups*, only sporadic examples were known where both algebras in duality are non-commutative, but the situation is now radically different. Unfortunately, no general structure theorem is known, even in the finite-dimensional case.

1.4. A related duality is *Pontrjagin duality* for commutative locally compact groups. Let G be such a group and $\hat{G}$ its Pontrjagin dual. If $\langle x, \hat{x} \rangle$ describes the pairing between G and $\hat{G}$, we can put in duality the convolution algebras $L^1(G)$ and $L^1(\hat{G})$ by

$$\langle f, \hat{f} \rangle = \int_G \int_{\hat{G}} f(x) \, \hat{f}(\hat{x}) \, \langle x, \hat{x} \rangle \, dx \, d\hat{x}$$

for f in $L^1(G)$ and $\hat{f}$ in $L^1(\hat{G})$. Equivalently the Fourier transformation $\mathcal{F}$ maps $L^1(G)$ into $L^\infty(\hat{G})$ and $L^1(\hat{G})$ into $L^\infty(G)$, exchanging the convolution product with the pointwise product $\mathcal{F}(f * g) = \mathcal{F}f \cdot \mathcal{F}g$. Notice that in this case the two sides $L^1(G)$ and $L^\infty(G)$ of the Hopf algebra attached to G are commutative algebras. When G is commutative and compact, its character group $\hat{G}$ is commutative and discrete. The elements of $\hat{G}$ correspond to continuous one-dimensional linear representations of G, and $\hat{G}$ is a basis of the

[4] Here, both algebras are finite-dimensional and graded-commutative.

[5] See subsection 3.8.

vector space $R_c(G)$ of continuous representative functions[6] on G. This algebra $R_c(G)$ is a subalgebra of the algebra $L^\infty(G)$ with pointwise multiplication. In this case, Pontrjagin duality theorem, which asserts that if $\hat{G}$ is the dual of G, then G is the dual of $\hat{G}$, amounts to the identification of G with the (real) *spectrum* of $R_c(G)$, that is the set of algebra homomorphisms from $R_c(G)$ to $\mathbb{C}$ compatible with the operation of complex conjugation.

1.5. Assume now that G is a *compact topological group*, not necessarily commutative. We can still introduce the ring $R_c(G)$ of continuous representative functions, and *Tannaka-Krein duality theorem* asserts that here also we recover G as the real spectrum of $R_c(G)$.

In order to describe $R_c(G)$ as a Hopf algebra, duality of vector spaces is not the most convenient way. It is better to introduce the *coproduct*, a map

$$\Delta : R_c(G) \to R_c(G) \otimes R_c(G)$$

which is an algebra homomorphism and corresponds to the product in the group via the equivalence

$$\Delta f = \sum_i f_i' \otimes f_i'' \Leftrightarrow f(g'g'') = \sum_i f_i'(g')\, f_i''(g'')$$

for f in $R_c(G)$ and g', g'' in G.

In the early 1960's, Tannaka-Krein duality was understood as meaning that a compact Lie group G is in an intrinsic way a *real algebraic group*, or rather the set $\Gamma(\mathbb{R})$ of the real points of such an algebraic group Γ. The complex points of Γ form the group $\Gamma(\mathbb{C})$, a complex reductive group of which G is a maximal compact subgroup (see [24], [72]).

1.6. It was later realized that the following notions:

- a group Γ together with a ring of representative functions, and the corresponding algebraic envelope,
- a commutative Hopf algebra,
- an affine group scheme,

are more or less equivalent. This was fully developed by A. Grothendieck and M. Demazure [31] (see also J.-P. Serre [72]).

The next step was the concept of a *Tannakian category*, as introduced by A. Grothendieck and N. Saavedra [69]. One of the formulations of the Tannaka-Krein duality for compact groups deals not with the representative ring, but the linear representations themselves. One of the best expositions is contained in the book [24] by C. Chevalley. An analogous theorem about semisimple *Lie algebras* was proved by Harish-Chandra [44]. The treatment of these two cases (compact Lie groups/semisimple Lie algebras) depends

[6] That is, the coefficients of the *continuous* linear representations of G in finite-dimensional vector spaces.

heavily on the *semisimplicity* of the representations. P. Cartier [14] was able to reformulate the problem without the assumption of semisimplicity, and to extend the Tannaka-Krein duality to an arbitrary algebraic linear group.

What Grothendieck understood is the following: if we start from a group (or Lie algebra) we have at our disposal various categories of representations. But, in many situations of interest in number theory and algebraic geometry, what is given is a certain category $\mathcal{C}$ and we want to create a group G such that $\mathcal{C}$ be equivalent to a category of representations of G. A similar idea occurs in physics, where the classification schemes of elementary particles rest on representations of a group to be discovered (like the isotopic spin group $SU(2)$ responsible for the pair $n-p$ of nucleons[7]).

If we relax some commutativity assumptions, we have to replace "group" (or "Lie algebra") by "Hopf algebra". One can thus give an axiomatic characterization of the category of representations of a Hopf algebra, and this is one of the most fruitful ways to deal with quantum groups.

1.7. G.C. Rota, in his lifelong effort to create a structural science of *combinatorics* recognised early that the pair product/coproduct for Hopf algebras corresponds to the use of the pair

assemble/disassemble

in combinatorics. Hopf algebras are now an established tool in this field. To quote a few applications:

- construction of free Lie algebras, and by duality of the shuffle product;
- graphical tensor calculus *à la* Penrose;
- trees and composition of operations;
- Young tableaus and the combinatorics of the symmetric groups and their representations;
- symmetric functions, noncommutative symmetric functions, quasi-symmetric functions;
- Faa di Bruno formula.

These methods have been applied to problems in topology (fundamental group of a space), number theory (symmetries of polylogarithms and multizeta numbers), and more importantly, via the notion of a Feynman diagram, to problems in quantum field theory (the work of Connes and Kreimer). In our third part, we shall review some of these developments.

1.8. The main emphasis of this book is about the mathematical methods at the interface of theoretical physics and number theory. Accordingly, our choice of topics is somewhat biased. We left aside a number of interesting subjects, most notably:

[7] For the foundations of this method, see the work of Doplicher and Roberts [35, 36].

- finite-dimensional Hopf algebras, especially semisimple and cosemisimple ones;
- algebraic groups and formal groups in characteristic $p \neq 0$ (see [16, 18]);
- quantum groups and integrable systems, that is Hopf algebras which are neither commutative, nor cocommutative.

Acknowledgments. These notes represent an expanded and improved version of the lectures I gave at les Houches meeting. Meanwhile, I lectured at various places (Chicago (University of Illinois), Tucson, Nagoya, Banff, Bertinoro, Bures-sur-Yvette) on this subject matter. I thank these institutions for inviting me to deliver these lectures, and the audiences for their warm response, and especially Victor Kac for providing me with a copy of his notes. I thank also my colleagues of the editorial board for keeping their faith and exerting sufficient pressure on me to write my contribution. Many special thanks for my typist, Cécile Cheikhchoukh, who kept as usual her smile despite the pressure of time.

2 Hopf algebras and topology of groups and *H*-spaces

2.1 Invariant differential forms on Lie groups

The theory of Lie groups had remained largely local from its inception with Lie until 1925, when H. Weyl [73] succeeded in deriving the characters of the semi-simple complex Lie groups using his "unitarian trick". One of the tools of H. Weyl was the theorem that the universal covering of a compact semi-simple Lie group is itself compact. Almost immediately, E. Cartan [11] determined explicitly the simply connected compact Lie groups, and from then on, the distinction between local and global properties of a Lie group has remained well established. The work of E. Cartan is summarized in his booklet [13] entitled "La théorie des groupes finis et continus et l'*Analysis situs*" (published in 1930).

The first results pertained to the *homotopy* of groups:

- for a compact semi-simple Lie group G, $\pi_1(G)$ is finite and $\pi_2(G) = 0$;
- any semi-simple connected Lie group is homeomorphic to the product of a compact semi-simple Lie group and a Euclidean space.

But, from 1926 on, E. Cartan was interested in the Betti numbers of such a group, or what is the same, the *homology* of the group. He came to this subject as an application of his theory of symmetric Riemannian spaces. A Riemannian space X is called symmetric[8] if it is connected and if, for any point a in X, there exists an isometry leaving a fixed and transforming any

[8] An equivalent definition is that the covariant derivative of the Riemann curvature tensor, namely the five indices tensor $R^i_{jk\ell;m}$, vanishes everywhere.

oriented geodesic through a into the same geodesic with the opposite orientation. Assuming that X is compact, it is a homogeneous space $X = G/H$, where G is a compact Lie group and H a closed subgroup. In his fundamental paper [12], E. Cartan proved the following result:

Let $\mathcal{A}^p(X)$ denote the space of exterior differential forms of degree p on X, $\mathcal{Z}^p(X)$ the subspace of forms ω such that $d\omega = 0$, and $\mathcal{B}^p(X)$ the subspace of forms of type $\omega = d\varphi$ with φ in $\mathcal{A}^{p-1}(X)$. Moreover, let $\mathcal{T}^p(X)$ denote the finite-dimensional space consisting of the G-invariant forms on X. Then $\mathcal{Z}^p(X)$ is the direct sum of $\mathcal{B}^p(X)$ and $\mathcal{T}^p(X)$. We get therefore a natural isomorphism of $\mathcal{T}^p(X)$ with the so-called de Rham cohomology group $H^p_{DR}(X) = \mathcal{Z}^p(X)/\mathcal{B}^p(X)$.

Moreover, E. Cartan gave an algebraic method to determine $\mathcal{T}^p(X)$, by describing an isomorphism of this space with the H-invariants in $\Lambda^p(\mathfrak{g}/\mathfrak{h})^*$ (where $\mathfrak{g}$, resp. $\mathfrak{h}$ is the Lie algebra of G resp. H).

We use the following notations:

- the Betti number $b_p(X)$ is the dimension of $H^p_{DR}(X)$ (or $\mathcal{T}^p(X)$);
- the Poincaré polynomial is

$$P(X,t) = \sum_{p\geq 0} b_p(X)\, t^p\,. \tag{1}$$

E. Cartan noticed that an important class of symmetric Riemannian spaces consists of the connected compact Lie groups. If K is such a group, with Lie algebra $\mathfrak{k}$, the adjoint representation of K in $\mathfrak{k}$ leaves invariant a positive definite quadratic form q (since K is compact). Considering $\mathfrak{k}$ as the tangent space at the unit e of K, there exists a Riemannian metric on K, invariant under left and right translations, and inducing q on $T_e\,K$. The symmetry s_a around the point a is given by $s_a(g) = a\,g^{-1}\,a$, and the geodesics through e are the one-parameter subgroups of K. Finally if $G = K \times K$ and H is the diagonal subgroup of $K \times K$, then G operates on K by $(g, g')\cdot x = g\,x\,g'^{-1}$ and K is identified to G/H. Hence $\mathcal{T}^p(K)$ is the space of exterior differential forms of degree p, invariant under left and right translations, hence it is isomorphic to the space $(\Lambda^p\,\mathfrak{k}^*)^K$ of invariants in $\Lambda^p\,\mathfrak{k}^*$ under the adjoint group.

Calculating the Poincaré polynomial $P(K,t)$ remained a challenge for 30 years. E. Cartan guessed correctly

$$P(SU(n),t) = (t^3+1)(t^5+1)\ldots(t^{2n-1}+1) \tag{2}$$

$$P(SO(2n+1),t) = (t^3+1)(t^7+1)\ldots(t^{4n-1}+1) \tag{3}$$

as early as 1929, and obtained partial general results like $P(K,1) = 2^\ell$ where ℓ is the *rank*[9] of K; moreover $P(K,t)$ is divisible by $(t^3+1)(t+1)^{\ell-1}$. When

[9] In a compact Lie group K, the maximal connected closed commutative subgroups are all of the same dimension ℓ, the *rank* of K, and are isomorphic to the

$\ell = 2$, E. Cartan obtained the Poincaré polynomial in the form $(t^3+1)(t^{r-3}+1)$ if K is of dimension r. This settles the case of G_2. In 1935, R. Brauer [10] proved the results (2) and (3) as well as the following formulas

$$P(Sp(2n),t) = (t^3+1)(t^7+1)\dots(t^{4n-1}+1) \tag{4}$$

$$P(SO(2n),t) = (t^3+1)(t^7+1)\dots(t^{4n-5}+1)(t^{2n-1}+1)\,. \tag{5}$$

The case of the exceptional simple groups F_4, E_6, E_7, E_8 eluded all efforts until A. Borel and C. Chevalley [5] settled definitely the question in 1955. It is now known that to each compact Lie group K of rank ℓ is associated a sequence of integers $m_1 \leq m_2 \leq \ldots \leq m_\ell$ such that $m_1 \geq 0$ and

$$P(K,t) = \prod_{i=1}^{\ell} (t^{2m_i+1}+1)\,. \tag{6}$$

The *exponents* $m_1, \ldots, m_\ell$ have a wealth of properties[10] for which we refer the reader to N. Bourbaki [7].

Here we sketch R. Brauer's proof[11] for the case of $SU(n)$, or rather $U(n)$. The complexified Lie algebra of $U(n)$ is the algebra $\mathfrak{gl}_n(\mathbb{C})$ of complex $n \times n$ matrices, with the bracket $[A,B] = AB - BA$. Introduce the multilinear forms T_p on $\mathfrak{gl}_n(\mathbb{C})$ by

$$T_p(A_1, \ldots, A_p) = \mathrm{Tr}(A_1 \ldots A_p)\,. \tag{7}$$

By the fundamental theorem of invariant theory[12], any multilinear form on $\mathfrak{gl}_n(\mathbb{C})$ invariant under the group $U(n)$ (or the group $GL(n,\mathbb{C})$) is obtained from $T_1, T_2, \ldots$ by tensor multiplication and symmetrization. Hence any invariant antisymmetric multilinear form is a linear combination of forms obtained from a product $T_{p_1} \otimes \ldots \otimes T_{p_r}$ by complete antisymmetrization. If we denote by Ω_p the complete antisymmetrization of T_p, the previous form is $\Omega_{p_1} \wedge \ldots \wedge \Omega_{p_r}$. Some remarks are in order:

---

torus $\mathbb{T}^\ell = \mathbb{R}^\ell/\mathbb{Z}^\ell$. For instance, among the classical groups, $SU(n+1)$, $SO(2n)$, $SO(2n+1)$ and $Sp(2n)$ are all of rank n.

[10] For instance, the dimension of K is $\ell + 2\sum_{i=1}^{\ell} m_i$, the order of the Weyl group W is $|W| = \prod_{i=1}^{\ell}(m_i+1)$, the invariants of the adjoint group in the symmetric algebra $S(\mathfrak{k})$ form a polynomial algebra with generators of degrees $m_1+1, \ldots, m_\ell+1$. Similarly the invariants of the adjoint group in the exterior algebra $\Lambda(\mathfrak{k})$ form an exterior algebra with generators of degrees $2m_1+1, \ldots, 2m_\ell+1$.

[11] See a detailed exposition in H. Weyl [74], sections 7.11 and 8.16. It was noticed by Hodge that $\mathcal{T}^p(X)$, for a compact Riemannian symmetric space X, is also the space of harmonic forms of degree p. This fact prompted Hodge to give in Chapter V of his book [45] a detailed account of the Betti numbers of the classical compact Lie groups.

[12] See theorem (2.6.A) on page 45 in H. Weyl's book [74].

- if p is even, T_p is invariant under the cyclic permutation γ_p of $1, \ldots, p$, but γ_p has signature -1; hence by antisymmetrization $\Omega_p = 0$ for p even;
- by invariant theory, Ω_p for $p > 2n$ is decomposable as a product of forms of degree $\leq 2n-1$;
- the exterior product $\Omega_{p_1} \wedge \ldots \wedge \Omega_{p_r}$ is antisymmetric in $p_1, \ldots, p_r$.

It follows that the algebra $\mathcal{T}^\bullet(U(n)) = \bigoplus_{p \geq 0} \mathcal{T}^p(U(n))$ possesses a basis of the form

$$\Omega_{p_1} \wedge \ldots \wedge \Omega_{p_r}\,, \quad 1 \leq p_1 < \cdots < p_r < 2n\,, \quad p_i \text{ odd.}$$

Hence it is an exterior algebra with generators $\Omega_1, \Omega_3, \ldots, \Omega_{2n-1}$. To go from $U(n)$ to $SU(n)$, omit Ω_1. Then, remark that if $\mathcal{T}^\bullet(X)$ is an exterior algebra with generators of degrees $2m_i + 1$ for $1 \leq i \leq \ell$, the corresponding Poincaré polynomial is $\prod_{i=1}^{\ell} (t^{2m_i+1} + 1)$. Done!

On the matrix group $U(n)$ introduce the complex coordinates g_{jk} by $g = (g_{jk})$, and the differentials $dg = (dg_{jk})$. The Maurer-Cartan forms are given by

$$dg_{jk} = \sum_m g_{jm}\, \omega_{mk} \tag{8}$$

or, in matrix form, by $\Omega = g^{-1}\, dg$. Introducing the exterior product of matrices of differential forms by

$$(A \wedge B)_{jk} = \sum_m a_{jm} \wedge b_{mk}\,, \tag{9}$$

then we can write

$$\Omega_p = \operatorname{Tr}(\underbrace{\Omega \wedge \ldots \wedge \Omega}_{p \text{ factors}}) = \sum_{i_1 \ldots i_p} \omega_{i_1 i_2} \wedge \omega_{i_2 i_3} \wedge \ldots \wedge \omega_{i_p i_1}\,. \tag{10}$$

Since $\bar{\omega}_{jk} = -\omega_{kj}$, it follows that the differential forms $i^m\, \Omega_{2m-1}$ (for $m = 1, \ldots, n$) are *real*.

2.2 de Rham's theorem

In the memoir [12] already cited, E. Cartan tried to connect his results about the invariant differential forms in $\mathcal{T}^p(X)$ to the Betti numbers as defined in *Analysis Situs* by H. Poincaré [61]. In section IV of [12], E. Cartan states three theorems, and calls "very desirable" a proof of these theorems. He remarks in a footnote that they have just been proved by G. de Rham. Indeed it is the subject matter of de Rham's thesis [33], defended and published in 1931. As mentioned by E. Cartan, similar results were already stated (without proof and in an imprecise form) by H. Poincaré.

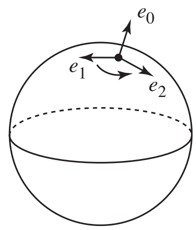

Fig. 1. e_0, e_1, e_2 positively oriented on V in $\mathbb{R}^3$, V the ball, bV the sphere, e_1, e_2 positively oriented on bV.

We need a few definitions. Let X be a smooth compact manifold (without boundary) of dimension n. We consider closed submanifolds V of dimension p in X, with a boundary denoted by bV. An orientation of V and an orientation of bV are compatible if, for every positively oriented frame $e_1, \ldots, e_{p-1}$ for bV at a point x of bV, and a vector e_0 pointing to the outside of V, the frame $e_0, e_1, \ldots, e_{p-1}$ is positively oriented for V. *Stokes formula* states that $\int_{bV} \varphi$ is equal to $\int_V d\varphi$ for every differential form φ in $\mathcal{A}^{p-1}(X)$. In particular, if V is a cycle (that is $bV = 0$) then the *period* $\int_V \omega$ of a form ω in $\mathcal{A}^p(X)$ is 0 if ω is a coboundary, that is $\omega = d\varphi$ for some φ in $\mathcal{A}^{p-1}(X)$.

de Rham's first theorem is a converse statement:

A. *If ω belongs to $\mathcal{A}^p(X)$, and is not a coboundary, then at least one period $\int_V \omega$ is not zero.*

As before, define the kernel $\mathcal{Z}^p(X)$ of the map $d : \mathcal{A}^p(X) \to \mathcal{A}^{p+1}(X)$ and the image $\mathcal{B}^p(X) = d\,\mathcal{A}^{p-1}(X)$. Since $dd = 0$, $\mathcal{B}^p(X)$ is included in $\mathcal{Z}^p(X)$ and we are entitled to introduce the de Rham cohomology group

$$H^p_{DR}(X) = \mathcal{Z}^p(X)/\mathcal{B}^p(X)\,.$$

It is a vector space over the real field $\mathbb{R}$, of finite dimension $b_p(X)$. According to Stokes theorem, for each submanifold V of X, without boundary, there is a linear form I_V on $H^p_{DR}(X)$, mapping the coset $\omega + \mathcal{B}^p(X)$ to $\int_V \omega$. According to theorem **A.**, the linear forms I_V span the space $H_p^{DR}(X)$ dual to $H^p_{DR}(X)$ (the so-called de Rham homology group). More precisely

B. *The forms I_V form a lattice $H_p^{DR}(X)_{\mathbb{Z}}$ in $H_p^{DR}(X)$.*

By duality, the cohomology classes $\omega + \mathcal{B}^p(X)$ of the closed forms with integral periods form a lattice $H^p_{DR}(X)_{\mathbb{Z}}$ in $H^p_{DR}(X)$.

We give now a topological description of these lattices. Let A be a commutative ring; in our applications A will be $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$. Denote by

$C_p(A)$ the free A-module with basis $[V]$ indexed by the (oriented[13]) closed connected submanifolds V of dimension p. There is an A-linear map

$$b : C_p(A) \to C_{p-1}(A)$$

mapping $[V]$ to $[bV]$ for any V. Since $bb = 0$, we define $H_p(X; A)$ as the

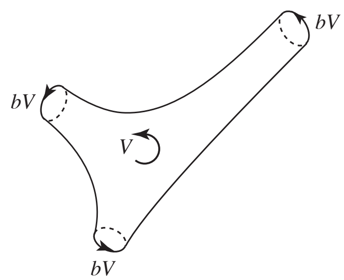

Fig. 2.

quotient of the kernel of $b : C_p(A) \to C_{p-1}(A)$ by the image of $b : C_{p+1}(A) \to C_p(A)$. By duality, $C^p(A)$ is the A-module dual to $C_p(A)$, and $\delta : C^p(A) \to C^{p+1}(A)$ is the transpose of $b : C_{p+1}(A) \to C_p(A)$. Since $\delta\delta = 0$, we can define the cohomology groups $H^p(X; A)$. Since X is compact, it can be shown that both $H_p(X; A)$ and $H^p(X; A)$ are *finitely generated A-modules*.

Here is the third statement:

C. *Let T_p be the torsion subgroup of the finitely generated $\mathbb{Z}$-module $H_p(X; \mathbb{Z})$. Then $H_p^{DR}(X)_{\mathbb{Z}}$ is isomorphic to $H_p(X; \mathbb{Z})/T_p$. A similar statement holds for $H^p_{DR}(X)_{\mathbb{Z}}$ and $H^p(X; \mathbb{Z})$. Hence, the Betti number $b_p(X)$ is the rank of the $\mathbb{Z}$-module $H_p(X; \mathbb{Z})$ and also of $H^p(X; \mathbb{Z})$.*

If the ring A has no torsion as a $\mathbb{Z}$-module (which holds for A equal to $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$), we have isomorphisms

$$H_p(X; A) \cong H_p(X; \mathbb{Z}) \otimes_{\mathbb{Z}} A\,, \tag{11}$$

$$H^p(X; A) \cong H^p(X; \mathbb{Z}) \otimes_{\mathbb{Z}} A\,. \tag{12}$$

Using Theorem **C.**, we get isomorphisms

$$H_p(X; \mathbb{R}) \cong H_p^{DR}(X), \quad H^p(X; \mathbb{R}) \cong H^p_{DR}(X)\,; \tag{13}$$

[13] If $\bar{V}$ is V with the reversed orientation, we impose the relation $[\bar{V}] = -[V]$: notice the integration formula $\int_{\bar{V}} \omega = -\int_V \omega$ for any p-form ω. The boundary bV is not necessarily connected (see fig. 2). If $B_1, \ldots, B_r$ are its components, with matching orientations, we make the convention $[bV] = [B_1] + \cdots + [B_r]$.

moreover, we can identify $H^p(X;\mathbb{Q})$ with the $\mathbb{Q}$-subspace of $H^p_{DR}(X)$ consisting of cohomology classes of p-forms ω all of whose periods are rational. The de Rham isomorphisms

$$H^p_{DR}(X) \cong H^p(X;\mathbb{R}) \cong H^p(X;\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{R}$$

are a major piece in describing *Hodge structures*.

To complete the general picture, we have to introduce products in cohomology. The exterior product of forms satisfies the Leibniz rule

$$d(\alpha \wedge \beta) = d\alpha \wedge \beta + (-1)^{\deg \alpha}\, \alpha \wedge d\beta\,, \tag{14}$$

hence[14] $\mathcal{Z}^\bullet(X)$ is a subalgebra of $\mathcal{A}^\bullet(X)$, and $\mathcal{B}^\bullet(X)$ an ideal in $\mathcal{Z}^\bullet(X)$; the quotient space $H^\bullet_{DR}(X) = \mathcal{Z}^\bullet(X)/\mathcal{B}^\bullet(X)$ inherits a product from the exterior product in $\mathcal{A}^\bullet(X)$. Topologists have defined a so-called *cup-product* in $H^\bullet(X;A)$, and the de Rham isomorphism is compatible with the products. Here is a corollary:

D. *If α, β are closed forms with integral (rational) periods, the closed form $\alpha \wedge \beta$ has integral (rational) periods.*

The next statement is known as *Poincaré duality*:

E. *Given any topological cycle V of dimension p in X, there exists a closed form ω_V of degree $n-p$ with integral periods such that*

$$\int_V \varphi = \int_X \omega_V \wedge \varphi \tag{15}$$

for any closed p-form φ.

The map $V \mapsto \omega_V$ extends to an isomorphism of $H_p^{DR}(X)$ with $H^{n-p}_{DR}(X)$, which is compatible with the lattices $H_p^{DR}(X)_{\mathbb{Z}}$ and $H^{n-p}_{DR}(X)_{\mathbb{Z}}$, hence it defines an isomorphism[15]

$$H_p(X;\mathbb{Q}) \cong H^{n-p}(X;\mathbb{Q})$$

known as *Poincaré isomorphism*. The cup-product on the right-hand side defines a product $(V,W) \mapsto V \cdot W$ from[16] $H_p \otimes H_q$ to H_{p+q-n}, called *intersection product* [61]. Here is a geometric description: after replacing V (resp. W) by a cycle V' homologous to V (resp. W' homologous to W) we can assume that

[14] We follow the standard practice, that is $\mathcal{Z}^\bullet(X)$ is the direct sum of the spaces $\mathcal{Z}^p(X)$ and similarly in other cases.

[15] This isomorphism depends on the choice of an orientation of X; going to the opposite orientation multiplies it by -1.

[16] Here H_p is an abbreviation for $H_p(X;\mathbb{Q})$.

V' and W' are *transverse*[17] to each other everywhere. Then the intersection $V' \cap W'$ is a cycle of dimension $p + q - n$ whose class in H_{p+q-n} depends only on the classes of V in H_p and W in H_q. In the case $p = 0$, a 0-cycle z is a linear combination $m_1 \cdot x_1 + \cdots + m_r \cdot x_r$ of points; the degree $\deg(z)$ is $m_1 + \cdots + m_r$. The Poincaré isomorphism $H_0(X; \mathbb{Q}) \cong H^n(X; \mathbb{Q})$ satisfies the property

$$\deg(V) = \int_X \omega_V \tag{16}$$

for any 0-cycle V. As a corollary, we get

$$\deg(V \cdot W) = \int_X \omega_V \wedge \omega_W \tag{17}$$

for any two cycles of complementary dimension.

2.3 The theorems of Hopf and Samelson

Between 1935 and 1950, a number of results about the topology of compact Lie groups and their homogeneous spaces were obtained. We mention the contributions of Ehresmann, Hopf, Stiefel, de Siebenthal, Samelson, Leray, Hirsch, Borel,... They used alternatively methods from differential geometry (through de Rham's theorems) and from topology.

Formula (6) for the Poincaré polynomial is "explained" by the fact that the cohomology $H^\bullet(K; \mathbb{Q})$ of a compact Lie group K is an *exterior algebra* with generators of degrees $2m_1 + 1, \ldots, 2m_\ell + 1$. Hence we get an isomorphism

$$H^\bullet(K; \mathbb{Q}) \cong H^\bullet(S^{2m_1+1} \times \ldots \times S^{2m_\ell+1}; \mathbb{Q}) \,. \tag{18}$$

The same statement is valid for $\mathbb{Q}$ replaced by any $\mathbb{Q}$-algebra (for instance $\mathbb{R}$ or $\mathbb{C}$), but it is not true for the cohomology with integral coefficients: it was quite complicated to obtain the torsion of the groups $H^p(K; \mathbb{Z})$, an achievement due essentially to A. Borel [3].

It is well-known that $SU(2)$ is homeomorphic to S^3, that $U(1)$ is homeomorphic to S^1, hence $U(2)$ is homeomorphic to $S^1 \times S^3$ [*Hint*: use the decomposition

$$g = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \begin{pmatrix} x + iy & z + it \\ -z + it & x - iy \end{pmatrix} \tag{19}$$

with $x^2 + y^2 + z^2 + t^2 = 1$]. In general $U(n)$ and $S^1 \times S^3 \times \cdots \times S^{2n-1}$ have the same cohomology in any coefficients, but they are not homeomorphic for $n \geq 3$. Nevertheless, $U(n)$ can be considered as a principal fibre bundle with

[17] Transversality means that at each point x in $V' \cap W'$ we can select a coordinate system $(x^1, \ldots, x^n)$ such that V' is given by equations $x^1 = \ldots = x^r = 0$ and W' by $x^{r+1} = \ldots = x^{r+s} = 0$. Hence $\dim_x V' = n - r =: p$, $\dim_x W' = n - s =: q$ and $\dim_x(V' \cap W') = n - r - s = p + q - n$.

group $U(n-1)$ and a base space $U(n)/U(n-1)$ homeomorphic to S^{2n-1}. Using results of Leray proved around 1948, one can show that the spaces $U(n)$ and $U(n-1) \times S^{2n-1}$ have the same cohomology, hence by induction on n the statement that $U(n)$ and $S^1 \times S^3 \times \cdots \times S^{2n-1}$ have the same cohomology. Similar geometric arguments, using Grassmannians, Stiefel manifolds,... have been used by Ch. Ehresmann [40] for the other classical groups. The first general proof that (for any connected compact Lie group K) *the cohomology* $H^\bullet(K;\mathbb{Q})$ *is an exterior algebra with generators of odd degree* was given by H. Hopf [47] in 1941. Meanwhile, partial results were obtained by L. Pontrjagin [63].

We have noticed that for any compact manifold X, *the cup-product* in cohomology maps $H^p \otimes H^q$ into H^{p+q}, where $H^p := H^p(X;\mathbb{Q})$. If X and Y are compact manifolds, and f is a continuous map from X to Y, there is a map f^* going backwards (the "Umkehrungs-Homomorphisms" of Hopf) from $H^\bullet(Y;\mathbb{Q})$ into $H^\bullet(X;\mathbb{Q})$ and *respecting the grading and the cup-product.* For homology, there is a natural map f_* from $H_\bullet(X;\mathbb{Q})$ to $H_\bullet(Y,\mathbb{Q})$, dual to f^* in the natural duality between homology and cohomology. We have remarked that, using Poincaré's duality isomorphism

$$H_p(X;\mathbb{Q}) \cong H^{n-p}(X;\mathbb{Q})$$

(where n is the dimension of X), one can define the *intersection product* mapping $H_p \otimes H_q$ into H_{p+q-n}. In general, the *map f_* from $H_\bullet(X;\mathbb{Q})$ to $H_\bullet(Y;\mathbb{Q})$ respects the grading, but not the intersection product*[18].

What Pontrjagin noticed is that when the manifold X is a compact Lie group K, there is another product in $H_\bullet(K;\mathbb{Q})$ (now called Pontrjagin's product) mapping $H_p \otimes H_q$ into H_{p+q}. It is defined as follows: the multiplication in K is a continuous map $m : K \times K \to K$ inducing a linear map for the homology groups (with rational coefficients)

$$m_* : H_\bullet(K \times K) \to H_\bullet(K)\,.$$

Since $H_\bullet(K \times K)$ is isomorphic to $H_\bullet(K) \otimes H_\bullet(K)$ by Künneth theorem, we can view m_* as a multiplication in homology, mapping $H_p(K) \otimes H_q(K)$ into $H_{p+q}(K)$. Hence both $H_\bullet(K;\mathbb{Q})$ and $H^\bullet(K;\mathbb{Q})$ are graded, finite-dimensional algebras, in duality. H. Samelson proved in [70] the conjecture made by Hopf at the end of his paper [47] that both $H_\bullet(K;\mathbb{Q})$ and $H^\bullet(K;\mathbb{Q})$ *are exterior algebras with generators of odd degree*. In particular, they are both graded-commutative[19]. It is a generic feature that the cohomology groups of a compact space X with arbitrary coefficients form a graded-commutative algebra

[18] Here is a simple counterexample. Assume that Y is a real projective space of dimension 3, X is a plane in Y, and $f : X \to Y$ the inclusion map. If L and L' are lines in X, their intersections $L \cdot L'$ in X is a point (of dimension 0). But their images in Y have a homological intersection product which is 0, because it is allowed to move L in Y to another line L_1 not meeting L'.

[19] This means that any two homogeneous elements a and b commute $ab = ba$, unless both are of odd degree and we have then $ab = -ba$

for the cup-product. But for the Pontrjagin product in homology, there are exceptions, for instance $H_\bullet(\mathrm{Spin}(n); \mathbb{Z}/2\mathbb{Z})$ for infinitely many values of n (see A. Borel [3]).

In his 1941 paper [47], H. Hopf considered a more general situation. He called[20] H-space any topological space X endowed with a continuous multiplication $m : X \times X \to X$ for which there exist two points a, b such that the maps $x \mapsto m(a, x)$ and $x \mapsto m(x, b)$ are homotopic[21] to the identity map of X. Using the induced map in cohomology and Künneth theorem, one obtains an algebra homomorphism

$$m^* : H^\bullet(X) \to H^\bullet(X \times X) = H^\bullet(X) \otimes_k H^\bullet(X)$$

where the cohomology is taken with coefficients in any field k. Assuming X to be a compact manifold, the k-algebra $H^\bullet(X)$ is finite-dimensional, and in duality with the space $H_\bullet(X)$ of homology. The multiplication in X defines a Pontrjagin product in $H_\bullet(X)$ as above. By duality[22], the maps

$$m^* : H^\bullet(X) \to H^\bullet(X) \otimes H^\bullet(X)$$

$$m_* : H_\bullet(X) \otimes H_\bullet(X) \to H_\bullet(X)$$

are transpose of each other. So the consideration of the Pontrjagin product in $H_\bullet(X)$, or of the coproduct m^* in $H^\bullet(X)$, are equivalent. Notice that the product m in the H-space X is neither assumed to be associative nor commutative (even up to homotopy).

The really new idea was the introduction of the coproduct m^*. The existence of this coproduct implies that $H^\bullet(K; \mathbb{Q})$ is an exterior algebra in a number of generators $c_1, \ldots, c_\lambda$ of odd degree. Hence if X is a compact H-space, it has the same cohomology as a product of spheres of odd dimension $S^{p_1} \times \cdots \times S^{p_\lambda}$. As proved by Hopf, there is no restriction on the sequence of odd dimensions $p_1, \ldots, p_\lambda$. The Poincaré polynomial is given by

$$P(X, t) = \prod_{i=1}^{\lambda} (1 + t^{p_i})$$

[20] His terminology is "Γ-Mannigfaltigkeit", where Γ is supposed to remind of G in "Group", and where the german "Mannigfaltigkeit" is usually translated as "manifold" in english. The standard terminology H-space is supposed to be a reminder of H(opf).

[21] It is enough to assume that they are homotopy equivalences.

[22] We put $H_\bullet \otimes H_\bullet$ and $H^\bullet \otimes H^\bullet$ in duality in such a way that

$$\langle a \otimes b, \alpha \otimes \beta \rangle = (-1)^{|b|\,|\alpha|} \langle a, \alpha \rangle \langle b, \beta \rangle$$

for a, b, α, β homogeneous. In general $|x|$ is the degree of a homogeneous element x. The sign is dictated by *Koszul's sign rule*: when you interchange homogeneous elements x, y, put a sign $(-1)^{|x|\,|y|}$.

and in particular the sum $P(X,1) = \sum_{p \geq 0} b_p(X)$ of the Betti numbers is equal to 2^λ. To recover E. Cartan's result $P(K,1) = 2^\ell$ (see [12]), we have to prove $\ell = \lambda$. This is done by Hopf in another paper [48] in 1941, as follows. Let K be a compact connected Lie group of dimension d; for any integer $m \geq 1$, let Ψ_m be the (contravariant) action on $H^\bullet(K;\mathbb{Q})$ of the map $g \mapsto g^m$ from K to K. This operator can be defined entirely in terms of the cup-product and the coproduct m^* in $H^\bullet(K;\mathbb{Q})$, that is in terms of the Hopf algebra $H^\bullet(K;\mathbb{Q})$ (see the proof of Theorem 3.8.1). It is easy to check that Ψ_m multiplies by m every primitive element in $H^\bullet(K;\mathbb{Q})$. According to Hopf [47] and Samelson [70], the algebra $H^\bullet(K;\mathbb{Q})$ is an exterior algebra generated by primitive elements $c_1, \ldots, c_\lambda$ of respective degree $p_1, \ldots, p_\lambda$. Then $p_1 + \cdots + p_\lambda$ is the dimension d of K, and $c = c_1 \ldots c_\lambda$ lies in $H^d(K;\mathbb{Q})$. The map Ψ_m respects the cup-product and multiply $c_1, \ldots, c_\lambda$ by m. Hence $\Psi_m(c) = m^\lambda c$. This means that the degree of the map $g \mapsto g^m$ from K to K is m^λ. But according to the classical topological results obtained in the 1930's by Hopf and others, this means that the equation $g^m = g_0$ has m^λ solutions g for a generic g_0. Using the known structure theorems for Lie groups, if g_0 lies in a maximal torus $T \subset K$, of dimension ℓ, the m-th roots of g_0 are in T for a generic g_0, but in a torus of dimension ℓ, each generic element has m^ℓ m-th roots. that is $m^\lambda = m^\ell$ for $m \geq 1$, hence $\ell = \lambda$.

Hopf was especially proud that his proofs were general and didn't depend on the classification of simple Lie groups. More than once, results about Lie groups have been obtained by checking through the list of simple Lie groups, and the search for a "general" proof has been a strong incentive.

2.4 Structure theorems for some Hopf algebras I

Let us summarize the properties of the cohomology $A^\bullet = H^\bullet(X;k)$ of a connected H-space X with coefficients in a field k.

(I) The space $A^\bullet$ is graded $A^\bullet = \bigoplus_{n \geq 0} A^n$, and connected $A^0 = k$.

(II) $A^\bullet$ is a graded-commutative algebra, that is there is given a multiplication $m : A^\bullet \otimes A^\bullet \to A^\bullet$ with the following properties[23]

$$\begin{array}{ll} |a \cdot b| = |a| + |b| & \text{(homogeneity)} \\ (a \cdot b) \cdot c = a \cdot (b \cdot c) & \text{(associativity)} \\ b \cdot a = (-1)^{|a|\,|b|}\, a \cdot b & \text{(graded commutativity),} \end{array}$$

for homogeneous elements a, b, c.

(III) There exists an element 1 in A^0 such that $1 \cdot a = a \cdot 1 = a$ for any a in $A^\bullet$ (unit).

[23] We write $a \cdot b$ for $m(a \otimes b)$ and $|a|$ for the degree of a.

(IV) There is a coproduct $\Delta : A^\bullet \to A^\bullet \otimes A^\bullet$, which is a homomorphism of graded algebras, such that $\Delta(a) - a \otimes 1 - 1 \otimes a$ belongs to $A_+ \otimes A_+$ for any a in A_+. Here we denote by A_+ the augmentation ideal $\underset{n\geq 1}{\oplus} A^n$ of $A^\bullet$.

Hopf's Theorem. (Algebraic version.) *Assume moreover that the field k is of characteristic 0, and that $A^\bullet$ is finite-dimensional. Then $A^\bullet$ is an exterior algebra generated by homogeneous elements of odd degree.*

Here is a sketch of the proof. It is quite close to the original proof by Hopf, except for the introduction of the filtration $(B_p)_{p\geq 0}$ and the associated graded algebra C. The idea of a filtration was introduced only later by J. Leray [52].

A. Besides the augmentation ideal $B_1 = A_+$, introduce the ideals $B_2 = A_+ \cdot A_+$, $B_3 = A_+ \cdot B_2$, $B_4 = A_+ \cdot B_3$ etc. We have a decreasing sequence

$$A^\bullet = B_0 \supset B_1 \supset B_2 \supset \dots$$

with intersection 0 since B_p is contained in $\underset{i\geq p}{\oplus} A^i$. We can form the corresponding (bi)graded[24] algebra

$$C = \bigoplus_{p\geq 0} B_p/B_{p+1}\,.$$

It is associative and graded-commutative (with respect to the second degree q in $C^{p,q}$). But now it is generated by B_1/B_2 that is $C^{1,\bullet} = \underset{q\geq 0}{\oplus} C^{1,q}$.

B. The coproduct $\Delta : A^\bullet \to A^\bullet \otimes A^\bullet$ maps B_p in $\sum_{i=0}^{p} B_i \otimes B_{p-i}$. Hence the filtration $(B_p)_{p\geq 0}$ is compatible with the coproduct Δ and since $C^{p,\bullet} = B_p/B_{p+1}$, Δ induces an algebra homomorphism $\delta : C \to C \otimes C$. The assumption $\Delta(a) - a \otimes 1 - 1 \otimes a$ in $A_+ \otimes A_+$ for any a in A_+ amounts to say that any element in $C^{1,\bullet}$ is *primitive*, that is

$$\delta(x) = x \otimes 1 + 1 \otimes x\,. \tag{20}$$

C. Changing slightly the notation, we consider an algebra $D^\bullet$ satisfying the assumptions (I) to (IV) and the extra property that $D^\bullet$ as an algebra is generated by the space $P^\bullet$ of primitive elements. First we prove that $P^\bullet$ has

[24] Each B_p is a graded subspace of $A^\bullet$, i.e. $B_p = \underset{q\geq 0}{\oplus} (B_p \cap A^q)$. Hence $C = \underset{p,q\geq 0}{\oplus} C^{p,q}$ with

$$C^{p,q} = (B_p \cap A^q)/(B_{p+1} \cap A^q)\,.$$

no homogeneous element of even degree. Indeed let x be such an element of degree $2m$. In $D^\bullet \otimes D^\bullet$ we have

$$\Delta(x^p) = x^p \otimes 1 + 1 \otimes x^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i \otimes x^{p-i} . \tag{21}$$

Since $D^\bullet$ is finite-dimensional, we can select p large enough so that $x^p = 0$. Hence we get $\Delta(x^p) = 0$ but in the decomposition (21), the various terms belong to different homogeneous components since $x^i \otimes x^{p-i}$ is in $D^{2mi} \otimes D^{2m(p-i)}$. They are all 0, and in particular $px \otimes x^{p-1} = 0$. We are in characteristic 0 hence $x \otimes x^{p-1} = 0$ in $D^{2m} \otimes D^{2m(p-1)}$ and this is possible only if $x = 0$.

D. By the previous result, $P^\bullet$ possesses a basis $(t_i)_{1 \leq i \leq r}$ consisting of homogeneous elements of odd degree. To show that $D^\bullet$ is the exterior algebra built on $P^\bullet$, we have to prove the following lemma:

Lemma 2.4.1. *If $t_1, \dots, t_r$ are linearly independent homogeneous primitive elements of odd degree, the products*

$$t_{i_1} \dots t_{i_s}$$

for $1 \leq i_1 < \dots < i_s \leq r$ are linearly independent.

Proof by induction on r. A relation between these elements can be written in the form $a + b\,t_r = 0$ where a, b depend on $t_1, \dots, t_{r-1}$ only. Apply Δ to this identity to derive $\Delta(a) + \Delta(b)\,(t_r \otimes 1 + 1 \otimes t_r) = 0$ and select the term of the form $u \otimes t_r$. It vanishes hence $b = 0$, hence $a = 0$ and by the induction hypothesis a linear combination of monomials in $t_1, \dots, t_{r-1}$ vanishes iff all coefficients are 0.

E. We know already that the algebra C in subsection **B.** is an exterior algebra over primitive elements of odd degrees. Lift the generators from $C^{1,\bullet}$ to B_1 to obtain independent generators of $A^\bullet$ as an exterior algebra.

2.5 Structure theorems for some Hopf algebras II

We shall relax the hypotheses in Hopf's theorem. Instead of assuming $A^\bullet$ to be finite-dimensional, we suppose that each component A^n is finite-dimensional.

A. *Suppose that the field k is of characteristic 0. Then $A^\bullet$ is a free graded-commutative algebra.*

More precisely, $A^\bullet$ is isomorphic to the tensor product of a symmetric algebra $S(V^\bullet)$ generated by a graded vector space $V^\bullet = \bigoplus_{n \geq 1} V^{2n}$ entirely in even degrees, and an exterior algebra $\Lambda(W^\bullet)$ where $W^\bullet = \bigoplus_{n\geq 0} W^{2n+1}$ is entirely in odd degrees.

B. *Assume that the field k is perfect of characteristic p different from 0 and 2. Then $A^\bullet$ is isomorphic to $S(V^\bullet)\otimes\Lambda(W^\bullet)\otimes B^\bullet$, where $B^\bullet$ is generated by elements $u_1, u_2, \dots$ of even degree subjected to relations of the form $u_i^{p^{m(i)}} = 0$ for $m(i)\geq 1$.*

Equivalently, the algebra $A^\bullet$ is isomorphic to a tensor product of a family (finite or infinite) of elementary algebras of the form $k[x]$, $\Lambda(\xi)$, $k[u]/(u^{p^m})$ with x, u of even degree and ξ of odd degree.

C. *Assume that the field k is perfect of characteristic 2. Then $A^\bullet$ is isomorphic to a tensor product of algebras of the type $k[x]$ or $k[x]/(x^{2^m})$ with x homogeneous.*

All the previous results were obtained by Borel in his thesis [1].

We conclude this section by quoting the results of Samelson [70] in an algebraic version. We assume that the field k is of characteristic 0, and that each vector space A^n is finite-dimensional. We introduce the vector space A_n dual to A^n and the graded dual $A_\bullet = \bigoplus_{n\geq 0} A_n$ of $A^\bullet$. Reasoning as in subsection 2.3, we dualize the coproduct

$$\Delta : A^\bullet \to A^\bullet \otimes A^\bullet$$

to a multiplication

$$\tilde{m} : A_\bullet \otimes A_\bullet \to A_\bullet\,.$$

D. *The following conditions are equivalent:*

(i) *The algebra $A^\bullet$ is generated by the subspace $P^\bullet$ of primitive elements.*
(ii) *With the multiplication $\tilde{m}$, the algebra $A_\bullet$ is associative and graded-commutative.*

The situation is now completely self-dual. The multiplication

$$m : A^\bullet \otimes A^\bullet \to A^\bullet$$

dualizes to a coproduct

$$\tilde{\Delta} : A_\bullet \to A_\bullet \otimes A_\bullet\,.$$

Denote by $P_\bullet$ the space of primitive elements in $A_\bullet$, that is the solutions of the equation $\tilde{\Delta}(x) = x\otimes 1 + 1\otimes x$. Then there is a natural duality between $P_\bullet$ and $P^\bullet$ and more precisely between the homogeneous components P_n and P^n.

Moreover $A^\bullet$ is the free graded-commutative algebra over $P^\bullet$ and similarly for $A_\bullet$ and $P_\bullet$.

In a topological application, we consider a compact Lie group K, and define

$$A^\bullet = H^\bullet(K;k)\,,\ A_\bullet = H_\bullet(K;k)$$

with the cup-product in cohomology, and the Pontrjagin product in homology. The field k is of characteristic 0, for instance $k = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. *Then both algebras $H^\bullet(K;k)$ and $H_\bullet(K;k)$ are exterior algebras with generators of odd degree.* Such results don't hold for general H-spaces. In a group, the multiplication is associative, hence the Pontrjagin product is associative. Dually, the coproduct

$$m^* : H^\bullet(K;k) \to H^\bullet(K;k) \otimes H^\bullet(K;k)$$

is coassociative (see subsection 3.5). Hence while results **A.**, **B.**, **C.** by Borel are valid for the cohomology of an arbitrary H-space, result **D.** by Samelson requires associativity of the H-space.

3 Hopf algebras in group theory

3.1 Representative functions on a group

Let G be a group and let k be a field. A *representation* π of G is a group homomorphism $\pi : G \to GL(V)$ where $GL(V)$ is the group of invertible linear maps in a finite-dimensional vector space V over k. We usually denote by V_π the space V corresponding to a representation π. Given a basis $(e_i)_{1\leq i\leq d(\pi)}$ of the space V_π, we can represent the operator $\pi(g)$ by the corresponding matrix $(u_{ij,\pi}(g))$. To π is associated a vector space $\mathcal{C}(\pi)$ of functions on G with values in k, the *space of coefficients*, with the following equivalent definitions:

- it is generated by the functions $u_{ij,\pi}$ for $1 \leq i \leq d(\pi)$, $1 \leq j \leq d(\pi)$;
- it is generated by the *coefficients*

$$c_{v,v^*,\pi} : g \mapsto \langle v^*, \pi(g)\cdot v\rangle$$

  for v in V_π, v^* in the dual V_π^* of V_π;
- it consists of the functions

$$c_{A,\pi} : g \mapsto \mathrm{Tr}\,(A\cdot \pi(g))$$

  for A running over the space $\mathrm{End}\,(V_\pi)$ of linear operators in V_π.

The union $R(G)$ of the spaces $\mathcal{C}(\pi)$ for π running over the class of representations of G is called the *representative space*. Its elements u are characterized by the following set of equivalent properties:

- the space generated by the left translates

$$L_{g'}u : g \mapsto u(g'^{-1}g)$$

of u (for g' in G) is finite-dimensional;
- similarly for the right translates

$$R_{g'}u : g \mapsto u(gg')\,;$$

- there exists finitely many functions u_i', u_i'' on G ($1 \leq i \leq N$) such that

$$u(g'g'') = \sum_{i=1}^{N} u_i'(g')\, u_i''(g'')\,. \tag{22}$$

An equivalent form of (22) is as follows: let us define

$$\Delta u : (g', g'') \mapsto u(g'g'')$$

for any function u on G, and identify $R(G) \otimes R(G)$ to a space of functions on $G \times G$, $u' \otimes u''$ being identified to the function $(g', g'') \mapsto u'(g')\, u''(g'')$. The rule of multiplication for matrices and the definition of a representation $\pi(g'g'') = \pi(g') \cdot \pi(g'')$ imply

$$\Delta\, u_{ij,\pi} = \sum_k u_{ik,\pi} \otimes u_{kj,\pi}\,. \tag{23}$$

Moreover, for u_i in $\mathcal{C}(\pi_i)$, the sum $u_1 + u_2$ is a coefficient of $\pi_1 \oplus \pi_2$ (direct sum) and $u_1 u_2$ a coefficient of $\pi_1 \otimes \pi_2$ (tensor product). We have proved the following lemma:

Lemma 3.1.1. *For any group G, the set $R(G)$ of representative functions on G is an algebra of functions for the pointwise operations and Δ is a homomorphism of algebras*

$$\Delta : R(G) \to R(G) \otimes R(G)\,.$$

Furthermore, there exist two algebra homomorphisms

$$S : R(G) \to R(G)\,, \quad \varepsilon : R(G) \to k$$

defined by

$$Su(g) = u(g^{-1})\,, \quad \varepsilon\, u = u(1)\,. \tag{24}$$

The maps Δ, S, ε are called, respectively, the coproduct, the antipodism[25] and the counit.

[25] The existence of the antipodism reflects the existence, for any representation π of the *contragredient* representation acting on V_π^* by $\pi^\vee(g) = {}^t\pi(g^{-1})$.

3.2 Relations with algebraic groups

Let G be a subgroup of the group $GL(d,k)$ of matrices. We say that G is an algebraic group if there exists a family (P_α) of polynomials in d^2 variables γ_{ij} with coefficients in k such that a matrix $g=(g_{ij})$ in $GL(d,k)$ belongs to G iff the equations $P_\alpha(\ldots g_{ij}\ldots)=0$ hold. The *coordinate ring* $\mathcal{O}(G)$ of G consists of rational functions on G regular at every point of G, namely the functions of the form

$$u(g)=P(\ldots g_{ij}\ldots)/(\det g)^N\,, \tag{25}$$

where P is a polynomial, and $N\geq 0$ an integer. The multiplication rule $\det(g'g'')=\det(g')\det(g'')$ implies that such a function u is in $R(G)$ and Cramer's rule for the inversion of matrices implies that Su is in $\mathcal{O}(G)$ for any u in $\mathcal{O}(G)$. Hence:

Lemma 3.2.1. *Let G be an algebraic subgroup of $GL(d,k)$. Then $\mathcal{O}(G)$ is a subalgebra of $R(G)$, generated by a finite number of elements*[26]*. Furthermore Δ maps $\mathcal{O}(G)$ into $\mathcal{O}(G)\otimes\mathcal{O}(G)$ and S maps $\mathcal{O}(G)$ into $\mathcal{O}(G)$. Finally, G is the spectrum of $\mathcal{O}(G)$, that is every algebra homomorphism $\varphi:\mathcal{O}(G)\to k$ corresponds to a unique element g of G such that φ is equal to $\delta_g:u\mapsto u(g)$.*

This lemma provides an intrinsic definition of an algebraic group as a pair $(G,\mathcal{O}(G))$ where $\mathcal{O}(G)$ satisfies the above properties. We give a short dictionary:

(i) If $(G,\mathcal{O}(G))$ and $(G',\mathcal{O}(G'))$ are algebraic groups, the homomorphisms of algebraic groups $\varphi:G\to G'$ are the group homomorphisms such that $\varphi^*(u'):=u'\circ\varphi$ is in $\mathcal{O}(G)$ for every u' in $\mathcal{O}(G')$.

(ii) The product $G\times G'$ is in a natural way an algebraic group such that $\mathcal{O}(G\times G')=\mathcal{O}(G)\otimes\mathcal{O}(G')$ (with the identification $(u\otimes u')(g,g')=u(g)\,u'(g')$).

(iii) A linear representation $u:G\to GL(n,k)$ is algebraic if and only if $u=(u_{ij})$ with elements u_{ij} in $\mathcal{O}(G)$ such that

$$\Delta\,u_{ij}=\sum_{k=1}^{n}u_{ik}\otimes u_{kj}\,. \tag{26}$$

More intrinsically, if $V=V_\pi$ is the space of a representation π of G, then V is a *comodule* over the *coalgebra* $\mathcal{O}(G)$, that is there exists a map $\Pi:V\to\mathcal{O}(G)\otimes V$ given by

$$\Pi(e_j)=\sum_{i=1}^{d(\pi)}u_{ij,\pi}\otimes e_i \tag{27}$$

[26] Namely the coordinates g_{ij} and the inverse $1/\det g$ of the determinant.

for any basis (e_i) of V and satisfying the rules[27]

$$(\varDelta \otimes 1_V) \circ \varPi = (1_{\mathcal{O}(G)} \otimes \varPi) \circ \varPi \,, \tag{28}$$

$$\pi(g) = (\delta_g \otimes 1_V) \circ \varPi \,. \tag{29}$$

3.3 Representations of compact groups

The purpose of this subsection is to show that any compact Lie group G is an algebraic group in a canonical sense. Here are the main steps in the proof:

(A) *Schur's orthogonality relations.*
(B) *Peter-Weyl's theorem.*
(C) *Existence of a faithful linear representation.*
(D) *Algebraicity of a compact linear group.*
(E) *Complex envelope of a compact Lie group.*

We shall consider only continuous complex representations of G. The corresponding representative algebra $R_c(G)$ consists of the complex representative functions which are continuous. We introduce in G a Haar measure m, that is a Borel measure which is both left and right-invariant:

$$m(gB) = m(Bg) = m(B) \tag{30}$$

for any Borel subset B of G and any g in G. We normalize m by $m(G) = 1$, and denote by $\int_G f(g)\, dg$ the corresponding integral. In the space $L^2(G)$ of square-integrable functions, we consider the scalar product

$$\langle f \mid f' \rangle = \int_G \overline{f(g)}\, f'(g)\, dg\,; \tag{31}$$

hence $L^2(G)$ is a (separable) Hilbert space.

Let $\pi : G \to GL(V)$ be a (continuous) representation of G. Let $\varPhi$ be any positive-definite hermitian form on $V_\pi = V$ and define

$$\langle v \mid v' \rangle = \int_G \varPhi(\pi(g) \cdot v, \pi(g) \cdot v')\, dg \tag{32}$$

for v, v' in V_π. This is a hermitian scalar product on V_π, invariant under G. Hence the representation π is *semisimple*, that is V_π is a direct sum $V_1 \oplus \cdots \oplus V_r$ of subspaces of V_π invariant under G, such that π induces an *irreducible* (or *simple*) representation π_i of G in the space V_i. Hence the vector space $\mathcal{C}(\pi)$ is the sum $\mathcal{C}(\pi_1) + \cdots + \mathcal{C}(\pi_r)$.

(A) *Schur's orthogonality relations.*

They can be given three equivalent formulations (π is an irreducible representation):

---

[27] In any vector space W, we denote by λ_W the multiplication by the number λ acting in W.

- the functions $d(\pi)^{1/2}\, u_{ij,\pi}$ form an orthonormal basis of the subspace[28] $\mathcal{C}(\pi)$ of $L^2(G)$;
- given vectors $v_1, \ldots, v_4$ in V_π, we have

$$\int_G \overline{\langle v_1 \,|\pi(g)|\, v_2\rangle}\ \langle v_3 \,|\pi(g)|\, v_4\rangle\, dg = d(\pi)^{-1}\ \overline{\langle v_1 \mid v_3\rangle}\ \langle v_2 \mid v_4\rangle\,; \tag{33}$$

- given two linear operators A, B in V_π, we have

$$\langle c_{A,\pi} \mid c_{B,\pi}\rangle = d(\pi)^{-1}\,\mathrm{Tr}(A^* B)\,. \tag{34}$$

The (classical) proof runs as follows. Let L be any operator in V_π. Then $L^\natural = \int_G \pi(g) \cdot L \cdot \pi(g^{-1})\, dg$ commutes to $\pi(G)$, hence by Schur's lemma, it is a scalar c_V. But obviously $\mathrm{Tr}(L^\natural) = \mathrm{Tr}(L)$, hence $c = \mathrm{Tr}(L)/d(\pi)$ and

$$L^\natural = d(\pi)^{-1}\,\mathrm{Tr}(L)\cdot 1_V\,. \tag{35}$$

Multiplying by an operator M in V_π and taking the trace, we get

$$\int_G \mathrm{Tr}(\pi(g)\, L\, \pi(g^{-1})\, M)\, dg = d(\pi)^{-1}\,\mathrm{Tr}(L)\,\mathrm{Tr}(M)\,. \tag{36}$$

Formula (33) is the particular case[29]

$$L = |v_4\rangle\langle v_2|\,, \quad M = |v_1\rangle\langle v_3| \tag{37}$$

of (36), since $\langle v \,|\pi(g^{-1})|\, v'\rangle = \overline{\langle v' \,|\pi(g)|\, v\rangle}$ by the unitarity of the operator $\pi(g)$. Specializing $v_1, \ldots, v_4$ to basis vectors e_i, we derive the orthonormality of the functions $d(\pi)^{1/2}\, u_{ij,\pi}$. Notice also that (34) reduces to (33) for

$$A = |v_2\rangle\langle v_1|\,, \quad B = |v_4\rangle\langle v_3| \tag{38}$$

and the general case follows by linearity.

Let now π and π' be two irreducible (continuous) non isomorphic representations of G. If $L : V_\pi \to V_{\pi'}$ is any linear operator define

$$L^\natural = \int_G \pi'(g)\cdot L \cdot \pi(g)^{-1}\, dg\,. \tag{39}$$

An easy calculation gives the *intertwining property*

$$\pi'(g)\, L^\natural = L^\natural\, \pi(g) \quad \text{for } g \text{ in } G. \tag{40}$$

Since π and π' are non isomorphic, we obtain $L^\natural = 0$ by Schur's lemma. Hence $\langle v' \,|L^\natural|\, v\rangle = 0$ for v in V_π and $v' \in V_{\pi'}$ and specializing to $L = |w'\rangle\langle w|$, we obtain the orthogonality relation

[28] The functions in $\mathcal{C}(\pi)$ being continuous, and G being compact, we have the inclusion $\mathcal{C}(\pi) \subset L^2(G)$.

[29] Here we use the *bra-ket notation*, hence L is the operator $v \mapsto \langle v_2 \mid v\rangle \cdot v_4$.

$$\int_G \overline{\langle v \,|\pi(g)|\, w\rangle}\ \langle v' \,|\pi'(g)|\, w'\rangle \, dg = 0 \,. \tag{41}$$

That is *the spaces* $\mathcal{C}(\pi)$ *and* $\mathcal{C}(\pi')$ *are orthogonal in* $L^2(G)$.

(B) *Peter-Weyl's theorem.*

We consider a collection $\hat{G}$ of irreducible (continuous) representations of G, such that every irreducible representation of G is isomorphic to one, and only one, member of $\hat{G}$. We keep the previous notations V_π, $d(\pi)$, $\mathcal{C}(\pi), \ldots$

Theorem of Peter-Weyl. *The family of functions* $d(\pi)^{1/2}\, u_{ij,\pi}$ *for* π *in* $\hat{G}$, $1 \leq i \leq d(\pi)$, $1 \leq j \leq d(\pi)$ *is an orthonormal basis of the Hilbert space* $L^2(G)$.

From the results in (A), we know already that the functions $d(\pi)^{1/2}\, u_{ij,\pi}$ form an orthonormal system and an algebraic basis of the vector space $R_c(G)$ of (continuous) representative functions. It suffices therefore to prove that $R_c(G)$ is a dense subspace of $L^2(G)$. Here is a simple proof[30].

For any continuous function f on G, define the convolution operator R_f in $L^2(G)$ by

$$(R_f\, \varphi)(g') = \int_G \varphi(g)\, f(g^{-1}\, g')\, dg \,. \tag{42}$$

This is an integral operator with a kernel $f(g^{-1}\, g')$ which is continuous on the compact space $G \times G$, hence in $L^2(G \times G)$. The operator R_f is therefore a *Hilbert-Schmidt operator*. By an elementary proof ([9], chapter 5), there exists an orthonormal basis (φ_n) in $L^2(G)$ such that the functions $R_f\, \varphi_n$ are mutually orthogonal. If we set $\lambda_n = \langle R_f\, \varphi_n \mid R_f\, \varphi_n\rangle$, it follows that $\lambda_n \geq 0$, $\sum\limits_n \lambda_n < +\infty$ (since R_f is Hilbert-Schmidt) and[31]

$$R_f^*\, R_f\, \varphi_n = \lambda_n\, \varphi_n \,. \tag{43}$$

From the relation $\sum\limits_n \lambda_n < +\infty$, it follows that for each $\lambda \neq 0$ the space $C_{\lambda,f}$ of solutions of the equation

$$R_f^*\, R_f\, \varphi = \lambda\, \varphi \tag{44}$$

is finite-dimensional. It is invariant under the left translations L_g since R_f commutes to L_g, and $R_f^*\, R_f$ transforms square-integrable functions into continuous functions by well-known properties of convolution. Hence $C_{\lambda,f}$ is a subspace of $R_c(G)$. If $I(f) := \operatorname{Im} R_f^*\, R_f$ is the range of the operator $R_f^*\, R_f$, it suffices to prove that the union of the ranges $I(f)$ for f continuous is dense in

[30] All known proofs [24], [55] rely on the theory of integral equations. Ours uses only the elementary properties of Hilbert-Schmidt operators.

[31] We denote by T^* the adjoint of any bounded linear operator T in $L^2(G)$.

$L^2(G)$. Choose a sequence (f_n) of continuous functions approximating[32] the Dirac "function" $\delta(g)$. Then for every continuous function φ in G, we have

$$\varphi = \lim_{n\to\infty} R^*_{f_n} R_{f_n} \varphi \tag{45}$$

uniformly on G, hence in $L^2(G)$. Moreover, the continuous functions are dense in $L^2(G)$. Q.E.D.

(C) *Existence of a faithful linear representation.*

Let $\mathfrak{g}$ be the Lie algebra of G, and $\exp : \mathfrak{g} \to G$ the exponential map. It is known that there exists a convex symmetric open set U in $\mathfrak{g}$ (containing 0) such that $\exp|_U$ is a homeomorphism of U onto an open subset V of G. Let $U_1 = \frac{1}{2}U$ and $V_1 = \exp(U_1)$. I claim that V_1 *contains no subgroup H of G, except $H = \{1\}$*. Indeed, for $h \in H$, $h \neq 1$ we can write $h = \exp x$, with $x \in U_1$, $x \neq 0$, hence $h^2 = \exp 2x$ belongs to V but not to V_1, hence not to H.

Since the Hilbert space $L^2(G)$ is separable, it follows from Peter-Weyl's theorem that we can enumerate $\hat{G}$ as a sequence $(\pi_n)_{n\geq 1}$. Denote by G_n the closed subgroup of G consisting of the elements g such that $\pi_1(g) = 1$, $\pi_2(g) = 1, \ldots, \pi_n(g) = 1$. Denote by H the intersection of the decreasing sequence $(G_n)_{n\geq 1}$. For h in H, it follows from Peter-Weyl's theorem that the left translation L_h in $L^2(G)$ is the identity, hence for any continuous function f on G, we have

$$f(h) = L_{h^{-1}} f(1) = f(1)\,, \tag{46}$$

hence $h = 1$ since the continuous functions on a compact space separate the points.

Hence $\bigcap_{n\geq 1} G_n = \{1\}$ and since V_1 is a neighborhood of 1, it follows from the compactness of G that V_1 contains one of the subgroups G_n, hence $G_n = \{1\}$ for some n by the first part of this proof. Otherwise stated, $\pi := \pi_1 \oplus \cdots \oplus \pi_n$ is a faithful representation.

(D) *Algebraicity of a compact linear group.*

Lemma 3.3.1. *Let $m \geq 1$ be an integer, and $K \subset GL(m, \mathbb{R})$ a compact subgroup. Then K is a real algebraic subgroup.*

Indeed, let g be a matrix[33] in $M_m(\mathbb{R})$, not in K. The closed subsets K and Kg of $M_m(\mathbb{R})$ are disjoint, hence there exists a continuous function φ on $K \cup Kg$ taking the value 0 on K and 1 on Kg. By Weierstrass' approximation

[32] That is, each f_n is continuous, non negative, normalized $\int_G f_n(g)\,dg = 1$, and there exists a basis (V_n) of the neighborhoods of 1 in G, such that f_n vanishes outside V_n.

[33] We denote by $M_m(\mathbb{R})$ the space of square matrices of size $m \times m$, with real entries.

theorem, we find a real polynomial in m^2 variables such that $|\varphi - P| \leq \frac{1}{4}$ on $K \cup Kg$. Average P:

$$P^\natural(h) = \int_K P(kh)\,dk\,. \tag{47}$$

Then $P^\natural$ is an invariant polynomial hence take constant values a on K, b on Kg. From $|\varphi - P| \leq \frac{1}{4}$ one derives $|a| \leq \frac{1}{4}$, $|1-b| \leq \frac{1}{4}$, hence $b \neq a$. The polynomial $P^\natural - a$ is identically 0 on K, and takes a non zero value at g. *Conclusion*: K is a real algebraic submanifold of the space $M_m(\mathbb{R})$ of square real matrices of order m.

(E) *Complex envelope of a compact Lie group.*

We can repeat for the real representations of G what was said for the complex representations: direct sum, tensor product, orthogonality, semisimplicity. For any complex representative function u, its complex conjugate $\bar{u}$ is a representative function, hence also the real and imaginary part of u. That is

$$R_c(G) = R_{c,\mathrm{real}}(G) \oplus i\,R_{c,\mathrm{real}}(G) \tag{48}$$

where $R_{c,\mathrm{real}}(G)$ is the set of continuous representative functions which take real values only. Moreover $R_{c,\mathrm{real}}(G)$ is the orthogonal direct sum $\bigoplus\limits_\pi \mathcal{C}(\pi)_\mathbb{R}$ extended over all irreducible real representations π of G, where $\mathcal{C}(\pi)_\mathbb{R}$ is the real vector space generated by the coefficients π_{ij} for π given in matrix form

$$\pi = (\pi_{ij}) : G \to GL(m,\mathbb{R})\,.$$

Since any complex vector space of dimension n can be considered as a real vector space of dimension $m = 2n$, and since G admits a faithful complex representation, we can select a faithful real representation ρ given in matrix form

$$\rho = (\rho_{ij}) : G \to GL(m;\mathbb{R})\,.$$

Theorem 3.3.1. (i) *Any irreducible real representation π of G is isomorphic to a subrepresentation of some $\rho^{\otimes N}$ with $N \geq 0$.*

(ii) *The algebra $R_{c,\mathrm{real}}(G)$ is generated by the functions ρ_{ij} for $1 \leq i \leq m$, $1 \leq j \leq m$.*

(iii) *The space G is the real spectrum*[34] *of the algebra $R_{c,\mathrm{real}}(G)$.*

Let I be the set of irreducible real representations π of G which are contained in some tensor representation $\rho^{\otimes N}$. Then, by the semisimplicity of real representations of G, the subalgebra of $R_{c,\mathrm{real}}(G)$ generated by $\mathcal{C}(\rho)_\mathbb{R}$ is the direct sum $A = \bigoplus\limits_{\pi \in I} \mathcal{C}(\pi)_\mathbb{R}$. Since the continuous real functions ρ_{ij} on G separate the points, it follows from the Weierstrass-Stone theorem that A is dense

[34] That is, for every algebra homomorphism $\varphi : R_{c,\mathrm{real}}(G) \to \mathbb{R}$ there exists a unique point g in G such that $\varphi(u) = u(g)$ for every u in $R_{c,\mathrm{real}}(G)$.

in the Banach space $C^0(G;\mathbb{R})$ of real continuous functions on G, with the supremum norm. Hence

$$A \subset R_{c,\mathrm{real}}(G) \subset C^0(G;\mathbb{R})\,.$$

If there existed an irreducible real representation σ not in I, then $\mathcal{C}(\sigma)_{\mathbb{R}}$ would be orthogonal to A in $L^2(G;\mathbb{R})$ by Schur's orthogonality relations. But A is dense in the Banach space $C^0(G;\mathbb{R})$, continuously and densely embedded in the Hilbert space $L^2(G;\mathbb{R})$, and its orthogonal complement reduces therefore to 0. Contradiction! This proves (i) and (ii).

The set $\Gamma = \rho(G)$ is real algebraic in the space $M_m(\mathbb{R})$, (by (D)), hence it is the real spectrum of the algebra $\mathcal{O}(\Gamma)$ generated by the coordinate functions on Γ. The bijection $\rho : G \to \Gamma$ transforms $R_{c,\mathrm{real}}(G)$ into $\mathcal{O}(\Gamma)$ by (ii), hence G is the real spectrum of $R_{c,\mathrm{real}}(G)$. Q.E.D.

Let $G(\mathbb{C})$ be the complex spectrum of the algebra $R_c(G)$. By the previous theorem and (48), the complex algebra $R_c(G)$ is generated by the ρ_{ij}'s. Furthermore as above, we show that ρ extends to an isomorphism $\rho_{\mathbb{C}}$ of $G(\mathbb{C})$ onto the smallest complex algebraic subgroup of $GL(m,\mathbb{C})$ containing $\rho(G) \subset GL(m,\mathbb{R})$. Hence $G(\mathbb{C})$ is a complex algebraic group, and there is an involution r in $G(\mathbb{C})$ with the following properties:

(i) *G is the set of fixed points of r in $G(\mathbb{C})$.*
(ii) *For u in $R_c(G)$ and g in $G(\mathbb{C})$, one has*

$$u(r(g)) = \overline{\overline{u}(g)} \tag{49}$$

and in particular $u(r(g)) = \overline{u(g)}$ for u in $R_{c,\mathrm{real}}(G)$.

The group $G(\mathbb{C})$ is called the *complex envelope of* G. For instance if $G = U(n)$, then $G(\mathbb{C}) = GL(n,\mathbb{C})$ with the natural inclusion $U(n) \subset GL(n,\mathbb{C})$ and $r(g) = (g^*)^{-1}$.

3.4 Categories of representations

We come back to the situation of subsection 3.1. We consider an "abstract" group G and the algebra $R(G)$ of representative functions on G together with the mappings Δ, S, ε.

Let L be a sub-Hopf-algebra of $R(G)$, that is a subalgebra such that $\Delta(L) \subset L \otimes L$, and $S(L) = L$. Denote by $\mathcal{C}_L$ the class of representations π of G such that $\mathcal{C}(\pi) \subset L$. We state the main properties:

(i) *If π_1 and π_2 are in the class $\mathcal{C}_L$, so are the direct sum $\pi_1 \oplus \pi_2$ and the tensor product $\pi_1 \otimes \pi_2$.*

(ii) *For any π in $\mathcal{C}_L$, every subrepresentation π' of π, as well as the quotient representation π/π' (in $V_\pi/V_{\pi'}$) are in $\mathcal{C}_L$.*

(iii) *For any representation* π *in* $\mathcal{C}_L$*, the contragredient representation*[35] $\pi^\vee$ *is in* $\mathcal{C}_L$*; the unit representation* $\mathbf{1}$ *is in* $\mathcal{C}_L$*.*

(iv) L *is the union of the spaces* $\mathcal{C}(\pi)$ *for* π *running over* $\mathcal{C}_L$*.*

Hints of proof:

- For (i), use the relations

$$\mathcal{C}(\pi_1 \oplus \pi_2) = \mathcal{C}(\pi_1) + \mathcal{C}(\pi_2)\,,\ \mathcal{C}(\pi_1 \otimes \pi_2) = \mathcal{C}(\pi_1)\,\mathcal{C}(\pi_2)\,.$$

- For (ii) use the relations

$$\mathcal{C}(\pi') \subset \mathcal{C}(\pi)\,,\ \mathcal{C}(\pi/\pi') \subset \mathcal{C}(\pi)\,.$$

- For (iii) use the relations

$$\mathcal{C}(\pi^\vee) = S(\mathcal{C}(\pi))\,,\ \mathcal{C}(\mathbf{1}) = \mathbb{C}\,.$$

- To prove (iv), let u in L. By definition of a representative function, the vector space V generated by the right translates of u is finite-dimensional, and the operators R_g define a representation ρ in V. Since u is in V, it remains to prove $V = \mathcal{C}(\rho)$. We leave it as an exercise for the reader.

Conversely, let $\mathcal{C}$ be a class of representations of G satisfying the properties analogous to (i) to (iii) above. Then the union L of the spaces $\mathcal{C}(\pi)$ for π running over $\mathcal{C}$ is a sub-Hopf-algebra of $R(G)$. In order to prove that $\mathcal{C}$ is the class $\mathcal{C}_L$ corresponding to L, one needs to prove the following lemma:

Lemma 3.4.1. *If* π *and* π' *are representations of* G *such that* $\mathcal{C}(\pi) \subset \mathcal{C}(\pi')$*, then* π *is isomorphic to a subquotient of* π'^N *for some integer* $N \geq 0$*.*

Proof left to the reader (see [72], page 47).

Consider again a sub-Hopf-algebra L of $R(G)$. Let G_L be the spectrum of L, that is the set of algebra homomorphisms from L to k. For g, g' in G_L, the map

$$g \cdot g' := (g \otimes g') \circ \Delta \tag{50}$$

is again in G_L, as well as $g \circ S$. It is easy to check that we define a multiplication in G_L which makes it a group, with $g \circ S$ as inverse of g, and $\varepsilon|_L$ as unit element. Furthermore, there is a group homomorphism

$$\delta : G \to G_L$$

[35] The contragredient $\pi^\vee$ of π acts on the dual V_π^* of V_π in such a way that

$$\langle \pi^\vee(g) \cdot v^*, v \rangle = \langle v^*, \pi(g^{-1}) \cdot v \rangle$$

for v in V_π, v^* in V_π^* and g in G. Equivalently $\pi^\vee(g) = {}^t\pi(g)^{-1}$.

transforming any g in G into the map $u \mapsto u(g)$ from L to k. The group G_L is called the *envelope of* G corresponding to the Hopf-algebra $L \subset R(G)$, or equivalently to the class $\mathcal{C}_L$ of representations of G corresponding to L.

We reformulate these constructions in terms of categories. Given two representations π, π' of G, let $\mathrm{Hom}(\pi, \pi')$ be the space of all linear operators $T : V_\pi \to V_{\pi'}$ such that $\pi'(g)\, T = T\, \pi(g)$ for all g in G ("intertwining operators"). With the obvious definition for the composition of intertwining operators, the *class* $\mathcal{C}_L$ *is a category*. Furthermore, one defines a functor Φ from $\mathcal{C}_L$ to the category Vect_k of finite-dimensional vector spaces over k: namely $\Phi(\pi) = V_\pi$ for π in $\mathcal{C}_L$ and $\Phi(T) = T$ for T in $\mathrm{Hom}(\pi, \pi')$. This functor is called the *forgetful functor*. Finally, the group $\mathrm{Aut}(\Phi)$ of automorphisms of the functor Φ consists of the families $g = (g_\pi)_{\pi \in \mathcal{C}_L}$ such that $g_\pi \in GL(V_\pi)$ and

$$g_{\pi'}\, T = T\, g_\pi \tag{51}$$

for π, π' in $\mathcal{C}_L$ and T in $\mathrm{Hom}(\pi, \pi')$. Hence $\mathrm{Aut}(\Phi)$ is a subgroup of $\prod_{\pi \in \mathcal{C}_L} GL(V_\pi)$.

With these definitions, one can identify G_L with the subgroup of $\mathrm{Aut}(\Phi)$ consisting of the elements $g = (g_\pi)$ satisfying the equivalent requirements:

(i) *For any* π *in* $\mathcal{C}_L$*, the operator* g_π *in* V_π *belongs to the smallest algebraic subgroup of* $GL(V_\pi)$ *containing the image* $\pi(G)$ *of the representation* π.

(ii) *For* π, π' *in* $\mathcal{C}_L$*, the operator* $g_{\pi \otimes \pi'}$ *in* $V_{\pi \otimes \pi'} = V_\pi \otimes V_{\pi'}$ *is equal to* $g_\pi \otimes g_{\pi'}$.

Examples. 1) Let G be an algebraic group, and $\mathcal{O}(G)$ its coordinate ring. For $L = \mathcal{O}(G)$, the class $\mathcal{C}_L$ of representations of G coincides with its class of representations as an algebraic group. In this case $\delta : G \to G_{\mathcal{O}(G)}$ is an isomorphism.

2) Let G be a compact Lie group and $L = R_c(G)$. Then the class $\mathcal{C}_L$ consists of the continuous complex representations of G, and G_L is the complex envelope $G(\mathbb{C})$ of G defined in subsection 3.3(E). Using the semisimplicity of the representations of G, we can reformulate the definition of $G_L = G(\mathbb{C})$: it is the subgroup of the product $\prod_{\pi \text{ irred.}} GL(V_\pi)$ consisting of the families $g = (g_\pi)$ such that $g_{\pi_1} \otimes g_{\pi_2} \otimes g_{\pi_3}$ fixes any element of $V_{\pi_1} \otimes V_{\pi_2} \otimes V_{\pi_3}$ which is invariant under G (for π_1, π_2, π_3 irreducible). In the embedding $\delta : G \to G(\mathbb{C})$, G is identified with the subgroup of $G(\mathbb{C}) \subset \prod_{\pi \text{ irred.}} GL(V_\pi)$ where each component g_π is a unitary operator in V_π. In this way, we recover the classical Tannaka-Krein duality theorem for compact Lie groups.

3) Let Γ be a discrete finitely generated group, and let $\mathcal{C}$ be the class of its unipotent representations over the field $\mathbb{Q}$ of rational numbers (see subsection 3.9). Then the corresponding envelope is called the unipotent (or Malcev) completion of Γ. This construction has been extensively used when Γ is the fundamental group of a manifold [21, 29].

Remark 3.4.1. If $\mathcal{C}$ is any k-linear category with an internal tensor product, and $\Phi : \mathcal{C} \to \mathrm{Vect}_k$ a functor respecting the tensor products, one can define the group $\mathrm{Aut}(\Phi)$ as above, and the subgroup $\mathrm{Aut}^{\otimes}(\Phi)$ of the elements $g = (g_\pi)$ of $\mathrm{Aut}(\Phi)$ satisfying the condition (ii) above. It can be shown that $\Gamma = \mathrm{Aut}^{\otimes}(\Phi)$ is the spectrum of a Hopf algebra L of representative functions on Γ; there is a natural functor from $\mathcal{C}$ to $\mathcal{C}_L$. Grothendieck, Saavedra [69] and Deligne [30] have given conditions ensuring the equivalence of $\mathcal{C}$ and $\mathcal{C}_L$ ("Tannakian categories").

3.5 Hopf algebras and duality

(A) We give at last the axiomatic description of a Hopf algebra. Take for instance a *finite group* G and a field k, and introduce the group algebra kG in duality with the space k^G of all maps from G to k (see subsection 1.3). The coproduct in kG is given by

$$\Delta\left(\sum_{g\in G} a_g \cdot g\right) = \sum_{g\in G} a_g \cdot (g \otimes g) \tag{52}$$

and the bilinear multiplication by

$$m(g \otimes g') = g \cdot g' \,. \tag{53}$$

Hence we have maps (for $A = kG$)

$$\Delta : A \to A \otimes A \,, \quad m : A \otimes A \to A$$

which satisfy the following properties:

Associativity[36] *of* $m : m \circ (m \otimes 1_A) = m \circ (1_A \otimes m)$.

Coassociativity of $\Delta : (\Delta \otimes 1_A) \circ \Delta = (1_A \otimes \Delta) \circ \Delta$.

Compatibility of m *and* Δ*: the following diagram is commutative*

$$\begin{array}{ccccc} A^{\otimes 2} & \xrightarrow{m} & A & \xrightarrow{\Delta} & A^{\otimes 2} \\ \Big\downarrow{\scriptstyle \Delta^{\otimes 2}} & & & & \Big\uparrow{\scriptstyle m^{\otimes 2}} \\ A^{\otimes 4} & & \xrightarrow{\sigma_{23}} & & A^{\otimes 4}\,, \end{array}$$

where $A^{\otimes 2} = A \otimes A$ and σ_{23} is the exchange of the factors A_2 and A_3 in the tensor product $A^{\otimes 4} = A_1 \otimes A_2 \otimes A_3 \otimes A_4$ (where each A_i is equal to A).

Furthermore the linear maps $S : A \to A$ and $\varepsilon : A \to k$ characterized by $S(g) = g^{-1}$, $\varepsilon(g) = 1$ satisfy the rules

$$m \circ (S \otimes 1_A) \circ \Delta = m \circ (1_A \otimes S) \circ \Delta = \eta \circ \varepsilon \,, \tag{54}$$

[36] In terms of elements this is the law $(a_1\, a_2)\, a_3 = a_1 (a_2\, a_3)$.

$$(\varepsilon \otimes 1_A) \circ \Delta = (1_A \otimes \varepsilon) \circ \Delta = 1_A \,, \tag{55}$$

and are uniquely characterized by these rules. We have introduced the map $\eta : k \to A$ given by $\eta(\lambda) = \lambda \cdot 1$ satisfying the rule[37]

$$m \circ (\eta \otimes 1_A) = m \circ (1_A \otimes \eta) = 1_A \,. \tag{56}$$

All these properties give the *axioms of a Hopf algebra* over the field k.

A word about terminology[38]. The map m is called the product, and η the unit map. An *algebra* is a triple (A, m, η) satisfying the condition of associativity for m and relation (56) for η, hence an algebra (A, m, η) is *associative and unital*. A *coalgebra* is a triple (A, Δ, ε) where Δ is called the coproduct and ε the counit. They have to satisfy the coassociativity for Δ and relation (55) for ε, hence a coalgebra is *coassociative and counital*. A *bialgebra* is a system $(A, m, \eta, \Delta, \varepsilon)$ where in addition of the previous properties, the compatibility of m and Δ holds. Finally a map S satisfying (54) is an *antipodism* for the bialgebra, and a *Hopf algebra* is a bialgebra with antipodism.

(B) When A is finite-dimensional, we can identify $A^* \otimes A^*$ to the dual of $A \otimes A$. Then the maps $\Delta, m, S, \varepsilon, \eta$ dualize to linear maps

$$\Delta^* = {}^t m \,, \quad m^* = {}^t \Delta \,, \quad S^* = {}^t S \,, \quad \varepsilon^* = {}^t \eta \,, \quad \eta^* = {}^t \varepsilon$$

by taking transposes. One checks that the axioms of a Hopf algebra are *self-dual*, hence $(A^*, m^*, \Delta^*, S^*, \varepsilon^*, \eta^*)$ is another Hopf algebra, the *dual* of $(A, m, \Delta, S, \varepsilon, \eta)$. In our example, where $A = kG$, $A^* = k^G$, the multiplication in k^G is the pointwise multiplication, and the coproduct is given by $\Delta^* u(g, g') = u(gg')$. Since G is finite, every function on G is a representative function, hence A^* is the Hopf algebra $R(G)$ introduced in subsection 3.1.

In general, if (A, Δ, ε) is any coalgebra, we can dualize the coproduct in A to a product in the dual A^* given by

$$f \cdot f' = (f \otimes f') \circ \Delta \,. \tag{57}$$

The product in A^* is associative[39], and ε acts as a unit

$$\varepsilon \cdot f = f \cdot \varepsilon = f \,. \tag{58}$$

Hence, the *dual of a coalgebra is an algebra.*

The duality for algebras is more subtle. Let (A, m, η) be an algebra, and define the subspace $R(A)$ of the dual A^* by the following characterization:

An element f of A^* is in $R(A)$ iff there exists a left (right, two-sided) *ideal I in A such that $f(I) = 0$ and A/I is finite-dimensional.*

[37] In terms of elements it means $1 \cdot a = a \cdot 1 = a$.

[38] Bourbaki, and after him Dieudonné and Serre, say “cogebra” for “coalgebra” and “bigebra” for “bialgebra”.

[39] This condition is equivalent to the coassociativity of Δ.

Equivalently $f \circ m : A^{\otimes 2} \to A \to k$ should be decomposable, that is there exist elements f_i', f_i'' in A^* such that

$$f(a'a'') = \sum_{i=1}^{N} f_i'(a')\, f_i''(a'') \tag{59}$$

for any pair of elements a', a'' of A. We can then select the elements f_i', f_i'' in $R(A)$ and define a coproduct in $R(A)$ by

$$\Delta(f) = \sum_{i=1}^{N} f_i' \otimes f_i'' \,. \tag{60}$$

Then $R(A)$ with the coproduct Δ, and the counit ε defined by $\varepsilon(f) = f(1)$, is a coalgebra, *the reduced dual of A*.

If $(A, m, \Delta, S, \varepsilon, \eta)$ is a Hopf algebra, the reduced dual $R(A)$ of the algebra (A, m, η) is a subalgebra of the algebra A^* dual to the coalgebra (A, Δ, ε). With these definitions, $R(A)$ is a Hopf algebra, the *reduced dual of the Hopf algebra A*.

Examples. 1) If A is finite-dimensional, $R(A)$ is equal to A^*, and the reduced dual Hopf algebra $R(A)$ coincides with the dual Hopf algebra A^*. In this case, the dual of A^* as a Hopf algebra is again A, but $R(R(A))$ is different from A for a general Hopf algebra A.

2) Suppose A is the group algebra kG with the coproduct (52). We don't assume that the group G is finite. Then $R(A)$ coincides with the algebra $R(G)$ of representative functions, with the structure of Hopf algebra defined in subsection 3.1 (see Lemma 3.1.1).

Remark 3.5.1. If (C, Δ, ε) is a coalgebra, its (full) dual C^* becomes an algebra for the product defined by (57). It can be shown (see [34], Chapter I) that the functor $C \mapsto C^*$ defines an equivalence of the category of coalgebras with the category of so-called *linearly compact algebras*. Hence, if $(A, m, \Delta, S, \varepsilon, \eta)$ is a Hopf algebra, the full dual A^* is a linearly compact algebra, and the multiplication $m : A \otimes A \to A$ dualizes to a coproduct $m^* : A^* \to A^* \hat{\otimes} A^*$, where $\hat{\otimes}$ denotes the completed tensor product in the category of linearly compact algebras.

3.6 Connection with Lie algebras

Another important example of a Hopf algebra is provided by the *enveloping algebra* $U(\mathfrak{g})$ of a Lie algebra $\mathfrak{g}$ over the field k. This is an associative unital algebra over k, containing $\mathfrak{g}$ as a subspace with the following properties:

- *as an algebra,* $U(\mathfrak{g})$ *is generated by* $\mathfrak{g}$*;*

- *for a, b in $\mathfrak{g}$, the bracket in $\mathfrak{g}$ is given by $[a,b] = ab - ba$;*
- *if A is any associative unital algebra, and $\rho : \mathfrak{g} \to A$ any linear map such that $\rho([a,b]) = \rho(a)\,\rho(b) - \rho(b)\,\rho(a)$, then ρ extends to a homomorphism of algebras $\bar{\rho} : U(\mathfrak{g}) \to A$ (in a unique way since $\mathfrak{g}$ generates $U(\mathfrak{g})$).*

In particular, taking for A the algebra of linear operators acting on a vector space V, we see that representations of the Lie algebra $\mathfrak{g}$ and representations of the associative algebra $U(\mathfrak{g})$ coincide.

One defines a linear map $\delta : \mathfrak{g} \to U(\mathfrak{g}) \otimes U(\mathfrak{g})$ by

$$\delta(x) = x \otimes 1 + 1 \otimes x\,. \tag{61}$$

It is easily checked that δ maps $[x,y]$ to $\delta(x)\,\delta(y) - \delta(y)\,\delta(x)$, hence δ extends to an algebra homomorphism Δ from $U(\mathfrak{g})$ to $U(\mathfrak{g}) \otimes U(\mathfrak{g})$. There exists also a homomorphism S from $U(\mathfrak{g})$ to $U(\mathfrak{g})^{\mathrm{op}}$ with the opposite multiplication mapping x to $-x$ for every x in $\mathfrak{g}$, and a homomorphism $\varepsilon : U(\mathfrak{g}) \to k$ vanishing identically on $\mathfrak{g}$ (this follows from the universal property of $U(\mathfrak{g})$). Then $U(\mathfrak{g})$ *with all its structure, is a Hopf algebra.*

Theorem 3.6.1. *Suppose that the field k is of characteristic 0. Then the Lie algebra $\mathfrak{g}$ can be recovered as the set of primitive elements in the Hopf algebra $U(\mathfrak{g})$, that is the solutions of the equation $\Delta(x) = x \otimes 1 + 1 \otimes x$.*

By (61), every element in $\mathfrak{g}$ is primitive. To prove the converse, assume for simplicity that the vector space $\mathfrak{g}$ has a finite basis $(x_1, \ldots, x_N)$. According to the Poincaré-Birkhoff-Witt theorem, the elements

$$Z_\alpha = \prod_{i=1}^{N} x_i^{\alpha_i} / \alpha_i\,! \tag{62}$$

for $\alpha = (\alpha_1, \ldots, \alpha_N)$ in $\mathbb{Z}_+^N$ form a basis of $U(\mathfrak{g})$. The coproduct satisfies

$$\Delta(Z_\alpha) = \sum_{\beta+\gamma=\alpha} Z_\beta \otimes Z_\gamma\,, \tag{63}$$

sum extended over all decompositions $\alpha = \beta + \gamma$ where β and γ are in $\mathbb{Z}_+^N$ and the sum is a vector sum. Let $u = \sum_\alpha c_\alpha\, Z_\alpha$ in $U(\mathfrak{g})$. We calculate

$$\Delta(u) - u \otimes 1 - 1 \otimes u = -c_0 \cdot 1 + \sum_{\substack{\beta \neq 0 \\ \gamma \neq 0}} c_{\beta+\gamma}\, Z_\beta \otimes Z_\gamma\,;$$

if u is primitive we have therefore $c_0 = 0$ and $c_{\beta+\gamma} = 0$ for $\beta, \gamma \neq 0$. This leaves only the terms $c_\alpha\, Z_\alpha$ where $\alpha_1 + \cdots + \alpha_N = 1$, that is a linear combination of $x_1, \ldots, x_N$. Hence u is in $\mathfrak{g}$. Q.E.D.

Remark 3.6.1. Let A be a Hopf algebra with the coproduct Δ. If π_i is a linear representation of A in a space V_i (for $i = 1, 2$), then we can define a representation $\pi_1 \otimes \pi_2$ of A in the space $V_1 \otimes V_2$ by

$$(\pi_1 \otimes \pi_2)(a) = \sum_i \pi_1(a_{i,1}) \otimes \pi_2(a_{i,2}) \tag{64}$$

if $\Delta(a) = \sum_i a_{i,1} \otimes a_{i,2}$. If A is of the form kG for a group G, or $U(\mathfrak{g})$ for a Lie algebra $\mathfrak{g}$, we recover the well-known constructions of the tensor product of two representations of a group or a Lie algebra. Similarly, the antipodism S gives a definition of the contragredient representation, and the counit ε that of the unit representation (in both cases, G or $\mathfrak{g}$).

3.7 A geometrical interpretation

We shall now discuss a theorem of L. Schwartz about Lie groups, which is an elaboration of old results of H. Poincaré [62]. See also [43].

Let G be a Lie group. We denote by $C^\infty(G)$ the algebra of real-valued smooth functions on G, with pointwise multiplication. The multiplication in G corresponds to a comultiplication

$$\Delta : C^\infty(G) \to C^\infty(G \times G)$$

given by

$$(\Delta\, u)(g_1, g_2) = u(g_1\, g_2)\,. \tag{65}$$

The algebra $C^\infty(G \times G)$ is bigger than the algebraic tensor product $C^\infty(G) \otimes C^\infty(G)$, but continuity properties enable us to dualize the coproduct Δ to a product (convolution) on a suitable dual of $C^\infty(G)$.

If we endow $C^\infty(G)$ with the topology of uniform convergence of all derivatives on all compact subsets of G, the dual is the space $C_c^{-\infty}(G)$ of *distributions* on G with compact support[40]. Let T_1 and T_2 be two such distributions. For a given element g_2 of G, the right-translate $R_{g_2} u : g_1 \mapsto u(g_1\, g_2)$ is in $C^\infty(G)$; it can therefore be coupled to T_1, giving rise to a smooth function $v : g_2 \mapsto \langle T_1, R_{g_2} u\rangle$. We can then couple T_2 to v and define the distribution $T_1 * T_2$ by

$$\langle T_1 * T_2, u\rangle = \langle T_2, v\rangle\,. \tag{66}$$

Using the notation of an integral, the right-hand side can be written as

$$\int_G T_2(g_2)\, dg_2 \int T_1(g_1)\, u(g_1\, g_2)\, dg_1\,. \tag{67}$$

[40] If T is a distribution on a manifold M, *its support* $\mathrm{Supp}(T)$ is the smallest closed subset F of M such that T vanishes identically on the open subset $U = M \backslash F$. This last condition means $\langle T, f\rangle = 0$ if f is a smooth function vanishing off a compact subset F_1 of M contained in U.

With this definition of the convolution product, one gets an algebra $C_c^{-\infty}(G)$.

Theorem 3.7.1. (L. Schwartz) *Let G be a Lie group. The distributions supported by the unit 1 of G form a subalgebra $C_{\{1\}}^{-\infty}(G)$ of $C_c^{-\infty}(G)$ which is isomorphic to the enveloping algebra $U(\mathfrak{g})$ of the Lie algebra $\mathfrak{g}$ of the Lie group G.*

Proof. It is a folklore theorem in mathematical physics that any generalized function (distribution) which vanishes outside a point is a sum of higher-order derivatives of a Dirac δ-function.

More precisely, choose a coordinate system $(u^1, \ldots, u^N)$ on G centered at the unit 1 of G. Use the standard notations (where $\alpha = (\alpha_1, \ldots, \alpha_N)$ belongs to $\mathbb{Z}_+^N$ as in the Theorem 3.6.1):

$$\partial_j = \partial / \partial\, u^j \,, \quad u^\alpha = \prod_{j=1}^N u_j^{\alpha_j} \,, \quad \partial^\alpha = \prod_{j=1}^N (\partial_j)^{\alpha_j}$$

and $\alpha! = \prod_{j=1}^N \alpha_j!$. If we set

$$\langle Z_\alpha, f \rangle = (\partial^\alpha f)(1)/\alpha! \,, \tag{68}$$

the distributions Z_α form an algebraic basis of the vector space $C := C_{\{1\}}^{-\infty} G$ of distributions supported by 1.

We proceed to compute the convolution $Z_\alpha * Z_\beta$. For this purpose, express analytically the multiplication in the group G by power series $\varphi^j(\boldsymbol{x}, \boldsymbol{y}) = \varphi^j(x^1, \ldots, x^N; y_1, \ldots, y^N)$ (for $1 \le j \le N$) giving the coordinates of the product $z = x \cdot y$ of a point x with coordinates $x^1, \ldots, x^N$ and a point y with coordinates $y^1, \ldots, y^N$. Since $\langle Z_\alpha, f \rangle$ is by definition the coefficient of the monomial u^α in the Taylor expansion of f around 1, to calculate $\langle Z_\alpha * Z_\beta, f \rangle$ we have to take the coefficient of $x^\alpha y^\beta$ in the Taylor expansion of

$$f(x \cdot y) = f(\varphi^1(\boldsymbol{x}, \boldsymbol{y}), \ldots, \varphi^N(\boldsymbol{x}, \boldsymbol{y}))\,.$$

If we develop $\varphi^\gamma(\boldsymbol{x}, \boldsymbol{y}) = \prod_{j=1}^N \varphi^j(\boldsymbol{x}, \boldsymbol{y})^{\gamma_j}$ in a Taylor series

$$\varphi^\gamma(\boldsymbol{x}, \boldsymbol{y}) \cong \sum_{\alpha,\beta} c_{\alpha\beta}^\gamma \, x^\alpha \, y^\beta \,, \tag{69}$$

an easy duality argument gives the answer

$$Z_\alpha * Z_\beta = \sum_\gamma c_{\alpha\beta}^\gamma \, Z_\gamma \,. \tag{70}$$

In the vector space $C = C^{-\infty}_{\{1\}}(G)$ we introduce a filtration $C_0 \subset C_1 \subset C_2 \subset \ldots \subset C_p \subset \ldots$, where C_p consists of the distributions T such that $\langle T, f \rangle = 0$ when f vanishes at 1 of order $\geq p+1$. Defining the order

$$|\alpha| = \alpha_1 + \cdots + \alpha_N \tag{71}$$

of an index vector $\alpha = (\alpha_1, \ldots, \alpha_N)$, the Z_α's with $|\alpha| \leq p$ form a basis of C_p. Moreover, since each series $\varphi^j(\boldsymbol{x}, \boldsymbol{y})$ is without constant term, the series $\varphi^\gamma(\boldsymbol{x}, \boldsymbol{y})$ begins with terms of order $|\gamma|$, hence by (69) we get

$$c^\gamma_{\alpha\beta} = 0 \qquad \text{for } |\alpha| + |\beta| < |\gamma|\,, \tag{72}$$

hence $Z_\alpha * Z_\beta$ belongs to $C_{|\alpha|+|\beta|}$ and we conclude

$$C_p * C_q \subset C_{p+q}\,. \tag{73}$$

Since 1 is a unit of the group G, that is $1 \cdot g = g \cdot 1 = g$ for any g in G, we get $\varphi^j(\boldsymbol{x}, \boldsymbol{0}) = \varphi^j(\boldsymbol{0}, \boldsymbol{x}) = x^j$, hence $\varphi^j(\boldsymbol{x}, \boldsymbol{y}) - x^j - y^j$ is a sum of terms of order ≥ 2. It follows that $\varphi^\gamma(\boldsymbol{x}, \boldsymbol{y}) - (\boldsymbol{x} + \boldsymbol{y})^\gamma$ is of order $> |\gamma|$ and by a reasoning similar to the one above, we derive the congruence

$$\alpha!\, Z_\alpha * \beta!\, Z_\beta \equiv (\alpha+\beta)!\, Z_{\alpha+\beta} \mod C_{|\alpha|+|\beta|-1}\,. \tag{74}$$

The distributions D_j defined by $\langle D_j, f \rangle = (\partial_j f)(1)$ (for $1 \leq j \leq N$) form a basis of the Lie algebra $\mathfrak{g}$ of G. If we denote by D^α the convolution $\underbrace{D_1 * \ldots * D_1}_{\alpha_1} * \ldots * \underbrace{D_N * \ldots * D_N}_{\alpha_N}$, an inductive argument based on (74) gives the congruence

$$\alpha!\, Z_\alpha \equiv D^\alpha \mod C_{|\alpha|-1} \tag{75}$$

and since the elements Z_α form a basis of C, so do the elements D^α.

Let now $U(\mathfrak{g})$ be the enveloping algebra of $\mathfrak{g}$. By its universal property[41] there exists an algebra homomorphism $\Phi : U(\mathfrak{g}) \to C$ inducing the identity on $\mathfrak{g}$. Hence Φ maps the product $\bar{D}^\alpha = \prod_{j=1}^{N} (D_j)^{\alpha_j}$ calculated in $U(\mathfrak{g})$ to the product D^α calculated in C. Since $[D_j, D_k] = D_j D_k - D_k D_j$ is a sum of terms of degree 1, a standard argument shows that the elements $\bar{D}^\alpha$ generate the vector space $U(\mathfrak{g})$, while the elements D^α form a basis of C. Since Φ maps $\bar{D}^\alpha$ to D^α, we conclude:

- Φ is an isomorphism of $U(\mathfrak{g})$ onto $C = C^{-\infty}_{\{1\}}(G)$;
- the elements $\bar{D}^\alpha$ form a basis of $U(\mathfrak{g})$ (theorem of Poincaré-Birkhoff-Witt).

[41] Here we use the possibility of defining the Lie bracket in $\mathfrak{g}$ by $[X, Y] = X * Y - Y * X$, after identifying $\mathfrak{g}$ with the set of distributions X of the form $\sum_{j=1}^{N} c_j\, D_j$, that is $X \in C_1$ and $\langle X, 1 \rangle = 0$.

Q.E.D.

Remark 3.7.1. The previous proof rests on the examination of the power series $\varphi^j(\boldsymbol{x},\boldsymbol{y})$ representing the product in the group. These power series satisfy the identities

$$\begin{array}{ll}\boldsymbol{\varphi}(\boldsymbol{\varphi}(\boldsymbol{x},\boldsymbol{y}),\boldsymbol{z}) = \boldsymbol{\varphi}(\boldsymbol{x},\boldsymbol{\varphi}(\boldsymbol{y},\boldsymbol{z}))\,, & \text{(associativity)} \\ \boldsymbol{\varphi}(\boldsymbol{x},\boldsymbol{0}) = \boldsymbol{\varphi}(\boldsymbol{0},\boldsymbol{x}) = \boldsymbol{x}\,. & \text{(unit)}\end{array}$$

A *formal group* over a field k is a collection of formal power series satisfying these identities. Let $\mathcal{O}$ be the ring of formal power series $k[[x^1,\ldots,x^N]]$, and let Z_α be the linear form on $\mathcal{O}$ associating to a series f the coefficient of the monomial x^α in f. The Z_α's form a basis for an algebra C, where the multiplication is defined by (69) and (70). We can introduce the filtration $C_0 \subset C_1 \subset C_2 \subset \ldots \subset C_p \subset \ldots$ as above and prove the formulas (72) to (75). *If the field k is of characteristic* 0, we can repeat the previous argument and construct an isomorphism $\varPhi : U(\mathfrak{g}) \to C$. If the field k is of characteristic $p \neq 0$, the situation is more involved. Nevertheless, the multiplication in $\mathcal{O} = k[[\boldsymbol{x}]]$ dualizes to a coproduct $\varDelta : C \to C \otimes C$ such that

$$\varDelta(Z_\alpha) = \sum_{\beta+\gamma=\alpha} Z_\beta \otimes Z_\gamma\,. \tag{76}$$

Then C is a Hopf algebra which encodes the formal group in an invariant way [34].

Remark 3.7.2. The restricted dual of the algebra $C^\infty(G)$ is the space $H(G) = C^{-\infty}_{\text{finite}}(G)$ of distributions with a finite support in G. Hence $H(G)$ is a coalgebra. It is immediate that $H(G)$ is stable under the convolution product of distributions, hence is a Hopf algebra. According to the previous theorem, $U(\mathfrak{g})$ is a sub-Hopf-algebra of $H(G)$. Furthermore, for every element g of G, the distribution δ_g is defined by $\langle \delta_g, f\rangle = f(g)$ for any function f in $C^\infty(G)$. It satisfies the convolution equation $\delta_g * \delta_{g'} = \delta_{gg'}$ and the coproduct rule $\varDelta(\delta_g) = \delta_g \otimes \delta_g$. Hence the group algebra $\mathbb{R}G$ associated to G considered as a discrete group is a sub-Hopf-algebra of $H(G)$. As an algebra, $H(G)$ is the twisted tensor product $G \ltimes U(\mathfrak{g})$ where G acts on $\mathfrak{g}$ by the adjoint representation (see subsection 3.8(B)).

Remark 3.7.3. Let k be an algebraically closed field of arbitrary characteristic. As in subsection 3.2, we can define an algebraic group over k as a pair $(G, \mathcal{O}(G))$ where $\mathcal{O}(G)$ is an algebra of representative functions on G with values in k satisfying the conditions stated in Lemma 3.2.1. Let $H(G)$ be the reduced dual Hopf algebra of $\mathcal{O}(G)$. It can be shown that $H(G)$ is a twisted tensor product $G \ltimes U(G)$ where $U(G)$ consists of the linear forms on $\mathcal{O}(G)$ vanishing on some power $\mathfrak{m}^N$ of the maximal ideal $\mathfrak{m}$ corresponding to the unit element of G ($\mathfrak{m}$ is the kernel of the counit $\varepsilon : \mathcal{O}(G) \to k$). If k is of characteristic 0, $U(G)$ is again the enveloping algebra of the Lie algebra $\mathfrak{g}$ of G. For the case of characteristic $p \neq 0$, we refer the reader to Cartier [18] or Demazure-Gabriel [32].

3.8 General structure theorems for Hopf algebras

(A) *The theorem of Cartier* [16].

Let $(A, m, \Delta, S, \varepsilon, \eta)$ be a Hopf algebra over a field k of characteristic 0. We define $\bar{A}$ as the kernel of the counit ε, and the *reduced coproduct* as the mapping $\bar{\Delta} : \bar{A} \to \bar{A} \otimes \bar{A}$ defined by

$$\bar{\Delta}(x) = \Delta(x) - x \otimes 1 - 1 \otimes x \qquad (x \text{ in } \bar{A})\,. \tag{77}$$

We iterate $\bar{\Delta}$ as follows (in general $\bar{\Delta}_n$ maps $\bar{A}$ into $\bar{A}^{\otimes n}$):

$$\begin{aligned} &\bar{\Delta}_0 = 0 \\ &\bar{\Delta}_1 = 1_{\bar{A}} \\ &\bar{\Delta}_2 = \bar{\Delta} \\ &\ldots\ldots \\ &\bar{\Delta}_{n+1} = (\bar{\Delta} \otimes \overbrace{1_{\bar{A}} \otimes \ldots \otimes 1_{\bar{A}}}^{n-1}) \circ \bar{\Delta}_n \text{ for } n \geq 2. \end{aligned} \tag{78}$$

Let $\bar{C}_n \subset \bar{A}$ be the kernel of $\bar{\Delta}_{n+1}$ (in particular $\bar{C}_0 = \{0\}$). Then the filtration

$$\bar{C}_0 \subset \bar{C}_1 \subset \bar{C}_2 \subset \ldots \subset \bar{C}_n \subset \bar{C}_{n+1} \subset \ldots$$

satisfies the rules

$$\bar{C}_p \cdot \bar{C}_q \subset \bar{C}_{p+q}\,,\ \Delta(\bar{C}_n) \subset \sum_{p+q=n} \bar{C}_p \otimes \bar{C}_q\,. \tag{79}$$

We say that the coproduct Δ is *conilpotent* if $\bar{A}$ is the union of the $\bar{C}_n$, that is for every x in $\bar{A}$, there exists an integer $n \geq 0$ with $\bar{\Delta}^n(x) = 0$.

Theorem 3.8.1. *Let A be a Hopf algebra over a field k of characteristic 0. Assume that the coproduct Δ is cocommutative*[42] *and conilpotent. Then $\mathfrak{g} = \bar{C}_1$ is a Lie algebra and the inclusion of $\mathfrak{g}$ into A extends to an isomorphism of Hopf algebras $\Phi : U(\mathfrak{g}) \to A$.*

Proof.[43] a) By definition, $\mathfrak{g} = \bar{C}_1$ consists of the elements x in A such that $\varepsilon(x) = 0$, $\Delta(x) = x \otimes 1 + 1 \otimes x$, the so-called *primitive* elements in A. For x, y in $\mathfrak{g}$, it is obvious that $[x, y] = xy - yx$ is in $\mathfrak{g}$, hence $\mathfrak{g}$ is a Lie algebra.

[42] This means $\sigma \circ \Delta = \Delta$ where σ is the automorphism of $A \otimes A$ defined by $\sigma(a \otimes b) = b \otimes a$.

[43] Our method of proof follows closely Patras [60].

By the universal property of the enveloping algebra $U(\mathfrak{g})$, there is an algebra homomorphism $\Phi : U(\mathfrak{g}) \to A$ extending the identity on $\mathfrak{g}$. In subsection 3.6 we defined a coproduct $\Delta_{\mathfrak{g}}$ on $U(\mathfrak{g})$ characterized by the fact that $\mathfrak{g}$ embedded in $U(\mathfrak{g})$ consists of the primitive elements. It is then easily checked that Φ is a homomorphism of Hopf algebras, that is the following identities hold

$$(\Phi \otimes \Phi) \circ \Delta_{\mathfrak{g}} = \Delta \circ \Phi\,,\ \varepsilon \circ \Phi = \varepsilon_{\mathfrak{g}}\,, \tag{80}$$

where $\varepsilon_{\mathfrak{g}}$ is the counit of $U(\mathfrak{g})$.

We shall associate to $\mathfrak{g}$ a certain coalgebra $\Gamma(\mathfrak{g})$ and construct a commutative diagram of coalgebras, namely

(D)

$$\begin{tikzcd} & U(\mathfrak{g}) \arrow[dd, "\Phi"] \\ \Gamma(\mathfrak{g}) \arrow[ur, "e_{\mathfrak{g}}"] \arrow[dr, "e_A"'] & \\ & A. \end{tikzcd}$$

Then we shall prove that e_A is an isomorphism of coalgebras. The Hopf algebra $U(\mathfrak{g})$ shares with A the properties that the coproduct is cocommutative and conilpotent. Hence $e_{\mathfrak{g}}$ is also an isomorphism[44]. The previous diagram then shows that Φ is an isomorphism of coalgebras, and since it was defined as a homomorphism of algebras, it is an isomorphism of Hopf algebras.

b) In general let V be a vector space (not necessarily finite-dimensional). We denote by $T^n(V)$ (or $V^{\otimes n}$) the tensor product of n copies of V (for $n \geq 0$), and by $T(V)$ the direct sum $\bigoplus\limits_{n\geq 0} T^n(V)$. We denote by $[v_1|\dots|v_n]$ the tensor product of a set of vectors $v_1, \dots, v_n$ in V. We define a coproduct Δ_T in $T(V)$ by

$$\begin{aligned} \Delta_T[v_1|\dots|v_n] = 1 \otimes [v_1|\dots|v_n] + [v_1|\dots|v_n] \otimes 1 \\ + \sum_{p=1}^{n-1} [v_1|\dots|v_p] \otimes [v_{p+1}|\dots|v_n]\,. \end{aligned} \tag{81}$$

Let $\Gamma^n(V) \subset T^n(V)$ be the set of tensors invariant under the natural action of the symmetric group S_n. For any v in V, put

$$\gamma_n(v) = \underbrace{[v|\dots|v]}_{n\,\text{factors}}\,. \tag{82}$$

[44] This follows also from the Poincaré-Birkhoff-Witt theorem. Our method of proof gives a proof for this theorem provided we know that any Lie algebra embeds into its enveloping algebra.

The standard polarization process shows that $\Gamma^n(V)$ is generated by the tensors $\gamma_n(v)$. For example, when $n = 2$, using a basis (e_α) of V, we see that the elements

$$[e_\alpha|e_\alpha] = \gamma_2(e_\alpha)\,,\ [e_\alpha|e_\beta] + [e_\beta|e_\alpha] = \gamma_2(e_\alpha + e_\beta) - \gamma_2(e_\alpha) - \gamma_2(e_\beta)$$

(for $\alpha < \beta$) form a basis of $\Gamma^2(V)$. I claim that the direct sum $\Gamma(V) := \bigoplus\limits_{n\geq 0} \Gamma^n(V)$ *is a subcoalgebra of* $T(V)$. Indeed, with the convention $\gamma_0(v) = 1$, formula (81) implies

$$\Delta_T(\gamma_n(v)) = \sum_{p=0}^{n} \gamma_p(v) \otimes \gamma_{n-p}(v)\,. \tag{83}$$

c) I claim that there exists[45] a linear map $e_A : \Gamma(\mathfrak{g}) \to A$ such that

$$e_A(\gamma_n(x)) = x^n/n! \tag{84}$$

for x in $\mathfrak{g}$, $n \geq 0$. Indeed since $\mathfrak{g}$ is a vector subspace of the algebra A, there exists, by the universal property of tensor algebras, a unique linear map E_A from $T(\mathfrak{g})$ to A mapping $[x_1|\ldots|x_n]$ to $\frac{1}{n!}\,x_1\ldots x_n$. Then we define e_A as the restriction of E_A to $\Gamma(\mathfrak{g}) \subset T(\mathfrak{g})$. By a similar construction, we define a map

$$e_{\mathfrak{g}} : \Gamma(\mathfrak{g}) \to U(\mathfrak{g})$$

such that $e_{\mathfrak{g}}(\gamma_n(x)) = x^n/n!$ for x in $\mathfrak{g}$, $n \geq 0$. Since Φ is a homomorphism of algebras it maps $x^n/n!$ calculated in $U(\mathfrak{g})$ to $x^n/n!$ calculated in A. The commutativity of the diagram (D), namely $e_A = \Phi \circ e_{\mathfrak{g}}$, follows immediately. Moreover, for x in $\mathfrak{g}$, we have $\Delta(x) = x \otimes 1 + 1 \otimes x$, hence

$$\Delta(x^n/n!) = (x \otimes 1 + 1 \otimes x)^n/n! = \sum_{p=0}^{n} \frac{x^p}{p!} \otimes \frac{x^{n-p}}{(n-p)!} \tag{85}$$

by the binomial theorem. Comparing with (83), we conclude that e_A (and similarly $e_{\mathfrak{g}}$) respects the coproducts $\Delta_\Gamma = \Delta_T\,|_{\Gamma(\mathfrak{g})}$ in $\Gamma(\mathfrak{g})$ and $\Delta_A = \Delta$ in A.

d) We introduce now a collection of operators Ψ_n (for $n \geq 1$) in A, reminiscent of the Adams operators in topology[46]. Consider the set E of linear

---

[45] This map is unique since the elements $\gamma_n(x)$ generate the vector space $\Gamma(\mathfrak{g})$.

[46] To explain the meaning of Ψ_n, consider the example of the Hopf algebra kG associated to a finite group (subsection 3.5). Then

$$\Psi_n\left(\sum_{g\in G} a_g \cdot g\right) = \sum_{g\in G} a_g \cdot g^n\,.$$

maps in A. We denote by $u \circ v$ (or simply uv) the composition of operators, and introduce another product $u * v$ by the formula

$$u * v = m_A \circ (u \otimes v) \circ \Delta_A \,, \tag{86}$$

where m_A is the product and Δ_A the coproduct in A. This product is associative, and the map $\iota = \eta \circ \varepsilon$ given by $\iota(x) = \varepsilon(x) \cdot 1$ is a unit

$$\iota * u = u * \iota = u \,. \tag{87}$$

Denoting by I the identity map in A, we define

$$\Psi_n = \underbrace{I * I * \ldots * I}_{n\,\text{factors}} \quad (\text{for } n \geq 1) \,. \tag{88}$$

We leave it as an exercise for the reader to check the formulas[47]

$$(\Psi_m \otimes \Psi_m) \circ \Delta_A = \Delta_A \circ \Psi_m \,, \tag{89}$$

$$\Psi_m \circ \Psi_n = \Psi_{mn} \,, \tag{90}$$

while the formula

$$\Psi_m * \Psi_n = \Psi_{m+n} \tag{91}$$

follows from the definition (88).

So far we didn't use the fact that Δ_A is conilpotent. Write $I = \iota + J$, that is J is the projection on $\bar{A}$ in the decomposition $A = k \cdot 1 \oplus \bar{A}$. From the binomial formula one derives

$$\Psi_n = I^{*n} = (\iota + J)^{*n} = \sum_{p=0}^{n} \binom{n}{p} J^{*p} \,. \tag{92}$$

But J^{*p} annihilates $k \cdot 1$ for $p > 0$ and coincides on $\bar{A}$ with $m_p \circ (\bar{\Delta}_A)_p$ where m_p maps $\bar{a}_1 \otimes \ldots \otimes \bar{a}_p$ in $\bar{A}^{\otimes p}$ to $\bar{a}_1 \ldots \bar{a}_p$ (product in A). Since Δ_A is conilpotent, for any given x in $\bar{A}$, there exists an integer $P \geq 0$ depending on x such that $J^{*p}(x) = 0$ for $p > P$. Hence $\Psi_n(x) = \sum\limits_{p=0}^{P} \binom{n}{p} J^{*p}(x)$ can be written as a polynomial in n (*at the cost of introducing denominators*), and there are operators π_p $(p \geq 0)$ in A such that

$$\Psi_n(x) = \sum_{p \geq 0} n^p \, \pi_p(x) \tag{93}$$

for x in A, $n \geq 1$, and $\pi_p(x) = 0$ for $p > P$.

[47] *Hint:* prove (89) by induction on m, using the cocommutativity of Δ_A and $\Psi_{m+1} = m_A \circ (I \otimes \Psi_m) \circ \Delta_A$. Then derive (90) by induction on m, using (89).

e) From the relations (90) and (93), it is easy to derive that the subspace $\pi_p(A)$ consists of the elements a in A such that $\Psi_n(a) = n^p a$ for all $n \geq 1$, and that A is the direct sum of the subspaces $\pi_p(A)$.

To conclude the proof of the theorem, it remains to establish that e_A induces an isomorphism of $\Gamma^p(\mathfrak{g})$ to $\pi_p(A)$ for any integer $p \geq 0$.

To prove that e_A maps $\Gamma^p(\mathfrak{g})$ into $\pi_p(A)$, it is enough to prove that x^p belongs to $\pi_p(A)$ for any primitive element x in $\mathfrak{g}$. Introduce the power series $e^{tx} = \sum\limits_{p \geq 0} t^p x^p / p!$ in the ring $A[[t]]$. Then e^{tx} is group-like, that is

$$\Delta_A(e^{tx}) = e^{tx} \otimes e^{tx} \,. \tag{94}$$

From the inductive definition

$$\Psi_{n+1} = m_A \circ (I \otimes \Psi_n) \circ \Delta_A \,, \tag{95}$$

one derives $\Psi_n(e^{tx}) = (e^{tx})^n = e^{tnx}$, that is

$$\Psi_n \left(\sum_{p \geq 0} \frac{t^p}{p!} \, x^p \right) = \sum_{p \geq 0} \frac{t^p}{p!} \, (nx)^p \tag{96}$$

and finally $\Psi_n(x^p) = n^p x^p$, that is $x^p \in \pi_p(A)$.

From the relations (93) and (91), one derives

$$\pi_p * \pi_q = \frac{(p+q)!}{p! \, q!} \, \pi_{p+q} \tag{97}$$

by the binomial formula, hence $\pi_p = \frac{1}{p!} \, \pi_1^{*p}$ for any $p \geq 0$. Moreover, from (93) and (89), one concludes

$$\Delta_A(\pi_m(A)) \subset \bigoplus_{i=0}^{m} \pi_i(A) \otimes \pi_{m-i}(A) \tag{98}$$

for $m \geq 0$. Hence $\pi_1(A) = \mathfrak{g}$ and $(\bar{\Delta}_A)_p$ maps $\pi_p(A)$ into $\pi_1(A)^{\otimes p} = \mathfrak{g}^{\otimes p}$. Since Δ_A is cocommutative, the image of $\pi_p(A)$ by $(\bar{\Delta}_A)_p$ consists of symmetric tensors, that is

$$(\bar{\Delta}_A)_p \, (\pi_p(A)) \subset \Gamma^p(\mathfrak{g}) \,.$$

Since e_A maps $\gamma_p(x)$ into $x^p/p!$, the relation $\pi_p = \frac{1}{p!} \, \pi_1^{*p}$ together with the definition of the $*$-product by (86) shows that e_A and $(\bar{\Delta}_A)_p$ induce inverse maps

$$\Gamma^p(\mathfrak{g}) \; \underset{(\bar{\Delta}_A)_p}{\overset{e_A}{\rightleftarrows}} \; \pi_p(A) \,.$$

Q.E.D.

As a corollary, let us describe the structure of the dual algebra of a Hopf algebra A, with a cocommutative and conilpotent coproduct. For simplicity, assume that the Lie algebra $\mathfrak{g} = \bar{C}_1$ of primitive elements is finite-dimensional. Then each subcoalgebra $C_n = k \cdot 1 \oplus \bar{C}_n$ is finite-dimensional. In the dual algebra A^*, the set $\mathfrak{m}$ of linear forms f on A with $\langle f, 1 \rangle = 0$ is the unique maximal ideal, and the ideal $\mathfrak{m}^n$ is the orthogonal of C_{n-1}. Then A^* is a noetherian complete local ring, that is it is isomorphic to a quotient $k[[x_1, \ldots, x_n]]/J$ of a power series ring. When the field k is a characteristic 0, it follows from Theorem 3.8.1 that A^* is isomorphic to a power series ring: if $D_1, \ldots, D_n$ is a basis of $\mathfrak{g}$ the mapping associating to f in A^* the power series

$$F(x_1, \ldots, x_n) := \left\langle f, \prod_{i=1}^{n} \exp x_i \, D_i \right\rangle$$

is an isomorphism of A^* to $k[[x_1, \ldots, x_n]]$. When the field k is of characteristic $p \neq 0$ and perfect, it has been shown in [16] and [34], Chap. II, 2, that A^* is isomorphic to an algebra of the form

$$k[[x_1, \ldots, x_n]]/(x_1^{p^{m_1}}, \ldots, x_r^{p^{m_r}})$$

for $0 \leq r \leq n$ and $m_1 \geq 0, \ldots, m_r \geq 0$. This should be compared to theorems **A.**, **B.** and **C.** by Borel, described in subsection 2.5.

(B) *The decomposition theorem of Cartier-Gabriel* [34].

Let again A be a Hopf algebra. We assume that the ground field k is *algebraically closed of characteristic* 0 and that its coproduct $\varDelta = \varDelta_A$ is cocommutative. We shall give a complete structure theorem for A.

Let again $\mathfrak{g}$ be the set of primitive elements, that is the elements x in A such that

$$\varDelta(x) = x \otimes 1 + 1 \otimes x \,, \qquad \varepsilon(x) = 0 \,. \tag{99}$$

Then $\mathfrak{g}$ is a Lie algebra for the bracket $[x, y] = xy - yx$, and we can introduce its enveloping algebra $U(\mathfrak{g})$ viewed as a Hopf algebra (see subsection 3.6).

Let $\varGamma$ be the set of group-like elements, that is the elements g in A such that

$$\varDelta(g) = g \otimes g \,, \qquad \varepsilon(g) = 1 \,. \tag{100}$$

For the multiplication in A, the elements of $\varGamma$ form a group, where the inverse of g is $S(g)$ (here S is the antipodism in A). We can introduce the group algebra $k\varGamma$ viewed as a Hopf algebra (see beginning of subsection 3.5).

Furthermore for x in $\mathfrak{g}$ and g in $\varGamma$, it is obvious that ${}^g x := g \, x \, g^{-1}$ belongs to $\mathfrak{g}$. Hence the group $\varGamma$ acts on the Lie algebra $\mathfrak{g}$ and therefore on its enveloping algebra $U(\mathfrak{g})$. We define the twisted tensor product $\varGamma \ltimes U(\mathfrak{g})$ as the tensor product $U(\mathfrak{g}) \otimes k\varGamma$ with the multiplication given by

$$(u \otimes g) \cdot (u' \otimes g') = u \cdot {}^g u' \otimes gg' \,. \tag{101}$$

There is a natural coproduct, which together with this product gives the definition of the Hopf algebra $\Gamma \ltimes U(\mathfrak{g})$.

Theorem 3.8.2. (Cartier-Gabriel) *Assume that the field k is algebraically closed of characteristic 0 and that A is a cocommutative Hopf algebra. Let $\mathfrak{g}$ be the space of primitive elements, and Γ the group of group-like elements in A. Then there is an isomorphism of $\Gamma \ltimes U(\mathfrak{g})$ onto A, as Hopf algebras, inducing the identity on Γ and on $\mathfrak{g}$.*

Proof. a) Define the reduced coproduct $\bar{\Delta}$, the iterates $\bar{\Delta}_p$ and the filtration (C_p) as in the beginning of subsection 3.8(A). Define $\bar{A}_1 = \bigcup_{p\geq 0} C_p$ and $A_1 = \bar{A}_1 + k \cdot 1$. Then A_1 is, according to the properties quoted there, a sub-Hopf-algebra. It is clear that the coproduct of A_1 is cocommutative and conilpotent. According to Theorem 3.8.1, we can identify A_1 with $U(\mathfrak{g})$. If we set $A_g := A_1 \cdot g$ for g in Γ, Theorem 8.3.2 amounts to assert that A is the direct sum of the subspaces A_g for g in Γ.

b) Let g in Γ. Since $\Delta(g) = g \otimes g$, and $\varepsilon(g) = 1$, then $A = \bar{A} \oplus k \cdot g$ where $\bar{A}$ is again the kernel of ε. Define a new reduced coproduct $\bar{\Delta}(g)$ in $\bar{A}$ by

$$\bar{\Delta}(g)(x) := \Delta(x) - x \otimes g - g \otimes x \qquad (x \text{ in } \bar{A}), \tag{102}$$

mapping $\bar{A}$ into $\bar{A}^{\otimes 2}$. Iterate $\bar{\Delta}(g)$ in a sequence of maps $\bar{\Delta}(g)_p : \bar{A} \to \bar{A}^{\otimes p}$. From the easy relation

$$\bar{\Delta}(g)_p\,(xg) = \bar{\Delta}_p(x) \cdot (\underbrace{g \otimes \ldots \otimes g}_{p}), \tag{103}$$

it follows that $\bar{A}_1 \cdot g$ is the union of the kernels of the maps $\bar{\Delta}(g)_p$.

c) **Lemma 3.8.1.** *The coalgebra A is the union of its finite-dimensional sub-coalgebras.*

Indeed, introduce a basis (e^α) of A, and define operators φ_α, ψ_α in A by

$$\Delta(x) = \sum_\alpha \varphi_\alpha(x) \otimes e^\alpha = \sum_\alpha e^\alpha \otimes \psi_\alpha(x) \tag{104}$$

for x in A.

From the coassociativity of Δ, one derives the relations

$$\varphi_\alpha\,\varphi_\beta = \sum_\gamma c^\gamma_{\alpha\beta}\,\varphi_\gamma \tag{105}$$

$$\psi_\alpha\,\psi_\beta = \sum_\gamma c^\gamma_{\beta\alpha}\,\psi_\gamma \tag{106}$$

$$\varphi_\alpha\,\psi_\beta = \psi_\beta\,\varphi_\alpha \tag{107}$$

with the constants $c_{\alpha\beta}^\gamma$ defined by

$$\Delta(e^\gamma) = \sum_{\alpha,\beta} c_{\alpha\beta}^\gamma\, e^\alpha \otimes e^\beta\,. \tag{108}$$

For any x in A, the family of indices α such that $\varphi_\alpha(x) \neq 0$ or $\psi_\alpha(x) \neq 0$ is finite, hence for any given x_0 in A, the *subspace C of A generated by the elements $\varphi_\alpha(\psi_\beta(x_0))$ is finite-dimensional.* By the property of the counit, we get

$$x_0 = \sum_{\alpha,\beta} \varphi_\alpha(\psi_\beta(x_0))\,\varepsilon(e^\alpha)\,\varepsilon(e^\beta) \tag{109}$$

hence x_0 belongs to C. Obviously, C is stable under the operators φ_α and ψ_α, hence by (104) one gets

$$\Delta(C) \subset (C \otimes A) \cap (A \otimes C) = C \otimes C$$

and *C is a sub-coalgebra of A.*

d) Choose C as above, and introduce the dual algebra C^*. It is a commutative finite-dimensional algebra over the algebraically closed field k. By a standard structure theorem, it is a direct product

$$C^* = E_1 \times \ldots \times E_r\,, \tag{110}$$

where E_i possesses a unique maximal ideal $\mathfrak{m}_i$, such that $E_i/\mathfrak{m}_i$ is isomorphic to k, and $\mathfrak{m}_i$ is nilpotent: $\mathfrak{m}_i^N = 0$ for some large N. The algebra homomorphisms from C^* to k correspond to the group-like elements in C.

By duality, the decomposition (110) corresponds to a direct sum decomposition $C = C_1 \oplus \ldots \oplus C_r$ where each C_i contains a unique element g_i in Γ. Furthermore, from the nilpotency of $\mathfrak{m}_i$, it follows that $C_i \cap \bar{A}$ is annihilated by $\bar{\Delta}(g_i)_N$ for large N, hence $C_i \subset A_{g_i}$ and

$$C = \bigoplus_{i=1}^r \,(C \cap A_{g_i})\,. \tag{111}$$

Since A is the union of such coalgebras C, the previous relation entails $A = \bigoplus_{g\in\Gamma} A_g$, hence the theorem of Cartier-Gabriel.

Q.E.D.

When the field k is algebraically closed of characteristic $p \neq 0$, the previous proof works almost unchanged, and the result is that the cocommutative Hopf algebra A is the semidirect product $\Gamma \ltimes A_1$ where Γ is a group acting on a Hopf algebra A_1 with conilpotent coproduct. The only difference lies in the structure of A_1. We refer the reader to Dieudonné [34], Chapter II: in section II,1 there is a proof of the decomposition theorem and in section II,2 the structure of a Hopf algebra with conilpotent coproduct is discussed. See also [18] and [32].

Another corollary of Theorem 3.8.2 is as follows:

Assume that k is algebraically closed of characteristic 0*. Then any finite-dimensional cocommutative Hopf algebra over k is a group algebra kG.*

(C) *The theorem of Milnor-Moore.*

The results of this subsection are dual of those of the previous one and concern Hopf algebras which are commutative as algebras.

Theorem 3.8.3. *Let $A = \bigoplus_{n\geq 0} A_n$ be a graded Hopf algebra*[48] *over a field k of characteristic* 0*. Assume:*

(M_1) *A is* connected, *that is $A_0 = k \cdot 1$.*

(M_2) *The product in A is commutative.*

Then A is a free commutative algebra (a polynomial algebra) *generated by homogeneous elements.*

A proof can be given which is a dual version of the proof of Theorem 3.8.1. Again, introduce operators Ψ_n in A by the recursion $\Psi_1 = 1_A$ and

$$\Psi_{n+1} = m_A \circ (1_A \otimes \Psi_n) \circ \Delta_A \,. \tag{112}$$

They are endomorphisms of the algebra A and there exists a direct sum decomposition $A = \bigoplus_{p\geq 0} \pi_p(A)$ such that $\Psi_n(a) = n^p\, a$ for a in $\pi_p(A)$ and any $n \geq 1$. The formula $\pi_p(A) \cdot \pi_q(A) \subset \pi_{p+q}(A)$ follows from $\Psi_n(ab) = \Psi_n(a)\,\Psi_n(b)$ and since A is a commutative algebra, there is a well-defined algebra homomorphism[49]

$$\Theta : \mathrm{Sym}\,(\pi_1(A)) \to A$$

mapping $\mathrm{Sym}^p(\pi_1(A))$ into $\pi_p(A)$. Denote by Θ_p the restriction of Θ to $\mathrm{Sym}^p(\pi_1(A))$. An inverse map Λ_p to Θ_p can be defined as the composition of the iterated coproduct $\bar{\Delta}_p$ which maps $\pi_p(A)$ to $\pi_1(A)^{\otimes p}$ with the natural projection of $\pi_1(A)^{\otimes p}$ to $\mathrm{Sym}^p(\pi_1(A))$. Hence Θ is an isomorphism of algebras.

48 That is, the product m_A maps $A_p \otimes A_q$ into A_{p+q}, and the coproduct Δ_A maps A_n into $\bigotimes_{p+q=n} A_p \otimes A_q$. It follows that ε annihilates A_n for $n \geq 1$, and that the antipodism S is homogeneous $S(A_n) = A_n$ for $n \geq 0$.

49 For any vector space V, we denote by $\mathrm{Sym}\,(V)$ the *symmetric algebra* built over V, that is the free commutative algebra generated by V. If (e^α) is a basis of V, then $\mathrm{Sym}\,(V)$ is the polynomial algebra in variables u^α corresponding to e^α.

We sketch another proof which makes Theorem 3.8.3 a corollary of Theorem 3.8.1, under the supplementary assumption (valid in most of the applications):

(M_3) *Each A_n is a finite-dimensional vector space.*

Let B_n be the dual of A_n and let $B = \bigoplus_{n\geq 0} B_n$. The product $m_A : A \otimes A \to A$ dualizes to a coproduct $\Delta_B : B \to B \otimes B$, and similarly the coproduct $\Delta_A : A \to A \otimes A$ dualizes to a product $m_B : B \otimes B \to B$. Since m_A is commutative, Δ_B is cocommutative. Moreover the reduced coproduct $\bar{\Delta}_B$ maps B_n (for $n \geq 1$) into $\sum_{i,j} B_i \otimes B_j$ where i, j runs over the decompositions[50]

$$i \geq 1\,, \quad j \geq 1\,, \quad i + j = n\,.$$

Hence $(\bar{\Delta}_B)_p$ maps B_n into the direct sum of the spaces $B_{n_1} \otimes \ldots \otimes B_{n_p}$ where

$$n_1 \geq 1, \ldots, n_p \geq 1\,, \quad n_1 + \ldots + n_p = n\,.$$

It follows $(\bar{\Delta}_B)_p(B_n) = \{0\}$ for $p > n$, hence *the coproduct Δ_B is conilpotent.*

Let $\mathfrak{g}$ be the Lie algebra of primitive elements in the Hopf algebra B. It is graded $\mathfrak{g} = \bigoplus_{p\geq 1} \mathfrak{g}_p$ and $[\mathfrak{g}_p, \mathfrak{g}_q] \subset \mathfrak{g}_{p+q}$. From (the proof of) Theorem 3.8.1, we deduce a natural isomorphism of coalgebras $e_B : \Gamma(\mathfrak{g}) \to B$. By the assumption ($M_3$), we can identify A_n to the dual of B_n, hence the algebra A to the graded dual[51] of the coalgebra B. We leave it to the reader to check that the graded dual of the coalgebra $\Gamma(\mathfrak{g})$ is the symmetric algebra $\mathrm{Sym}(\mathfrak{g}^\vee)$, where $\mathfrak{g}^\vee$ is the graded dual of $\mathfrak{g}$. The dual of $e_B : \Gamma(\mathfrak{g}) \to B$ is then an isomorphism of algebras

$$\Theta : \mathrm{Sym}(\mathfrak{g}^\vee) \to A\,.$$

Notice also the isomorphism of Hopf algebras

$$\Phi : U(\mathfrak{g}) \to B$$

where the Hopf algebra B is the graded dual of A. Q.E.D.

Remark 3.8.1. By the connectedness assumption (M_1), the kernel of the counit $\varepsilon : A \to k$ is $A^+ = \bigoplus_{n\geq 1} A_n$. From the existence of the isomorphism Θ, one derives that $\mathfrak{g}$ as a graded vector space is the graded dual of $A^+/A^+ \cdot A^+$.

Remark 3.8.2. The complete form of Milnor-Moore's Theorem 3.8.3 deals with a combination of symmetric and exterior algebras, and implies the theorems of Hopf and Samelson, described in subsections 2.4 and 2.5. Instead

[50] Use here the connectedness of A (cf. (M_1)).

[51] The graded dual of a graded vector space $V = \bigoplus_n V_n$ is $W = \bigoplus_n W_n$ where W_n is the dual of V_n.

of assuming that A is a commutative algebra, we have to assume that it is "graded-commutative", that is

$$a_q \cdot a_p = (-1)^{pq} \, a_p \cdot a_q \tag{113}$$

for a_p in A_p and a_q in A_q.

The graded dual $\mathfrak{g}$ of $A^+/A^+ \cdot A^+$ is then a super Lie algebra (or graded Lie algebra), and A as an algebra is the free graded-commutative algebra generated by $A^+/A^+ \cdot A^+$.

Remark 3.8.3. In Theorem 3.8.3, assume that the product m_A is commutative and the coproduct Δ_A is cocommutative. Then the corresponding Lie algebra $\mathfrak{g}$ is commutative $[x, y] = 0$, and $U(\mathfrak{g}) = \mathrm{Sym}(\mathfrak{g})$. It follows easily that A as an algebra is the free commutative algebra $\mathrm{Sym}(P)$ built over the space P of primitive elements in A. A similar result holds in the case where A is graded-commutative, and graded-cocommutative (see subsection 2.5).

3.9 Application to prounipotent groups

In this subsection, we assume that k *is a field of characteristic* 0.

(A) *Unipotent algebraic groups.*

An algebraic group G over k is called *unipotent* if it is *geometrically connected*[52] (as an algebraic variety) and its Lie algebra $\mathfrak{g}$ is nilpotent[53]. A typical example is the group $T_n(k)$ of strict triangular matrices $g = (g_{ij})$ with entries in k, where $g_{ii} = 1$ and $g_{ij} = 0$ for $i > j$. We depict these matrices for $n = 4$

$$g = \begin{pmatrix} 1 & g_{12} & g_{13} & g_{14} \\ 0 & 1 & g_{23} & g_{24} \\ 0 & 0 & 1 & g_{34} \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

The corresponding Lie algebra $\mathfrak{t}_n(k)$ consists of the matrices $x = (x_{ij})$ with $x_{ij} = 0$ for $i \geq j$, example

$$x = \begin{pmatrix} 0 & x_{12} & x_{13} & x_{14} \\ 0 & 0 & x_{23} & x_{24} \\ 0 & 0 & 0 & x_{34} \\ 0 & 0 & 0 & 0 \end{pmatrix} .$$

The product of n matrices in $\mathfrak{t}_n(k)$ is always 0, and $T_n(k)$ is the set of matrices $I_n + x$, with x in $\mathfrak{t}_n(k)$ (and I_n the unit matrix in $M_n(k)$). Hence we get inverse maps

[52] An algebraic variety X over a field k is called geometrically connected if it is connected and remains connected over any field extension of k.

[53] That is, the adjoint map $\mathrm{ad}\, x : y \mapsto [x, y]$ in $\mathfrak{g}$ is nilpotent for any x in $\mathfrak{g}$.

$$T_n(k) \underset{\exp}{\overset{\log}{\rightleftarrows}} \mathfrak{t}_n(k)\,,$$

where log, and exp, are truncated series

$$\log(I_n + x) = x - \frac{x^2}{2} + \cdots + (-1)^{n-1}\, x^{n-1}/(n-1)\,, \tag{114}$$

$$\exp\, x = I_n + x + \frac{x^2}{2!} + \cdots + \frac{x^{n-1}}{(n-1)!}\,. \tag{115}$$

Hence log and exp are inverse polynomial maps. Moreover, by the Baker-Campbell-Hausdorff formula, the product in $T_n(k)$ is given by

$$\exp\, x \cdot \exp\, y = \exp \sum_{i=1}^{n-1} H_i(x,y)\,, \tag{116}$$

where $H_i(x,y)$ is made of iterated Lie brackets of order $i-1$, for instance

$$\begin{aligned} H_1(x,y) &= x + y \\ H_2(x,y) &= \frac{1}{2}\,[x,y] \\ H_3(x,y) &= \frac{1}{12}\,[x,[x,y]] + \frac{1}{12}\,[y,[y,x]]\,. \end{aligned}$$

From these properties, it follows that the exponential map from $\mathfrak{t}_n(k)$ to $T_n(k)$ maps the Lie subalgebras $\mathfrak{g}$ of $\mathfrak{t}_n(k)$ to the algebraic subgroups G of $T_n(k)$. In this situation, the representative functions in $\mathcal{O}(G)$ correspond to the polynomial functions of $\mathfrak{g}$, hence $\mathcal{O}(G)$ is a polynomial algebra.

Let now G be any unipotent group, with the nilpotent Lie algebra $\mathfrak{g}$. According to the classical theorems of Ado and Engel, $\mathfrak{g}$ is isomorphic to a Lie subalgebra of $\mathfrak{t}_n(k)$ for some $n \geq 1$. It follows that *the exponential map is an isomorphism of $\mathfrak{g}$ with G as algebraic varieties, and as above, $\mathcal{O}(G)$ is a polynomial algebra.*

(B) *Infinite triangular matrices.*

We consider now the group $T_\infty(k)$ of infinite triangular matrices $g = (g_{ij})_{i\geq 1, j\geq 1}$ with $g_{ii} = 1$ and $g_{ij} = 0$ for $i > j$. Notice that the product of two such matrices g and h is defined by $(g \cdot h)_{im} = \sum_{j=i}^{m} g_{ij}\, h_{jm}$ for $i \leq m$, *a finite sum*!! For such a matrix g denote by $\tau_N(g)$ its truncation: the finite matrix $(g_{ij})_{\substack{1\leq i\leq N \\ 1\leq j\leq N}}$. An infinite matrix appears therefore as a tower of matrices

$$\tau_1(g)\,,\ \tau_2(g), \ldots, \tau_N(g)\,,\ \tau_{N+1}(g), \ldots$$

that is $T_\infty(k)$ is the inverse limit of the tower of groups

$$T_1(k) \longleftarrow T_2(k) \longleftarrow \cdots \longleftarrow T_N(k) \xleftarrow{\tau_N} T_{N+1}(k) \longleftarrow \ .$$

By duality, one gets a sequence of embeddings for the rings of representative functions

$$\mathcal{O}(T_1(k)) \hookrightarrow \mathcal{O}(T_2(k)) \hookrightarrow \dots$$

whose union we denote $\mathcal{O}(T_\infty(k))$. Hence *a representative function on $T_\infty(k)$ is a function which can be expressed as a polynomial in a finite number of entries.*

A subgroup G of $T_\infty(k)$ is called (pro)algebraic if there exists a collection of representative functions P_α in $\mathcal{O}(T_\infty(k))$ such that

$$g \in G \Leftrightarrow P_\alpha(g) = 0 \quad \text{for all } \alpha \,,$$

for any g in $T_\infty(k)$. We denote by $\mathcal{O}(G)$ the algebra of functions on G obtained by restricting functions in $\mathcal{O}(T_\infty(k))$ from $T_\infty(k)$ to G. It is tautological that $\mathcal{O}(G)$ is a Hopf algebra, and that G is its spectrum[54]. A vector subspace V of $\mathfrak{t}_\infty(k)$ will be called *linearly closed* if it is given by a family of linear equations of the form $\sum\limits_{\substack{1\le i\le N\\ 1\le j\le N}} \lambda_{ij}\, x_{ji} = 0$ (with a suitable finite $N \geq 1$ depending on the equation). Notice also, that for any matrix $x = (x_{ij})$ in $\mathfrak{t}_\infty(k)$, its powers satisfy $(x^N)_{ij} = 0$ for $N \geq \max(i,j)$, hence one can define the inverse maps

$$T_\infty(k) \underset{\exp}{\overset{\log}{\rightleftarrows}} \mathfrak{t}_\infty(k) \,.$$

The calculation of any entry of $\log(I + x)$ or $\exp x$ for a given x in $\mathfrak{t}_\infty(k)$ requires a finite amount of algebraic operations.

From the results of subsection 3.9(A), one derives a bijective correspondence between the proalgebraic subgroups G of $T_\infty(k)$ and the linearly closed Lie subalgebras $\mathfrak{g}$ of $\mathfrak{t}_\infty(k)$. Moreover, if $J \subset \mathcal{O}(G)$ is the kernel of the counit, then $\mathfrak{g}$ is naturally the dual of[55] $J/J \cdot J =: L$. Finally, the exponential map $\exp : \mathfrak{g} \to G$ transforms $\mathcal{O}(G)$ into the polynomial functions on $\mathfrak{g}$ coming from the duality between $\mathfrak{g}$ and L, hence an isomorphism of algebras

$$\Theta : \mathrm{Sym}(L) \to \mathcal{O}(G) \,.$$

If G is as before, let $G_N := \tau_N(G)$ be the truncation of G. Then G_N is an algebraic subgroup of $T_N(k)$, a unipotent algebraic group, and G can be recovered as the inverse limit (also called projective limit) $\varprojlim G_N$ of the tower

[54] Here the spectrum is relative to the field k, that is for any algebra homomorphism $\varphi : \mathcal{O}(G) \to k$, there exists a unique element g in G such that $\varphi(u) = u(g)$ for every u in $\mathcal{O}(G)$.

[55] Hence L is a Lie coalgebra, whose dual $\mathfrak{g}$ is a Lie algebra. The structure map of a Lie coalgebra L is a linear map $\delta : L \to \Lambda^2 L$ which dualizes to the bracket $\Lambda^2\mathfrak{g} \to \mathfrak{g}$.

$$G_1 \leftarrow G_2 \leftarrow \cdots \leftarrow G_N \leftarrow G_{N+1} \leftarrow \cdots$$

It is therefore called a *prounipotent group.*

(C) *Unipotent groups and Hopf algebras.*

Let G be a group. We say that a representation $\pi : G \to GL(V)$ (where V is a vector space of finite dimension n over the field k) is *unipotent* if, after the choice of a suitable basis of V, the image $\pi(G)$ is a subgroup of the triangular group $T_n(k)$. More intrinsically, there should exist a sequence $\{0\} = V_0 \subset V_1 \subset \cdots \subset V_{n-1} \subset V_n = V$ of subspaces of V, with $\dim V_i = i$ and $(\pi(g) - 1)\, V_i \subset V_{i-1}$ for g in G and $1 \leq i \leq n$. The class of unipotent representations of G is stable under direct sum, tensor products, contragredient, subrepresentations and quotient representations.

Assume now that G is an algebraic unipotent group. By the results of subsection 3.9(A), there exists an embedding of G into some triangular group $T_n(k)$, hence a faithful unipotent representation π. Since the determinant of any element in $T_n(k)$ is 1, the coordinate ring of G is generated by the coefficients of π, and according to the previous remarks, any algebraic linear representation of the group G is unipotent.

Let f be a function in the coordinate ring of G. Then f is a coefficient of some unipotent representation $\pi : G \to GL(V)$; if n is the dimension of V, the existence of the flag $(V_i)_{0 \leq i \leq n}$ as above shows that $\prod_{i=1}^{n} (\pi(g_i) - 1) = 0$ as an operator on V, hence[56], for any system $g_1, \ldots, g_n$ of elements of G,

$$\left\langle f, \prod_{i=1}^{n} (g_i - 1) \right\rangle = 0\,. \tag{117}$$

A quick calculation describes the iterated coproducts $\bar{\Delta}_p$ in $\mathcal{O}(G)$, namely

$$(\bar{\Delta}_p\, f)(g_1, \ldots, g_p) = \left\langle f, \prod_{i=1}^{p} (g_i - 1) \right\rangle \tag{118}$$

when $\varepsilon(f) = f(1)$ is 0. Hence the coproduct Δ in $\mathcal{O}(G)$ is conilpotent. Notice that $\mathcal{O}(G)$ is a Hopf algebra, and that as an algebra it is commutative and finitely generated.

The converse was essentially proved by Quillen [65], and generalizes Milnor-Moore theorem.

Theorem 3.9.1. *Let A be a Hopf algebra over a field k of characteristic* 0 *satisfying the following properties:*

[56] To calculate this, expand the product and use linearity, as for instance in

$$\langle f, (g_1 - 1)(g_2 - 1)\rangle = \langle f, g_1\, g_2 - g_1 - g_2 + 1\rangle = f(g_1\, g_2) - f(g_1) - f(g_2) + f(1)\,.$$

(Q1) *The multiplication* m_A *is commutative.*

(Q2) *The coproduct* Δ_A *is conilpotent.*

Then, as an algebra, A *is a free commutative algebra.*

The proof is more or less the first proof of Milnor-Moore theorem. One defines again the Adams operators Ψ_n by the induction

$$\Psi_{n+1} = m_A \circ (1_A \otimes \Psi_n) \circ \Delta_A \,. \tag{119}$$

The commutativity of m_A suffices to show that Ψ_n is an algebra homomorphism

$$\Psi_n \circ m_A = m_A \circ (\Psi_n \otimes \Psi_n) \tag{120}$$

satisfying $\Psi_m \circ \Psi_n = \Psi_{mn}$. The formula

$$\Psi_m * \Psi_n = \Psi_{m+n} \tag{121}$$

is tautological. Furthermore, since Δ_A is conilpotent one sees that for any given x in A, and p large enough, one gets $J^{*p}(x) = 0$ (where $J(x) = x - \varepsilon(x) \cdot 1$). This implies the "spectral theorem"

$$\Psi_n(x) = \sum_{p \geq 0} n^p \, \pi_p(x) \tag{122}$$

where $\pi_p(x) = 0$ for given x and $p \geq P(x)$. We leave the rest of the proof to the reader (see first proof of Milnor-Moore theorem). Q.E.D.

If A is graded and connected, with a coproduct $\Delta = \Delta_A$ satisfying $\Delta(A_n) \subset \bigoplus_{p+q=n} A_p \otimes A_q$, one gets

$$\bar{\Delta}_p(A_n) \subset \oplus A_{n_1} \otimes \ldots \otimes A_{n_p} \tag{123}$$

with $n_1 \geq 1, \ldots, n_p \geq 1$, $n_1 + \cdots + n_p = n$, hence $\bar{\Delta}_p(A_n) = 0$ for $p > n$. Hence Δ_A is conilpotent and Milnor-Moore theorem is a corollary of Theorem 3.9.1.

As a consequence of Theorem 3.9.1, *the unipotent groups correspond to the Hopf algebras satisfying* (Q1) *and* (Q2) *and finitely generated as algebras.* For the prounipotent groups, replace the last condition by the assumption that the linear dimension of A is countable[57].

Remark 3.9.1. Let A be a Hopf algebra satisfying (Q1) and (Q2). Let A^* be the full dual of the vector space A. It is an algebra with multiplication dual to the coproduct Δ_A. The spectrum G of A is a subset of A^*, and a group under the multiplication of A^*. Similarly, the set $\mathfrak{g}$ of linear forms f on A satisfying

[57] *Hint*: By Lemma 3.8.1, A is the union of an increasing sequence $C_1 \subset C_2 \subset \ldots$ of finite-dimensional coalgebras. The algebra H_r generated by C_r is a Hopf algebra corresponding to a unipotent group G_r, and $A = \mathcal{O}(G)$ where $G = \varprojlim G_r$.

$$f(1) = 0 \,, \quad f(xy) = \varepsilon(x)\, f(y) + f(x)\, \varepsilon(y) \tag{124}$$

for x, y in A is a Lie algebra for the bracket $[f,g] = fg - gf$ induced by the multiplication in A^*. From the conilpotency of Δ_A follows that any series $\sum_{n \geq 0} c_n \langle f^n, x \rangle$ (with c_n in k, x in A, f in A^* with $f(1) = 0$) has only finitely many nonzero terms. Hence for any f in $\mathfrak{g}$, the exponential $\exp f = \sum_{n \geq 0} f^n/n!$ is defined. Furthermore, the map $f \mapsto \exp f$ is a bijection from $\mathfrak{g}$ to G. This remark gives a concrete description of the exponential map for unipotent (or prounipotent) groups.

4 Applications of Hopf algebras to combinatorics

In this section, we give a sample of the applications of Hopf algebras to various problems in combinatorics, having in mind mainly the relations with the polylogarithms.

4.1 Symmetric functions and invariant theory

(A) *The Hopf algebra of the symmetric groups.*

We denote by S_n the group consisting of the $n!$ permutations of the set $\{1, 2, \ldots, n\}$. By convention $S_0 = S_1 = \{1\}$. For σ in S_n and τ in S_m, denote by $\sigma \times \tau$ the permutation ρ in S_{n+m} such that

$$\begin{cases} \rho(i) = \sigma(i) & \text{for } 1 \leq i \leq n \\ \rho(n+j) = n + \tau(j) & \text{for } 1 \leq j \leq m \,. \end{cases}$$

The mapping $(\sigma, \tau) \mapsto \sigma \times \tau$ gives an identification of $S_n \times S_m$ with a subgroup of S_{n+m}.

Let k be a field of characteristic 0. We denote by Ch_n the vector space consisting of the functions $f : S_n \to k$ such that $f(\sigma\tau) = f(\tau\sigma)$ for σ, τ in S_n (central functions). On Ch_n, we define a scalar product by

$$\langle f \mid g \rangle = \frac{1}{n!} \sum_{\sigma \in S_n} f(\sigma)\, g(\sigma^{-1}) \,. \tag{125}$$

It is known that the irreducible characters[58] of the finite group S_n form an orthonormal basis of Ch_n. We identify Ch_0 to k, but not Ch_1.

If $n = p + q$, with $p \geq 0$, $q \geq 0$, the vector space $\mathrm{Ch}_p \otimes \mathrm{Ch}_q$ can be identified with the space of functions f on the subgroup $S_p \times S_q$ of S_n satisfying $f(\alpha\beta) = f(\beta\alpha)$ for α, β in $S_p \times S_q$. We have therefore a restriction map

[58] We remind the reader that these characters take their values in the field $\mathbb{Q}$ of rational numbers, and $\mathbb{Q}$ is a subfield of k.

$$\Delta_{p,q} : \mathrm{Ch}_n \to \mathrm{Ch}_p \otimes \mathrm{Ch}_q$$

and taking direct sums a map Δ_n from Ch_n to $\bigoplus\limits_{p+q=n} \mathrm{Ch}_p \otimes \mathrm{Ch}_q$. Defining $\mathrm{Ch}_\bullet = \bigoplus\limits_{n\geq 0} \mathrm{Ch}_n$, the collection of maps Δ_n defines a map

$$\Delta : \mathrm{Ch}_\bullet \to \mathrm{Ch}_\bullet \otimes \mathrm{Ch}_\bullet\,.$$

Define also $\varepsilon : \mathrm{Ch}_\bullet \to k$ by $\varepsilon(1) = 1$, and $\varepsilon|_{\mathrm{Ch}_n} = 0$ for $n > 0$. Then $\mathrm{Ch}_\bullet$ is a coalgebra, with coproduct Δ and counit ε.

Using the scalar products, $\Delta_{p,q}$ has an adjoint

$$m_{p,q} : \mathrm{Ch}_p \otimes \mathrm{Ch}_q \to \mathrm{Ch}_{p+q}\,.$$

Explicitly, if u is in $\mathrm{Ch}_p \otimes \mathrm{Ch}_q$, it is a function on $S_p \times S_q$ that we extend to S_{p+q} as a function $u^0 : S_{p+q} \to k$ which vanishes outside $S_p \times S_q$. Then

$$m_{p,q}\, u(\sigma) = \frac{1}{n!} \sum_{\tau\in S_n} u^0(\tau\sigma\tau^{-1})\,. \tag{126}$$

Collecting the maps $m_{p,q}$ we define a multiplication

$$m : \mathrm{Ch}_\bullet \otimes \mathrm{Ch}_\bullet \to \mathrm{Ch}_\bullet$$

with the element 1 of Ch_0 as a unit.

With these definitions, $\mathrm{Ch}_\bullet$ is a graded Hopf algebra which is both commutative and cocommutative. According to Milnor-Moore's theorem, $\mathrm{Ch}_\bullet$ is therefore a polynomial algebra in a family of primitive generators. We proceed to an explicit description.

(B) *Three families of generators.*

For each $n \geq 0$, denote by σ_n the function on S_n which is identically 1. In particular $\sigma_0 = 1$, and $\mathrm{Ch}_1 = k \cdot \sigma_1$. It can be shown that $\mathrm{Ch}_\bullet$ *is a polynomial algebra in the generators* $\sigma_1, \sigma_2, \ldots$ and a trivial calculation gives the coproduct

$$\Delta(\sigma_n) = \sum_{p=0}^{n} \sigma_p \otimes \sigma_{n-p}\,. \tag{127}$$

Similarly, let $\lambda_n : S_n \to k$ be the signature map. In particular $\lambda_0 = 1$ and $\lambda_1 = \sigma_1$. Again, $\mathrm{Ch}_\bullet$ *is a polynomial algebra in the generators* $\lambda_1, \lambda_2, \ldots$ and

$$\Delta(\lambda_n) = \sum_{p=0}^{n} \lambda_p \otimes \lambda_{n-p}\,. \tag{128}$$

The two families are connected by the relations

$$\sum_{p=0}^{n}(-1)^p \, \lambda_p \, \sigma_{n-p} = 0 \qquad \text{for } n \geq 1 \, . \tag{129}$$

A few consequences:

$$\begin{array}{ll} \sigma_1 = \lambda_1 & \lambda_1 = \sigma_1 \\ \sigma_2 = \lambda_1^2 - \lambda_2 & \lambda_2 = \sigma_1^2 - \sigma_2 \\ \sigma_3 = \lambda_3 - 2\,\lambda_1\,\lambda_2 + \lambda_1^3 & \lambda_3 = \sigma_3 - 2\,\sigma_1\,\sigma_2 + \sigma_1^3 \, . \end{array}$$

A third family $(\psi_n)_{n\geq 1}$ is defined by the recursion relations (Newton's relations) for $n \geq 2$

$$\psi_n = \lambda_1\,\psi_{n-1} - \lambda_2\,\psi_{n-2} + \lambda_3\,\psi_{n-3} - \ldots + (-1)^n\,\lambda_{n-1}\,\psi_1 + n(-1)^{n-1}\,\lambda_n \tag{130}$$

with the initial condition $\psi_1 = \lambda_1$. They can be solved by

$$\begin{aligned} \psi_1 &= \lambda_1 \\ \psi_2 &= \lambda_1^2 - 2\,\lambda_2 \\ \psi_3 &= \lambda_1^3 - 3\,\lambda_1\,\lambda_2 + 3\,\lambda_3 \, . \end{aligned}$$

Hence $\mathrm{Ch}_\bullet$ *is a polynomial algebra in the generators* $\psi_1, \psi_2, \ldots$

To compute the coproduct, it is convenient to introduce generating series

$$\lambda(t) = \sum_{n\geq 0} \lambda_n\,t^n \, , \quad \sigma(t) = \sum_{n\geq 0} \sigma_n\,t^n \, , \quad \psi(t) = \sum_{n\geq 1} \psi_n\,t^n \, .$$

Then formula (129) is equivalent to

$$\sigma(t)\,\lambda(-t) = 1 \tag{131}$$

and Newton's relations (130) are equivalent to

$$\lambda(t)\,\psi(-t) + t\,\lambda'(t) = 0 \, , \tag{132}$$

where $\lambda'(t)$ is the derivative of $\lambda(t)$ with respect to t. Differentiating (131), we transform (132) into

$$\sigma(t)\,\psi(t) - t\,\sigma'(t) = 0 \, , \tag{133}$$

or taking the coefficients of t^n,

$$\psi_n = -(\sigma_1\,\psi_{n-1} + \sigma_2\,\psi_{n-2} + \cdots + \sigma_{n-1}\,\psi_1) + n\,\sigma_n \, . \tag{134}$$

This can be solved

$$\begin{aligned} \psi_1 &= \sigma_1 \\ \psi_2 &= -\sigma_1^2 + 2\,\sigma_2 \\ \psi_3 &= \sigma_1^3 - 3\,\sigma_1\,\sigma_2 + 3\,\sigma_3 \, . \end{aligned}$$

We translate the relations (127) and (128) as

$$\Delta(\sigma(t)) = \sigma(t) \otimes \sigma(t) \tag{135}$$

$$\Delta(\lambda(t)) = \lambda(t) \otimes \lambda(t)\,. \tag{136}$$

Taking logarithmic derivatives and using (133) into the form[59] $\psi(t) = t\frac{d}{dt}\log\sigma(t)$, we derive

$$\Delta(\psi(t)) = \psi(t) \otimes 1 + 1 \otimes \psi(t)\,. \tag{137}$$

Otherwise stated, *the* ψ_n*'s are primitive generators of the Hopf algebra* $\mathrm{Ch}_\bullet$.

(C) *Invariants.*

Let V be a vector space of finite dimension n over the field k of characteristic 0. The group $GL(V)$ of automorphisms of V is the complement in the algebra $\mathrm{End}\,(V)$ (viewed as a vector space of dimension n^2 over k) of the algebraic subvariety defined by $\det u = 0$. The regular functions on the algebraic group $GL(V)$ are then of the form $F(g) = P(g)/(\det g)^N$ where P is a polynomial function[60] on $\mathrm{End}(V)$ and N a nonnegative integer. We are interested in the *central functions* F, that is the functions F on $GL(V)$ satisfying $F(g_1\,g_2) = F(g_2\,g_1)$. Since

$$\det(g_1\,g_2) = (\det g_1) \cdot (\det g_2) = \det(g_2\,g_1)\,,$$

we consider only the case where F is a polynomial.

If F is a polynomial on $\mathrm{End}(V)$, homogeneous of degree d, there exists by polarization a unique symmetric multilinear form $\Phi(u_1, \ldots, u_d)$ on $\mathrm{End}(V)$ such that $F(u) = \Phi(u, \ldots, u)$. Furthermore, Φ is of the form

$$\Phi(u_1, \ldots, u_d) = \mathrm{Tr}\,(A \cdot (u_1 \otimes \cdots \otimes u_d))\,, \tag{138}$$

where A is an operator acting on $V^{\otimes d}$. On the tensor space $V^{\otimes d}$, there are two actions of groups:

- the group $GL(V)$ acts by $g \mapsto g \otimes \cdots \otimes g$ (d factors);
- the symmetric group S_d acts by $\sigma \mapsto T_\sigma$ where

$$T_\sigma(v_1 \otimes \cdots \otimes v_d) = v_{\sigma^{-1}(1)} \otimes \ldots \otimes v_{\sigma^{-1}(d)}\,. \tag{139}$$

Hence the function F on $GL(V)$ defined by

$$F(g) = \mathrm{Tr}(A \cdot (\underbrace{g \otimes \cdots \otimes g}_{d})) \tag{140}$$

[59] Equivalent to

$$1 + \sum_{n \geq 1} \sigma_n\, t^n = \exp \sum_{n \geq 1} \psi_n\, t^n / n\,.$$

It is then easy to give an explicit formula for the σ_n's in terms of the ψ_n's.

[60] That is a polynomial in the entries g_{ij} of the matrix representing g in any given basis of V.

is central iff A commutes to the action of the group $GL(V)$, and by *Schur-Weyl duality*, A is a linear combination of operators T_σ. Moreover the multilinear form Φ being symmetric one has $A\,T_\sigma = T_\sigma\,A$ for all σ in S_d. Conclusion:

The central function F on $GL(V)$ is given by

$$F(g) = \frac{1}{d!}\sum_{\sigma\in S_d} \mathrm{Tr}(T_\sigma\cdot(g\otimes\cdots\otimes g))\cdot f(\sigma) \tag{141}$$

for a suitable function f in Ch_d.

We have defined an algebra homomorphism

$$T_V : \mathrm{Ch}_\bullet \to \mathcal{O}_Z(GL(V))\,,$$

where $\mathcal{O}_Z(GL(V))$ denotes the ring of regular central functions on $GL(V)$. We have the formulas

$$T_V(\lambda_d)(g) = \mathrm{Tr}(\Lambda^d\,g)\,, \tag{142}$$

$$T_V(\sigma_d)(g) = \mathrm{Tr}(S^d\,g)\,, \tag{143}$$

$$T_V(\psi_d)(g) = \mathrm{Tr}(g^d)\,. \tag{144}$$

Here $\Lambda^d\,g$ (resp. $S^d\,g$) means the natural action of $g\in GL(V)$ on the exterior power $\Lambda^d(V)$ (resp. the symmetric power $\mathrm{Sym}^d(V)$). Furthermore, g^d is the power of g in $GL(V)$.

Remark 4.1.1. From (144), one derives an explicit formula for ψ_d in Ch_d, namely

$$\psi_d/d = \sum_{\gamma\,\text{cycle}} \gamma\,, \tag{145}$$

where the sum runs over the one-cycle permutations γ.

Remark 4.1.2. Since $\Lambda^d(V) = \{0\}$ for $d > n$, we have $T_V(\lambda_d) = 0$ for $d > n$. Recall that $\mathrm{Ch}_\bullet$ is a polynomial algebra in $\lambda_1, \lambda_2, \ldots$; the kernel of T_V is then the ideal generated by $\lambda_{n+1}, \lambda_{n+2}, \ldots$ Moreover $\mathcal{O}_Z(GL(V))$ is the polynomial ring

$$k\,[T_V(\lambda_1), \ldots, T_V(\lambda_{n-1}), T_V(\lambda_n), T_V(\lambda_n)^{-1}]\,.$$

(D) *Relation with symmetric functions* [20].

Choose a basis $(e_1, \ldots, e_n)$ in V to represent operators in V by matrices, and consider the "generic" diagonal matrix $D_n = \mathrm{diag}(x_1, \ldots, x_n)$ in $\mathrm{End}(V)$, where $x_1, \ldots, x_n$ are indeterminates. Since the eigenvalues of a matrix are defined up to a permutation, and u and gug^{-1} have the same eigenvalues for g in $GL(V)$, the map $F \mapsto F(D_n)$ is an *isomorphism of the ring of central polynomial functions on* $\mathrm{End}(V)$ *to the ring of symmetric polynomials in* $x_1, \ldots, x_n$. In this isomorphism $T_V(\lambda_d)$ goes into the *elementary symmetric function*

$$e_d(x_1,\dots,x_n) = \sum_{1\le i_1<\dots<i_d\le n} x_{i_1}\dots x_{i_d}\,, \tag{146}$$

$T_V(\sigma_d)$ goes into the *complete monomial function*

$$h_d(x_1,\dots,x_n) = \sum_{\alpha_1+\dots+\alpha_n=d} x_1^{\alpha_1}\dots x_n^{\alpha_n}\,, \tag{147}$$

and $T_V(\psi_d)$ into the *power sum*

$$\psi_d(x_1,\dots,x_n) = x_1^d+\dots+x_n^d\,. \tag{148}$$

All relations derived in subsection 4.1(A) remain valid, but working in a space of finite dimension n, or with a fixed number of variables, imposes $e_{n+1} = e_{n+2} = \dots = 0$. At the level of the algebra $\mathrm{Ch}_\bullet$, no such restriction occurs.

(E) *Interpretation of the coproduct.*

Denote by X an alphabet $x_1,\dots,x_n$, similarly by Y the alphabet $y_1,\dots,y_m$ and by $X+Y$ the combined alphabet $x_1,\dots,x_n,y_1,\dots,y_m$. Then

$$e_r(X+Y) = \sum_{p+q=r} e_p(X)\,e_q(Y)\,, \tag{149}$$

$$h_r(X+Y) = \sum_{p+q=r} h_p(X)\,h_q(Y)\,, \tag{150}$$

$$\psi_r(X+Y) = \psi_r(X)+\psi_r(Y)\,. \tag{151}$$

Alternatively, by omitting T_V in notations like $T_V(\lambda_d)(g)$, one gets

$$\lambda_r(g\oplus g') = \sum_{p+q=r} \lambda_p(g)\,\lambda_q(g')\,, \tag{152}$$

$$\sigma_r(g\oplus g') = \sum_{p+q=r} \sigma_p(g)\,\sigma_q(g')\,, \tag{153}$$

$$\psi_r(g\oplus g') = \psi_r(g)+\psi_r(g')\,. \tag{154}$$

Here g acts on V, g' on V' and $g\oplus g'$ is the direct sum acting on $V\oplus V'$. For tensor products, one has

$$\psi_r(g\otimes g') = \psi_r(g)\,\psi_r(g')\,,$$

or in terms of alphabets

$$\psi_r(X\cdot Y) = \psi_r(X)\cdot\psi_r(Y)$$

where $X\cdot Y$ consists of the products $x_i\cdot y_j$. It is a notoriously difficult problem to calculate $\lambda_d(g\otimes g')$ and $\sigma_d(g\otimes g')$. The usual procedure is to go back to the ring $\mathrm{Ch}_\bullet$ and to use the transformation formulas $\lambda \leftrightarrow \psi$ or $\sigma \leftrightarrow \psi$ (see subsection 4.1(B)).

(F) *Noncommutative symmetric functions.*

In subsection 4.1(A) we described the structure of the Hopf algebra $\mathrm{Ch}_\bullet$. This can be reformulated as follows: let C be the coalgebra with a basis $(\lambda_n)_{n\geq 0}$, counit ε given by $\varepsilon(\lambda_0) = 1$, $\varepsilon(\lambda_n) = 0$ for $n > 0$, coproduct given by (128). Let $\bar{C}$ be the kernel of $\varepsilon : C \to k$, and $A = \mathrm{Sym}(\bar{C})$ the free commutative algebra over $\bar{C}$. We embed $C = \bar{C} \oplus k \cdot \lambda_0$ into A by identifying λ_0 with $1 \in A$. The universal property of the algebra A enables us to extend the map $\Delta : C \to C \otimes C$ to an algebra homomorphism $\Delta_A : A \to A \otimes A$. The coassociativity is proved by noticing that $(\Delta_A \otimes 1_A) \circ \Delta_A$ and $(1_A \otimes \Delta_A) \circ \Delta_A$ are algebra homomorphisms from A to $A^{\otimes 3}$ which coincide on the set C of generators of A, hence are equal. Similarly, the cocommutativity of C implies that of A.

We can repeat this construction by replacing the symmetric algebra $\mathrm{Sym}(\bar{C})$ by the tensor algebra $T(\bar{C})$. We obtain a graded Hopf algebra $\mathrm{NC}_\bullet$ which is *cocommutative*. It is described as the algebra of noncommutative polynomials in the generators $\Lambda_1, \Lambda_2, \Lambda_3, \dots$ satisfying the coproduct relation

$$\Delta(\Lambda_n) = \sum_{p=0}^{n} \Lambda_p \otimes \Lambda_{n-p}\,, \tag{155}$$

with the convention $\Lambda_0 = 1$. We introduce the generating series $\Lambda(t) = \sum\limits_{n\geq 0} \Lambda_n\, t^n$ and reformulate the previous relation as

$$\Delta(\Lambda(t)) = \Lambda(t) \otimes \Lambda(t)\,. \tag{156}$$

By inversion, we define the generating series $\Sigma(t) = \sum\limits_{n\geq 0} \Sigma_n\, t^n$ such that $\Sigma(t)\, \Lambda(-t) = 1$. It is group-like as $\Lambda(t)$ hence the coproduct

$$\Delta(\Sigma_n) = \sum_{p=0}^{n} \Sigma_p \otimes \Sigma_{n-p}\,. \tag{157}$$

We can also define primitive elements $\Psi_1, \Psi_2, \dots$ in $\mathrm{NC}_\bullet$ by their generating series

$$\Psi(t) = t\, \Sigma'(t)\, \Sigma(t)^{-1}\,. \tag{158}$$

The algebra $\mathrm{NC}_\bullet$ *is the algebra of noncommutative polynomials in each of the families* $(\Lambda_n)_{n\geq 1}$, $(\Sigma_n)_{n\geq 1}$ *and* $(\Psi_n)_{n\geq 1}$. *The Lie algebra of primitive elements in the Hopf algebra* $\mathrm{NC}_\bullet$ *is generated by the elements* Ψ_n, *and coincides with the free Lie algebra generated by these elements (see subsection* 4.2*).*

We can call $\mathrm{Ch}_\bullet$ the algebra of symmetric functions (in an indeterminate number of variables, see subsection 4.1(D)). It is customary to call $\mathrm{NC}_\bullet$ the

Hopf algebra of noncommutative symmetric functions. There is a unique homomorphism π of Hopf algebras from $\mathrm{NC}_\bullet$ to $\mathrm{Ch}_\bullet$ mapping Λ_n to λ_n, Σ_n to σ_n, Ψ_n to ψ_n. Since each of these elements is of degree n, the map π from $\mathrm{NC}_\bullet$ to $\mathrm{Ch}_\bullet$ respects the grading.

(G) *Quasi-symmetric functions.*

The algebra (graded) dual to the coalgebra C is the polynomial algebra $\Gamma = k[z]$ in one variable, the basis $(\lambda_n)_{n\geq 0}$ of C being dual to the basis $(z^n)_{n\geq 0}$ in $k[z]$. This remark gives us a more natural description of C as the (graded) dual of Γ. Define $\bar{\Gamma} \subset \Gamma$ as the set of polynomials without constant term, and consider the tensor module $T(\bar{\Gamma}) = \bigoplus\limits_{m\geq 0} \bar{\Gamma}^{\otimes m}$. We use the notation $[\gamma_1|\ldots|\gamma_m]$ to denote the tensor product $\gamma_1\otimes\cdots\otimes\gamma_m$ in $T(\bar{\Gamma})$, for the elements γ_i of $\bar{\Gamma}$. We view $T(\bar{\Gamma})$ as a coalgebra, where the coproduct is obtained by *deconcatenation*

$$\begin{aligned}\Delta\,[\gamma_1|\ldots|\gamma_m] &= 1\otimes[\gamma_1|\ldots|\gamma_m] \\ &\quad + \sum_{i=1}^{m-1}[\gamma_1|\ldots|\gamma_i]\otimes[\gamma_{i+1}|\ldots|\gamma_m] + [\gamma_1|\ldots|\gamma_m]\otimes 1\,.\end{aligned} \tag{159}$$

We embed $\Gamma = \bar{\Gamma}\oplus k\cdot 1$ into $T(\bar{\Gamma})$ by identifying 1 in Γ with the unit $[\,]\in\bar{\Gamma}^{\otimes 0}$. By dualizing the methods of the previous subsection, one shows that there is a unique multiplication[61] in $T(\bar{\Gamma})$ inducing the given multiplication in Γ, and such that Δ be an algebra homomorphism from $T(\bar{\Gamma})$ to $T(\bar{\Gamma})\otimes T(\bar{\Gamma})$. Hence we have constructed a commutative graded Hopf algebra.

It is customary to denote this Hopf algebra by $\mathrm{QSym}_\bullet$, and to call it *the algebra of quasi-shuffles*, or *quasi-symmetric functions*. We explain this terminology. By construction, the symbols

$$Z(n_1,\ldots,n_r) = [z^{n_1}|\ldots|z^{n^r}] \tag{160}$$

for $r\geq 0$, $n_1\geq 1,\ldots,n_r\geq 1$ form a basis of $\mathrm{QSym}_\bullet$. Explicitly, the product of such symbols is given by the *rule of quasi-shuffles*:

- consider two sequences $n_1,\ldots,n_r$ and $m_1,\ldots,m_s$;
- in all possible ways insert zeroes in these sequences to get two sequences

$$\nu = (\nu_1,\ldots,\nu_p) \qquad \text{and} \qquad \mu = (\mu_1,\ldots,\mu_p)$$

  of the same length, by excluding the cases where $\mu_i = \nu_i = 0$ for some i between 1 and p;
- for such a combination, introduce the element $Z(\nu_1+\mu_1,\ldots,\nu_p+\mu_p)$ and take the sum of all these elements as the product of $Z(n_1,\ldots,n_r)$ and $Z(m_1,\ldots,m_s)$.

[61] For details about this construction, see Loday [53].

We describe the algorithm in an example: to multiply $Z(3)$ with $Z(1,2)$

$$\frac{\begin{cases}\nu = 30\\ \mu = 12\end{cases}}{Z(3+1,0+2)} \qquad \frac{\begin{cases}\nu = 03\\ \mu = 12\end{cases}}{Z(0+1,3+2)} \qquad \frac{\begin{cases}\nu = 300\\ \mu = 012\end{cases}}{Z(3+0,0+1,0+2)}$$

$$\frac{\begin{cases}\nu = 030\\ \mu = 102\end{cases}}{Z(0+1,3+0,0+2)} \qquad \frac{\begin{cases}\nu = 003\\ \mu = 120\end{cases}}{Z(0+1,0+2,3+0)}$$

hence the result

$$Z(3)\cdot Z(1,2) = Z(4,2) + Z(1,5) + Z(3,1,2) + Z(1,3,2) + Z(1,2,3)\,.$$

The sequences $(3,1,2), (1,3,2)$ and $(1,2,3)$ are obtained by shuffling the sequences $(1,2)$ and (3) (see subsection 4.2). The other terms are obtained by partial addition, so the terminology[62] "quasi-shuffles".

The interpretation as *quasi-symmetric functions* requires an infinite sequence of commutative variables $x_1, x_2, \ldots$. The symbol $Z(n_1,\ldots,n_r)$ is then interpreted as the formal power series

$$\sum_{1\le k_1<\ldots<k_r} x_{k_1}^{n_1}\ldots x_{k_r}^{n_r} = z(n_1,\ldots,n_r)\,. \tag{161}$$

It is easily checked that the series $z(n_1,\ldots,n_r)$ multiply according to the rule of quasi-shuffles, and are linearly independent.

Recall that $\mathrm{Ch}_\bullet$ is self-dual. Furthermore, there is a duality between $\mathrm{NC}_\bullet$ and $\mathrm{QSym}_\bullet$ such that the monomial basis $(\Lambda_{n_1}\ldots\Lambda_{n_r})$ of $\mathrm{NC}_\bullet$ is dual to the basis $(Z(n_1,\ldots,n_r))$ of $\mathrm{QSym}_\bullet$. The transpose of the projection $\pi : \mathrm{NC}_\bullet \to \mathrm{Ch}_\bullet$ is an embedding into $\mathrm{QSym}_\bullet$ of $\mathrm{Ch}_\bullet$ viewed as the algebra of symmetric functions in $x_1, x_2, \ldots$, generated by the elements $z(\underbrace{1,\ldots,1}_{r}) = e_r$.

4.2 Free Lie algebras and shuffle products

Let X be a finite alphabet $\{x_i | i \in I\}$. A *word* is an ordered sequence $w = x_{i_1}\ldots x_{i_\ell}$ of elements taken from X, with repetition allowed. We include the empty word $\emptyset$ (or 1). We use the *concatenation* product $w\cdot w'$ and denote by X^* the set of all words. We take X^* as a basis of the vector space $k\langle X\rangle$ of noncommutative polynomials. The *concatenation of words* defines by linearity a multiplication on $k\langle X\rangle$.

[62] Other denomination: "stuffles". See also [19] for another interpretation of quasi-shuffles.

It is an exercise in universal algebra that the free associative algebra $k\langle X\rangle$ is the enveloping algebra $U(\mathrm{Lie}(X))$ of the free Lie algebra $\mathrm{Lie}(X)$ on X. By Theorem 3.6.1, we can therefore identify $\mathrm{Lie}(X)$ to the Lie algebra of primitive elements in $k\langle X\rangle$, where the coproduct Δ is the unique homomorphism of algebras from $k\langle X\rangle$ to $k\langle X\rangle \otimes k\langle X\rangle$ mapping x_i to $x_i \otimes 1 + 1 \otimes x_i$ for any i ("*Friedrichs criterion*"). This result provides us with a workable construction of $\mathrm{Lie}(X)$.

To dualize, introduce another alphabet $\Xi = \{\xi_i | i \in I\}$ in a bijective correspondence with X. The basis X^* of $k\langle X\rangle$ and the basis Ξ^* of $k\langle\Xi\rangle$ are both indexed by the same set I^* of finite sequences in I, and we define a duality between $k\langle X\rangle$ and $k\langle\Xi\rangle$ by putting these two basis in duality. More precisely, we define a grading in $k\langle X\rangle$ and in $k\langle\Xi\rangle$ by giving degree ℓ to both $x_{i_1}\dots x_{i_\ell}$ and $\xi_{i_1}\dots\xi_{i_\ell}$. Then $k\langle\Xi\rangle$ is the graded dual of $k\langle X\rangle$, and conversely.

The product in $k\langle X\rangle$ dualizes to a coproduct in $k\langle\Xi\rangle$ which uses *deconcatenation*, namely[63]

$$\begin{aligned}\Delta(\xi_{i_1}\dots\xi_{i_\ell}\rangle &= \xi_{i_1}\dots\xi_{i_\ell}\otimes 1 + 1\otimes\xi_{i_1}\dots\xi_{i_\ell} \\ &\quad + \sum_{j=1}^{\ell-1}\xi_{i_1}\dots\xi_{i_j}\otimes\xi_{i_{j+1}}\dots\xi_{i_\ell}\,. \end{aligned} \tag{162}$$

To compute the product in $k\langle\Xi\rangle$ we need the coproduct in $k\langle X\rangle$. For any $i \in I$, put

$$x_i^{(1)} = x_i \otimes 1\,, \qquad x_i^{(2)} = 1 \otimes x_i\,. \tag{163}$$

Then $\Delta(x_i) = x_i^{(1)} + x_i^{(2)}$, hence for any word $w = x_{i_1}\dots x_{i_\ell}$ we get

$$\begin{aligned}\Delta(w) &= \Delta(x_{i_1})\dots\Delta(x_{i_\ell}) = (x_{i_1}^{(1)} + x_{i_1}^{(2)})\dots(x_{i_\ell}^{(1)} + x_{i_\ell}^{(2)}) \\ &= \sum_{\alpha_1\dots\alpha_\ell} x_{i_1}^{(\alpha_1)}\dots x_{i_\ell}^{(\alpha_\ell)}\,.\end{aligned} \tag{164}$$

The sum is extended over the 2^ℓ sequences $(\alpha_1,\dots,\alpha_\ell)$ made of 1's and 2's. Otherwise stated

$$\Delta(w) = \sum w^{(1)} \otimes w^{(2)}\,, \tag{165}$$

where $w^{(1)}$ runs over the 2^ℓ subwords of w (obtained by erasing some letters) and $w^{(2)}$ the complement of $w^{(1)}$ in w. For instance

$$\Delta(x_1\,x_2) = x_1\,x_2 \otimes 1 + x_1 \otimes x_2 + x_2 \otimes x_1 + 1 \otimes x_1\,x_2\,. \tag{166}$$

By duality, the product of $u = \xi_{i_1}\dots\xi_{i_\ell}$ and $v = \xi_{j_1}\dots\xi_{j_m}$ is the sum $u \sqcup\!\sqcup\, v$ of all words of length $\ell + m$ in Ξ^* containing u as a subword, with v as the complementary subword. This product is called "shuffle product" because of

[63] Compare with formulas (81) and (159).

the analogy with the shuffling of card decks. It was introduced by Eilenberg and MacLane in the 1940's in their work on homotopy. We give two examples:

$$\xi_1 \sqcup\!\sqcup\, \xi_2 = \xi_1\,\xi_2 + \xi_2\,\xi_1\,, \tag{167}$$

$$\xi_1 \sqcup\!\sqcup\, \xi_2\,\xi_3 = \xi_1\,\xi_2\,\xi_3 + \xi_2\,\xi_1\,\xi_3 + \xi_2\,\xi_3\,\xi_1\,. \tag{168}$$

Notice that $k\langle \Xi \rangle$ with the shuffle product and the deconcatenation coproduct is a commutative graded Hopf algebra. Hence, by Milnor-Moore theorem, as an algebra, it is a polynomial algebra. A classical theorem by Radford gives an explicit construction[64] of a set of generators. Take any linear ordering on I, and order the words in Ξ according to the lexicographic ordering $u \prec u$. By cyclic permutations, a word w of length ℓ generates ℓ words $w(1), \ldots, w(\ell)$, with $w(1) = w$. A *Lyndon word* is a word w such that $w(1), \ldots, w(\ell)$ are all distinct and $w \prec w(j)$ for $j = 2, \ldots, \ell$. For instance $\xi_1\,\xi_2$ is a Lyndon word, but not $\xi_2\,\xi_1$, similarly $\xi_1\,\xi_2\,\xi_3$ and $\xi_1\,\xi_3\,\xi_2$ are Lyndon words, but the 4 others permutations of ξ_1, ξ_2, ξ_3 are not.

Radford's theorem. *The shuffle algebra $k\langle \Xi \rangle$ is a polynomial algebra in the Lyndon words as generators.*

4.3 Application I: free groups

We consider a free group F_n on a set of n generators $g_1, \ldots, g_n$. We want to *describe the envelope of F_n corresponding to the class of its unipotent representations* (see subsection 3.4).

Let $\pi : F_n \to GL(V)$ be a unipotent representation. It is completely characterized by the operators $\gamma_i = \pi(g_i)$ in V (for $i = 1, \ldots, n$). Hence γ_i is unipotent (that is, $\gamma_i - 1$ is nilpotent) and there exists a unique nilpotent operator u_i in V such that $\gamma_i = \exp u_i$. By choosing a suitable basis $(e_1, \ldots, e_d)$ of V, we can assume that the u_i are matrices in $\mathfrak{t}_d(k)$, hence $u_{i_1} \ldots u_{i_d} = 0$ for any sequence $(i_1, \ldots, i_d)$ of indices.

Conversely, consider a vector space V of dimension d and operators $u_1, \ldots, u_n$ such that $u_{i_1} \ldots u_{i_p} = 0$ for some p. In particular $u_i^p = 0$ for all i, and we can define the exponential $\gamma_i = \exp u_i$. Define subspaces $V_0, V_1, V_2 \ldots$ of V by $V_0 = V$ and the inductive rule

$$V_{r+1} = \sum_{i=1}^{n} u_i(V_r)\,. \tag{169}$$

By our assumption on $u_1, \ldots, u_n$, we obtain $V_p = \{0\}$. It is easy to check that the spaces V_r decrease

$$V = V_0 \supset V_1 \supset V_2 \supset \ldots \supset V_{p-1} \supset V_p = \{0\}\,,$$

[64] See the book of Reutenauer [66] for details.

and since each u_i maps V_r into V_{r+1}, so does $\gamma_i - 1 = \exp u_i - 1$. Hence we get a unipotent representation π of F_n, mapping g_i to γ_i.

Putting $X = \{x_1, \ldots, x_n\}$ and $\Xi = \{\xi_1, \ldots, \xi_n\}$, we conclude that the unipotent representations of F_n correspond to the representations of the algebra $k\langle X\rangle$ which annihilate one of the two-sided ideals

$$J_r = \bigoplus_{s \geq r} k\langle X\rangle_s$$

($k\langle X\rangle_s$ is the component of degree s in $k\langle X\rangle$). Using the duality between $k\langle X\rangle$ and $k\langle \Xi\rangle$, the algebra of representative functions on F_n corresponding to the unipotent representations can be identified to $k\langle \Xi\rangle$. We leave it to the reader to check that both the product and the coproduct are the correct ones.

To the graded commutative Hopf algebra $k\langle \Xi\rangle$ corresponds a prounipotent group Φ_n, the sought-for prounipotent envelope of F_n. Explicitly, the points of Φ_n with coefficients in k correspond to the algebra homomorphisms $k\langle \Xi\rangle \to k$; they can be interpreted as noncommutative formal power series $g = \sum_{m \geq 0} g_m$ in $k\langle\!\langle X\rangle\!\rangle$, with g_m in $k\langle X\rangle_m$, satisfying the coproduct rule

$$\Delta(g_m) = \sum_{r+s=m} g_r \otimes g_s \,, \tag{170}$$

or in a shorthand notation $\Delta(g) = g \otimes g$. The multiplication is inherited from the one in $k\langle\!\langle X\rangle\!\rangle$, that is the product of $g = \sum_{r \geq 0} g_r$ by $h = \sum_{s \geq 0} h_s$ is given by the Cauchy rule

$$(gh)_m = \sum_{r+s=m} g_r \, h_s \,. \tag{171}$$

The group Φ_n consists also of the exponentials

$$g = \exp(p_1 + p_2 + \cdots) \,, \tag{172}$$

where p_r is primitive of degree r, that is an element of degree r in the free Lie algebra $\mathrm{Lie}(X)$. Otherwise stated, *the Lie algebra of Φ_n is the completion of* $\mathrm{Lie}(X)$ *with respect to its grading.*

Finally, the map $\delta : F_n \to \Phi_n$ defined in subsection 3.4 maps g_i to $\exp x_i$.

4.4 Application II: multiple zeta values

We recall the definition of Riemann's zeta function

$$\zeta(s) = \sum_{k \geq 1} k^{-s} \,, \tag{173}$$

where the series converges absolutely for complex values of s such that $\mathrm{Re}\, s > 1$. It is well-known that $(s-1)\,\zeta(s)$ extends to an entire function, giving a meaning to $\zeta(0), \zeta(-1), \zeta(-2), \ldots$ It is known that these numbers are rational, and that the function $\zeta(s)$ satisfies the symmetry rule $\xi(s) = \xi(1-s)$ with $\xi(s) = \pi^{-s/2}\,\Gamma\left(\frac{s}{2}\right)\zeta(s)$. As a corollary, $\zeta(2k)/\pi^{2k}$ is a rational number for $k = 1, 2, \ldots$. Very little is known about the arithmetic nature of the numbers $\zeta(3), \zeta(5), \zeta(7), \ldots$. The famous theorem of Apéry (1979) asserts that $\zeta(3)$ *is irrational*, and it is generally believed (as part of a general array of conjectures by Grothendieck, Drinfeld, Zagier, Kontsevich, Goncharov,...) that *the numbers* $\zeta(3), \zeta(5), \ldots$ *are transcendental and algebraically independent over the field* $\mathbb{Q}$ *of rational numbers.*

Zagier introduced a class of numbers, known as *Euler-Zagier sums* or *multiple zeta values* (MZV). Here is the definition

$$\zeta(k_1, \ldots, k_r) = \sum_{1 \leq n_1 < \cdots < n_r} n_1^{-k_1} \ldots n_r^{-k_r}\,, \tag{174}$$

the series being convergent if $k_r \geq 2$. It is just the specialization of the quasi-symmetric function $z(k_1, \ldots, k_r)$ obtained by putting $x_n = 1/n$ for $n = 1, 2, \ldots$. Since the quasi-symmetric functions multiply according to the quasi-shuffle rule, so do the MZV. From the example described in subsection 4.1(G) we derive

$$\zeta(3)\,\zeta(1,2) = \zeta(4,2) + \zeta(1,5) + \zeta(3,1,2) + \zeta(1,3,2) + \zeta(1,2,3)\,. \tag{175}$$

In general

$$\zeta(a)\,\zeta(b) = \zeta(a+b) + \zeta(a,b) + \zeta(b,a) \tag{176}$$

and the previous example generalizes to

$$\zeta(c)\,\zeta(a,b) = \zeta(a+c,b) + \zeta(a,b+c) + \zeta(c,a,b) + \zeta(a,c,b) + \zeta(a,b,c)\,. \tag{177}$$

If we exploit the duality between $\mathrm{NC}_\bullet$ and $\mathrm{QSym}_\bullet$, we obtain the following result:

It is possible, in a unique way, to regularize the divergent series $\zeta(k_1, \ldots, k_r)$ *when* $k_r = 1$, *in such a way that* $\zeta_*(1) = 0$ *and that the regularized values*[65] $\zeta_*(k_1, \ldots, k_r)$ *and their generating series*

$$Z_* = \sum_{k_1, \ldots, k_r} \zeta_*(k_1, \ldots, k_r)\, y_{k_1} \ldots y_{k_r} \tag{178}$$

in the noncommutative variables $y_1, y_2, \ldots$ *satisfy*

$$\Delta_*(Z_*) = Z_* \otimes Z_*\,, \tag{179}$$

as a consequence of the coproduct rule $\Delta_*(y_k) = y_k \otimes 1 + 1 \otimes y_k + \sum_{j=1}^{k-1} y_j \otimes y_{k-j}$.

[65] Of course, for $k_r \geq 2$, the convergent series $\zeta(k_1, \ldots, k_r)$ is equal to its regularized version $\zeta_*(k_1, \ldots, k_r)$.

Remark 4.5.1. It is possible to give a direct proof of the quasi-shuffle rule by simple manipulations of series. For instance, by definition

$$\zeta(a)\,\zeta(b) = \sum_{m,n} m^{-a}\, n^{-b}\,, \tag{180}$$

where the summation is over all pairs m, n of integers with $m \geq 1$, $n \geq 1$. The summation can be split into three parts:

- if $m = n$, we get $\sum m^{-a-b} = \zeta(a+b)$,
- if $m < n$, we get $\zeta(a, b)$ by definition,
- if $m > n$, we get $\zeta(b, a)$ by symmetry.

Hence (176) follows.

4.5 Application III: multiple polylogarithms

The values $\zeta(k)$ for $k = 2, 3, \ldots$ are special values of functions $Li_k(z)$ known as polylogarithm functions[66]. Here is the definition (for $k \geq 0$)

$$Li_k(z) = \sum_{n \geq 1} z^n / n^k\,. \tag{181}$$

The series converges for $|z| < 1$, and one can continue analytically $Li_k(z)$ to the cut plane $\mathbb{C}\backslash[1, \infty[$. For instance

$$Li_0(z) = \frac{z}{1-z}\,, \qquad Li_1(z) = -\log(1-z)\,. \tag{182}$$

These functions are specified by the initial value $Li_k(0) = 0$ and the differential equations

$$d\, Li_k(z) = \omega_0(z)\, Li_{k-1}(z) \quad \text{for} \quad k \geq 1 \tag{183}$$

and in particular ($k = 1$)

$$d\, Li_1(z) = \omega_1(z)\,. \tag{184}$$

The differential forms are given by

$$\omega_0(z) = dz/z\,,\ \omega_1(z) = dz/(1-z)\,. \tag{185}$$

We give two integral representations for $Li_k(z)$. First

$$Li_k(z) = \int_{[0,1]^k} z\, d^k x/(1 - z\, x_1 \ldots x_k)\,, \tag{186}$$

where each variable $x_1, \ldots, x_k$ runs over the closed interval $[0, 1]$ and $d^k x = dx_1 \ldots dx_k$. To prove (186), expand the geometric series $1/(1-a) = \sum\limits_{n \geq 1} a^{n-1}$

[66] The case of $Li_2(z)$ was known to Euler (1739).

and integrate term by term by using $\int_0^1 x^{n-1}\,dx = 1/n$. Putting $z = 1$, we find (for $k \geq 2$)

$$\zeta(k) = Li_k(1) = \int_{[0,1]^k} \frac{d^k x}{1 - x_1 \ldots x_k}\,. \tag{187}$$

The second integral representation comes from the differential equations (183) and (184). Indeed

$$\begin{aligned} Li_1(z) &= \int_0^z \omega_1(t_1) \\ Li_2(z) &= \int_0^z \omega_0(t_2)\, Li_1(t_2) = \int_0^z \omega_0(t_2) \int_0^{t_2} \omega_1(t_1)\,, \end{aligned}$$

and iterating we get

$$Li_k(z) = \int_{\Delta_k(z)} \omega_1(t_1)\,\omega_0(t_2) \ldots \omega_0(t_k)\,, \tag{188}$$

where the domain of integration $\Delta_k(z)$ consists of systems of points $t_1, \ldots, t_k$ along the oriented straight line[67] $\overrightarrow{0z}$ such that $0 < t_1 < t_2 < \cdots < t_k < z$. As a corollary ($z = 1$):

$$\zeta(k) = \int_{\Delta_k} \omega_1(t_1)\,\omega_0(t_2) \ldots \omega_0(t_k) \tag{189}$$

where Δ_k is the simplex $\{0 < t_1 < t_2 < \cdots < t_k\}$ in $\mathbb{R}^k$.

Exercise 4.5.1. Deduce (188) from (186) by a change of variables of integration.

To take care of the MZV's, introduce the *multiple polylogarithms* in one variable z

$$Li_{n_1,\ldots,n_r}(z) = \sum z^{k_r}/(k_1^{n_1} \ldots k_r^{n_r})\,, \tag{190}$$

with the summation restricted by $1 \leq k_1 < \ldots < k_r$. Special value for $z = 1$, and $n_r \geq 2$

$$\zeta(n_1, \ldots, n_r) = Li_{n_1,\ldots,n_r}(1)\,. \tag{191}$$

By computing first the differential equations satisfied by these functions, we end up with an integral representation

$$Li_{n_1,\ldots,n_r}(z) = \int_{\Delta_p(z)} \omega_{\varepsilon_1}(t_1) \ldots \omega_{\varepsilon_p}(t_p) \tag{192}$$

with the following definitions:

[67] For z in the cut plane $\mathbb{C}\backslash[1,\infty[$, the segment $[0,z]$ does not contain the singularity $t = 1$ of $\omega_1(t)$ and since $\omega_1(t_1)$ is regular for $t_1 = 0$, the previous integral makes sense and gives the analytic continuation of $Li_k(z)$.

- $p = n_1 + \cdots + n_r$ is the *weight*;
- the sequence $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_p)$ consists of 0 and 1 according to the rule

$$1\underbrace{0\ldots0}_{n_1-1}\ 1\underbrace{0\ldots0}_{n_2-1}\ 1\ldots1\ \underbrace{0\ldots0}_{n_r-1}\ .$$

This is any sequence beginning with 1, and the case $n_r \geq 2$ corresponds to the case where the sequence ε ends with 0.

Exercise 4.5.2. Check that the condition $\varepsilon_1 = 1$ corresponds to the convergence of the integral around 0, and $\varepsilon_p = 0$ (when $z = 1$) guarantees the convergence around 1.

The meaning of the previous encoding

$$n_1, \ldots, n_r \leftrightarrow \varepsilon_1, \ldots, \varepsilon_p$$

is the following: introduce the generating series

$$Li(z) = \sum_{n_1,\ldots,n_r} Li_{n_1,\ldots,n_r}(z)\, y_{n_1} \ldots y_{n_r} \tag{193}$$

in the noncommutative variables $y_1, y_2, \ldots$ Introduce other noncommutative variables x_0, x_1. If we make the substitution $y_k = x_1\, x_0^{k-1}$, then

$$y_{n_1} \ldots y_{n_k} = x_{\varepsilon_1} \ldots x_{\varepsilon_p}\ . \tag{194}$$

This defines an embedding of the algebra $k\langle Y\rangle$ into the algebra $k\langle X\rangle$ for the two alphabets

$$Y = \{y_1, y_2, \ldots\}\ , \quad X = \{x_0, x_1\}\ .$$

In $k\langle Y\rangle$, we use the coproduct Δ_* defined by[68]

$$\Delta_*(y_k) = y_k \otimes 1 + 1 \otimes y_k + \sum_{j=1}^{k-1} y_j \otimes y_{k-j}\ , \tag{195}$$

while in $k\langle X\rangle$ we use the coproduct given by

$$\Delta_{\sqcup\sqcup}(x_0) = x_0 \otimes 1 + 1 \otimes x_0\ , \quad \Delta_{\sqcup\sqcup}(x_1) = x_1 \otimes 1 + 1 \otimes x_1\ . \tag{196}$$

They don't match!

The differential equations satisfied by the functions $Li_{n_1,\ldots,n_r}(z)$ are encoded in the following

$$dLi(z) = Li(z)\, \Omega(z) \tag{197}$$

$$\Omega(z) = x_0\, \omega_0(z) + x_1\, \omega_1(z) \tag{198}$$

[68] See subsection 4.1(F).

with

$$\omega_0(z) = dz/z\,, \quad \omega_1(z) = dz/(1-z) \tag{199}$$

as before. The initial conditions are given by $Li_{n_1,\ldots,n_r}(0) = 0$ for $r \geq 1$, hence $Li(0) = Li_\emptyset(0) \cdot 1 = 1$ since $Li_\emptyset(z) = 1$ by convention. The differential form $\omega_0(z)$ has a pole at $z = 0$, hence the differential equation (197) is singular at $z = 0$, and we cannot use directly the initial condition $Li(0) = 1$. To bypass this difficulty, choose a small real parameter $\varepsilon > 0$, and denote by $U_\varepsilon(z)$ the solution of the differential equation

$$dU_\varepsilon(z) = U_\varepsilon(z)\,\Omega(z)\,, \quad U_\varepsilon(\varepsilon) = 1\,. \tag{200}$$

Then

$$Li(z) = \lim_{\varepsilon\to 0} \exp(-x_0 \log\varepsilon) \cdot U_\varepsilon(z)\,. \tag{201}$$

We are now in a position to compute the product of multiple polylogarithms. Indeed, introduce the free group F_2 in two generators g_0, g_1, and its unipotent envelope Φ_2 realized as a multiplicative group of noncommutative series in $k\langle\langle x_0, x_1\rangle\rangle$. Embed F_2 into Φ_2 by the rule $g_0 = \exp x_0$, $g_1 = \exp x_1$ (see subsection 4.3). Topologically, we interpret F_2 as the fundamental group of $\mathbb{C}\backslash\{0,1\}$ based at ε, and g_i as the class of a loop around $i \in \{0,1\}$ in counterclockwise way. The Lie algebra $\mathfrak{f}_2$ of the prounipotent group Φ_2 consists of the Lie series in x_0, x_1 and since the differential form $\Omega(z)$ takes its values in $\mathfrak{f}_2$, the solution of the differential equation (200) takes its values in the group Φ_2, and by the limiting procedure (201) so does $Li(z)$. We have proved the formula

$$\Delta_{\sqcup\!\sqcup}(Li(z)) = Li(z) \otimes Li(z)\,. \tag{202}$$

This gives the following rule for the multiplication of two multiple polylogarithm functions $Li_{n_1,\ldots,n_r}(z)$ and $Li_{m_1,\ldots,m_s}(z)$:

- encode

$$\begin{aligned} n_1, \ldots, n_r &\leftrightarrow \varepsilon_1, \ldots, \varepsilon_p \\ m_1, \ldots, m_s &\leftrightarrow \eta_1, \ldots, \eta_q \end{aligned}$$

  by sequences of 0's and 1's;
- take any shuffle of $\varepsilon_1, \ldots, \varepsilon_p$ with $\eta_1, \ldots, \eta_q$, namely $\theta_1, \ldots, \theta_{p+q}$ and decode $\theta_1, \ldots, \theta_{p+q}$ to $r_1, \ldots, r_t$;
- take the sum of the $\frac{(p+q)!}{p!\,q!}$ functions of the form $Li_{r_1,\ldots,r_t}(z)$ corresponding to the various shuffles.

We want now to compute the product of two MZV's, namely $\zeta(n_1, \ldots, n_r)$ and $\zeta(m_1, \ldots, m_s)$. When $n_r \geq 2$, we have $\zeta(n_1, \ldots, n_r) = Li_{n_1,\ldots,n_r}(1)$ but $Li_{n_1,\ldots,n_r}(z)$ diverges at $z = 1$ when $n_r = 1$. By using the differential equation (197), it can be shown that the following limit exists

$$Z_{\sqcup\!\sqcup} = \lim_{\varepsilon\to 0} Li(1-\varepsilon) \exp(x_1 \log\varepsilon)\,. \tag{203}$$

If we develop this series as

$$Z_{\sqcup\!\sqcup} = \sum_{n_1,\ldots,n_r} \zeta_{\sqcup\!\sqcup}(n_1,\ldots,n_r)\, y_{n_1}\ldots y_{n_r}\,, \tag{204}$$

we obtain $\zeta_{\sqcup\!\sqcup}(n_1,\ldots,n_r) = \zeta(n_1,\ldots,n_r)$ when $n_r \geq 2$, together with regularized values $\zeta_{\sqcup\!\sqcup}(n_1,\ldots,n_{r-1},1)$. By a limiting process, one derives the equation

$$\Delta_{\sqcup\!\sqcup}(Z_{\sqcup\!\sqcup}) = Z_{\sqcup\!\sqcup} \otimes Z_{\sqcup\!\sqcup} \tag{205}$$

from (202). We leave it to the reader to explicit the shuffle rule for multiplying MZV's.

Remark 4.5.1. The shuffle rule and the quasi-shuffle rule give two multiplication formulas for ordinary MZV's. For instance

$$\zeta(2)\,\zeta(3) = \zeta(5) + \zeta(2,3) + \zeta(3,2) \tag{206}$$

by the quasi-shuffle rule, and

$$\zeta(2)\,\zeta(3) = 3\,\zeta(2,3) + 6\,\zeta(1,4) + \zeta(3,2) \tag{207}$$

by the shuffle rule. By elimination, we deduce a linear relation

$$\zeta(5) = 2\,\zeta(2,3) + 6\,\zeta(1,4)\,. \tag{208}$$

But in general, the two regularizations $\zeta_*(n_1,\ldots,n_r)$ and $\zeta_{\sqcup\!\sqcup}(n_1,\ldots,n_r)$ differ when $n_r = 1$. We refer the reader to our presentation in [22] for more details and precise conjectures about the linear relations satisfied by the MZV's.

Remark 4.5.2. From equation (192), one derives the integral relation

$$\zeta(n_1,\ldots,n_r) = \int_{\Delta_p} \omega_{\varepsilon_1}(t_1)\ldots\omega_{\varepsilon_p}(t_p) \tag{209}$$

with the encoding $n_1,\ldots,n_r \leftrightarrow \varepsilon_1,\ldots,\varepsilon_p$ (hence $p = n_1 + \ldots + n_r$ is the weight) and the domain of integration

$$\Delta_p = \{0 < t_1 < \cdots < t_p < 1\} \subset \mathbb{R}^p\,.$$

When multiplying $\zeta(n_1,\ldots,n_r)$ with $\zeta(m_1,\ldots,m_s)$ we encounter an integral over $\Delta_p \times \Delta_q$. This product of simplices can be subdivided into a collection of $\frac{(p+q)!}{p!\,q!}$ simplices corresponding to the various shuffles of $\{1,\ldots,p\}$ with $\{1,\ldots,q\}$, that is the permutations σ in S_{p+q} such that $\sigma(1) < \ldots < \sigma(p)$ and $\sigma(p+1) < \ldots < \sigma(p+q)$. Hence a product integral over $\Delta_p \times \Delta_q$ can be decomposed as a sum of $\frac{(p+q)!}{p!\,q!}$ integrals over Δ_{p+q}. This method gives another proof of the shuffle product formula for MZV's.

4.6 Composition of series [27]

The composition of series gives another example of a prounipotent group. We consider formal transformations of the form[69]

$$\varphi(x) = x + a_1\, x^2 + a_2\, x^3 + \cdots + a_i\, x^{i+1} + \cdots\,, \tag{210}$$

that is transformations defined around 0 by their Taylor series with $\varphi(0) = 0$, $\varphi'(0) = 1$. Under composition, they form a group $\mathrm{Comp}(\mathbb{C})$, and we proceed to interpret it as an algebraic group of infinite triangular matrices.

Given $\varphi(x)$ as above, develop

$$\varphi(x)^i = \sum_{j \geq 1} a_{ij}(\varphi)\, x^j\,, \tag{211}$$

for $i \geq 1$, and denote by $A(\varphi)$ the infinite matrix $(a_{ij}(\varphi))_{i\geq 1, j\geq 1}$. Since $\varphi(x)$ begins with x, then $\varphi(x)^i$ begins with x^i. Hence $a_{ii}(\varphi) = 1$ and $a_{ij}(\varphi) = 0$ for $j < i$: *the matrix $A(\varphi)$ belongs to* $T_\infty(\mathbb{C})$. Furthermore, since $(\varphi \circ \psi)^i = \varphi^i \circ \psi$, we have $A(\varphi \circ \psi) = A(\varphi)\, A(\psi)$. Moreover, $a_{1,j+1}(\varphi)$ is the coefficient $a_j(\varphi)$ of x^{j+1} in $\varphi(x)$, hence the map $\varphi \mapsto A(\varphi)$ is a faithful representation A of the group $\mathrm{Comp}(\mathbb{C})$ into $T_\infty(\mathbb{C})$. By expanding $\varphi(x)^i$ by the multinomial theorem, we obtain the following expression for the $a_{ij}(\varphi) = a_{ij}$ in terms of the parameters a_i

$$a_{ij} = \sum (i!/n_0!)(a_1^{n_1}/n_1!)(a_2^{n_2}/n_2!)\ldots(a_{j-1}^{n_{j-1}}/n_{j-1}!) \tag{212}$$

where the summation extends over all system of indices $n_0, n_1, \ldots, n_{j-1}$, where each n_k is a nonnegative integer and

$$\begin{cases} n_0 + \cdots + n_{j-1} = i\,, & (213)\\ 1 \cdot n_0 + 2 \cdot n_1 + \ldots + j \cdot n_{j-1} = j\,. & (214)\end{cases}$$

Since $a_1 = a_{12}$, $a_2 = a_{13}$, $a_3 = a_{14}, \ldots$ the formulas (212) to (214) give an explicit set of algebraic equations for the subgroup $A(\mathrm{Comp}(\mathbb{C}))$ of $T_\infty(\mathbb{C})$. The group $\mathrm{Comp}(\mathbb{C})$ is a proalgebraic group with $\mathcal{O}(\mathrm{Comp})$ equal to the polynomial ring $\mathbb{C}[a_1, a_2, \ldots]$. For the group $T_\infty(\mathbb{C})$, the coproduct in $\mathcal{O}(T_\infty)$ is given by $\Delta(a_{ij}) = \sum_{i \leq k \leq j} a_{ik} \otimes a_{kj}$. Hence the coproduct in $\mathcal{O}(\mathrm{Comp})$ is given by

$$\Delta(a_i) = 1 \otimes a_i + \sum_{j=1}^{i-1} a_j \otimes a_{j+1,i+1} + a_i \otimes 1\,, \tag{215}$$

[69] The coefficients a_i in the series $\varphi(x)$ are supposed to be complex numbers, but they might be taken from an arbitrary field k of characteristic 0.

where we use the rule (212) to define the elements $a_{j+1,i+1}$ in $\mathbb{C}[a_1, a_2, \ldots]$. This formula can easily be translated in *Faa di Bruno's formula* giving the higher derivatives of $f(g(x))$.

Exercise 4.6.1. Prove directly the coassociativity of the coproduct defined by (212) and (215)!

Remark 4.6.1. If we give degree i to a_i, it follows from (212), (213) and (214) that a_{ij} is homogeneous of degree $j-i$. Hence the coproduct given by (215) is homogeneous and $\mathcal{O}(\mathrm{Comp})$ is a graded Hopf algebra. Here is an explanation. We denote by $\mathbb{G}_m(\mathbb{C})$ the group $GL_1(\mathbb{C})$, that is the nonzero complex numbers under multiplication, with the coordinate ring $\mathcal{O}(\mathbb{G}_m) = \mathbb{C}[t, t^{-1}]$. It acts by scaling $H_t(x) = tx$, and the corresponding matrix $A(H_t)$ is the diagonal matrix M_t with entries $t, t^2, \ldots$. For t in $\mathbb{G}_m(\mathbb{C})$ and φ in $\mathrm{Comp}(\mathbb{C})$, the transformation $H_t^{-1} \circ \varphi \circ H_t$ is given by $t^{-1}\,\varphi(tx) = x + t\,a_1\,x^2 + t^2\,a_2\,x^3 + \cdots$ and this scaling property (a_i going into $t^i\,a_i$) explains why we give the degree i to a_i. Furthermore, in matrix terms, $M_t^{-1} A\, M_t$ has entries a_{ij} of A multiplied by t^{j-i}, hence the degree $j-i$ to a_{ij}!

To conclude, let us consider the Lie algebra $\mathfrak{comp}$ of the proalgebraic group $\mathrm{Comp}(\mathbb{C})$. In $\mathcal{O}(\mathrm{Comp})$ the kernel of the counit $\varepsilon : \mathcal{O}(\mathrm{Comp}) \to \mathbb{C}$ is the ideal J generated by $a_1, a_2, \ldots$, hence the vector space J/J^2 has a basis consisting of the cosets $\bar{a}_i = a_i + J$ for $i \geq 1$. The dual of J/J^2 can be identified with $\mathfrak{comp}$ and consists of the infinite series $u_1 D_1 + u_2 D_2 + \cdots$ where $\langle D_i, \bar{a}_j \rangle = \delta_{ij}$.

To compute the bracket in $\mathfrak{comp}$, consider the reduced coproduct $\bar{\Delta}$ defined by $\bar{\Delta}(x) = \Delta(x) - x \otimes 1 - 1 \otimes x$ for x in J, mapping J into $J \otimes J$. If σ exchanges the factors in $J \otimes J$, then $\bar{\Delta} - \sigma \circ \bar{\Delta}$ defines by factoring $\mod J^2$ a map δ from $L := J/J^2$ to $\Lambda^2 L$. Hence L is a Lie coalgebra and $\mathfrak{comp}$ is the dual Lie algebra of L. Explicitly, to compute $\delta(\bar{a}_i)$, keep in $\Delta(a_i)$ the bilinear terms in a_k's and replaces a_k by $\bar{a}_k$. We obtain a map δ_1 from L to $L \otimes L$, and δ is the antisymmetrisation of δ_1. We quote the result

$$\delta_1(\bar{a}_i) = \sum_{j=1}^{i-1} (j+1)\,\bar{a}_j \otimes \bar{a}_{i-j} \tag{216}$$

hence

$$\delta(\bar{a}_i) = \sum_{j=1}^{i-1} (2j-1)\,\bar{a}_j \otimes \bar{a}_{i-j}\,. \tag{217}$$

Dually, δ_1 defines a product in $\mathfrak{comp}$, defined by

$$D_j * D_k = (j+1)\,D_{j+k} \tag{218}$$

and the bracket, defined by $[D, D'] = D * D' - D' * D$, is dual to δ and is given explicitly by

$$[D_j, D_k] = (j-k)\,D_{j+k}\,. \tag{219}$$

Remark 4.6.2. D_j corresponds to the differential operator $-x^{j+1}\frac{d}{dx}$ and the bracket is the Lie bracket of first order differential operators.

Exercise 4.6.2. Give the matrix representation of D_i.

For a general algebraic group (or Hopf algebra), the operation $D * D'$ has no interesting, nor intrinsic, properties. The feature here is that in the coproduct (215), for the generators a_i of $\mathcal{O}(\mathrm{Comp})$, one has

$$\Delta(a_i) = 1 \otimes a_i + \sum_j a_j \otimes u_{ji}$$

where u_{ji} belongs to $\mathcal{O}(\mathrm{Comp})$ (linearity on the left). The $*$-product then satisfies the four-term identity

$$D * (D' * D'') - (D * D') * D'' = D * (D'' * D') - (D * D'') * D'$$

due to Vinberg. *From Vinberg's identity, one derives easily Jacobi identity for the bracket* $[D, D'] = D * D' - D' * D$. *Notice that Vinberg's identity is a weakening of the associativity for the* $*$*-product.*

4.7 Concluding remarks

To deal with the composition of functions in the many variables case, one needs graphical methods based on trees. The corresponding methods have been developed by Loday and Ronco [54, 67]. There exists a similar presentation of Connes-Kreimer Hopf algebra of Feynman diagrams interpreted in terms of composition of nonlinear transformations of Lagrangians (see a forthcoming paper [23]).

References

1. A. Borel, Sur l'homologie et la cohomologie des groupes de Lie compacts connexes, *Amer. J. Math.* **76** (1954), 273-342. Reprinted in *Œuvres, Collected Papers*, vol. 1, pp. 322-391, Springer, Berlin (1983).
2. A. Borel, Topology of Lie groups and characteristic classes, *Bull. Am. Math. Soc.* **61** (1955), 397-432. Reprinted in *Œuvres, Collected Papers*, vol. 1, pp. 402-437, Springer, Berlin (1983).
3. A. Borel, Sur la torsion des groupes de Lie, *J. Math. Pures Appl.* **35** (1955), 127-139. Reprinted in *Œuvres, Collected Papers*, vol. 1, pp. 477-489, Springer, Berlin (1983).
4. A. Borel, *Linear algebraic groups*, 2nd edition, Springer, Berlin (1982).
5. A. Borel (and C. Chevalley), The Betti numbers of the exceptional groups, *Mem. Amer. Math. Soc.* **14** (1955), 1-9. Reprinted in *Œuvres, Collected Papers*, vol. 1, pp. 451-459, Springer, Berlin (1983).

6. N. Bourbaki, *Groupes et algèbres de Lie*, Chap. 1, and Chap. 2, 3, Hermann, Paris (1971 and 1972).
7. N. Bourbaki, *Groupes et algèbres de Lie*, Chap. 4, 5 et 6, Masson, Paris (1981).
8. N. Bourbaki, *Algèbre*, Chap. 1, 2 et 3, Hermann, Paris (1970).
9. N. Bourbaki, *Espaces vectoriels topologiques*, Chap. 1 à 5, Masson, Paris (1981).
10. R. Brauer, Sur les invariants intégraux des variétés des groupes de Lie simples clos, *C.R. Acad. Sci. Paris* **201** (1935), 419-421.
11. E. Cartan, La géométrie des groupes simples, *Annali di Mat.* **4** (1927), 209-256. Reprinted in *Œuvres Complètes*, Part I, vol. 2, pp. 793-840, Gauthier-Villars, Paris (1952).
12. E. Cartan, Sur les invariants intégraux de certains espaces homogènes clos et les propriétés topologiques de ces espaces, *Ann. Soc. Pol. Math.* **8** (1929), 181-225. Reprinted in *Œuvres Complètes*, Part I, vol. 2, pp. 1081-1126, Gauthier-Villars, Paris (1952).
13. E. Cartan, La théorie des groupes finis et continus et l'*Analysis Situs*, *Mém. Sci. Math.*, Vol. 42, Gauthier-Villars, Paris (1930). Reprinted in *Œuvres Complètes*, Part I, vol. 2, pp. 1165-1226, Gauthier-Villars, Paris (1952).
14. P. Cartier, Dualité de Tannaka des groupes et algèbres de Lie, *C.R. Acad. Sci. Paris* **242** (1956), 322-325.
15. P. Cartier, Théorie différentielle des groupes algébriques, *C.R. Acad. Sci. Paris* **244** (1957), 540-542.
16. P. Cartier, *Hyperalgèbres et groupes de Lie formels*, Institut Henri Poincaré, Paris (1957).
17. P. Cartier, Isogénies des variétés de groupes, *Bull. Soc. Math. France* **87** (1959), 191-220.
18. P. Cartier, Groupes algébriques et groupes formels, *in "Colloque sur la théorie des groupes algébriques"* (Bruxelles, 1962), pp. 87-111, Gauthier-Villars, Paris (1962).
19. P. Cartier, On the structure of free Baxter algebras, *Adv. Math.* **9** (1972), 253-265.
20. P. Cartier, La théorie classique et moderne des fonctions symétriques, *Astérisque* **105–106** (1983), 1-23.
21. P. Cartier, Jacobiennes généralisées, monodromie unipotente et intégrales itérées, *Astérisque* **161–162** (1988), 31-52.
22. P. Cartier, Fonctions polylogarithmes, nombres polyzêtas et groupes pro-unipotents, *Astérisque* **282** (2002), 137-173.
23. P. Cartier and V. Féray, Nonlinear transformations in Lagrangians and Connes-Kreimer Hopf algebra, in preparation.
24. C. Chevalley, *Theory of Lie groups*, Princeton Univ. Press, Princeton (1946).
25. C. Chevalley, *Théorie des groupes de Lie*, tome II: *Groupes algébriques*, Hermann, Paris (1951).
26. A. Connes and M. Marcolli, Renormalization, the Riemann-Hilbert correspondence, and motivic Galois theory, in this volume, pages 617-714.
27. A. Connes and H. Moscovici, Hopf algebras, cyclic cohomology and the transverse index theorem, *Comm. Math. Phys.* **198** (1998), 199-246.
28. A. Connes and H. Moscovici, Modular Hecke algebras and their Hopf symmetry, *Moscow Math. J.* **4** (2004), 67-109.

29. P. Deligne, Le groupe fondamental de la droite projective moins trois points, *in "Galois groups over $\mathbb{Q}$"* (edited by Y. Ihara, K. Ribet and J.-P. Serre), pp. 79-297, Springer, Berlin (1989).
30. P. Deligne, Catégories tannakiennes, *in "The Grothendieck Festschrift"* (edited by P. Cartier and *al.*), vol. II, pp. 111-195, Birkhäuser, Boston (1990).
31. M. Demazure and A. Grothendieck, *Schémas en groupes*, 3 vol., Springer, Berlin (1970).
32. M. Demazure and P. Gabriel, *Introduction to algebraic geometry and algebraic groups*, North Holland, Amsterdam (1980).
33. G. de Rham, Sur l'*Analysis Situs* des variétés à n dimensions, *J. Math. Pures Appl.* **10** (1931), 115-200.
34. J. Dieudonné, *Introduction to the theory of formal groups*, Marcel Dekker, New York (1973).
35. S. Doplicher and J.E. Roberts, Endomorphisms of C^*-algebras, cross products and duality for compact groups, *Ann. of Math.* **130** (1989), 75-119.
36. S. Doplicher and J.E. Roberts, A new duality theory for compact groups, *Invent. Math.* **98** (1989), 157-218.
37. Ch. Ehresmann, Sur la topologie de certains espaces homogènes, *Ann. of Math.* **35** (1934), 396-443. Reprinted in *Charles Ehresmann: œuvres complètes et commentées*, Vol. I, pp. 6-53, Amiens (1984).
38. Ch. Ehresmann, Sur la topologie de certaines variétés algébriques réelles, *J. Math. Pures Appl.* **16** (1937), 69-100. Reprinted in *Charles Ehresmann: œuvres complètes et commentées*, Vol. I, pp. 55-86, Amiens (1984).
39. Ch. Ehresmann, Sur la variété des génératrices planes d'une quadrique réelle et sur la topologie du groupe orthogonal à n variables, *C.R. Acad. Sci. Paris* **208** (1939), 321-323. Reprinted in *Charles Ehresmann: œuvres complètes et commentées*, Vol. I, pp. 304-306, Amiens (1984).
40. Ch. Ehresmann, Sur la topologie des groupes simples clos, *C.R. Acad. Sci. Paris* **208** (1939), 1263-1265. Reprinted in *Charles Ehresmann: œuvres complètes et commentées*, Vol. I, pp. 307-309, Amiens (1984).
41. I.M. Gelfand, D. Krob, A. Lascoux, B. Leclerc, V.S. Retakh and J.-Y. Thibon, Noncommutative symmetric functions, *Adv. Math.* **112** (1995), 218-348.
42. F. Goichot, Un théorème de Milnor-Moore pour les algèbres de Leibniz, *in "Dialgebras and related operads"*, pp. 111-133, Springer, Berlin (2001).
43. P.P. Grivel, Une histoire du théorème de Poincaré-Birkhoff-Witt, *Expo. Math.* **22** (2004), 145-184.
44. Harish-Chandra, Lie algebras and the Tannaka duality theorem, *Ann. of Math.* **51** (1950), 299-330. Reprinted in *Collected Papers*, vol. I, pp. 259-290, Springer, Berlin (1984).
45. W.V.D. Hodge, *The theory and applications of harmonic integrals* (2nd edition), Cambridge University Press, Cambridge (1952).
46. M. Hoffman, Quasi-shuffle products, *J. Alg. Combinat.* **11** (2000), 46-68.
47. H. Hopf, Über die Topologie der Gruppen-Mannigfaltigkeiten und ihrer Verallgemeinerungen, *Ann. of Math.* **42** (1941), 22-52. Reprinted in *Selecta Heinz Hopf*, pp. 119-151, Springer, Berlin (1964).
48. H. Hopf, Über den Rang geschlossener Liescher Gruppen, *Comm. Math. Helv.* **13** (1940-1), 119-143. Reprinted in *Selecta Heinz Hopf*, pp. 152-174, Springer, Berlin (1964).
49. H. Hopf and H. Samelson, Ein Satz über die Wirkungsräume geschlossener Liescher Gruppen, *Comm. Math. Helv.* **13** (1940-1), 240-251.

50. D. Krob, B. Leclerc and J.-Y. Thibon, Noncommutative symmetric functions, II: transformations of alphabets, *J. Algebra Comput.* **7** (1997), 181-264.
51. J. Leray, Sur l'homologie des groupes de Lie, des espaces homogènes et des espaces fibrés principaux, *in "Colloque de Topologie Algébrique"*, Bruxelles (1950), pp. 101-115. Reprinted in *Œuvres scientifiques*, vol. I, pp. 447-461, Springer, Berlin (1998).
52. J. Leray, L'anneau spectral et l'anneau filtré d'homologie d'un espace localement compact et d'une application continue, *J. Math. Pures Appl.* **29** (1950), 1-139. Reprinted in *Œuvres scientifiques*, vol. I, pp. 261-401, Springer, Berlin (1998).
53. J.-L. Loday, On the algebra of quasi-shuffles, to appear.
54. J.-L. Loday and M. Ronco, Hopf algebra of the planar binary trees, *Adv. Math.* **139** (1998), 293-309.
55. L. Loomis, *An introduction to abstract harmonic analysis*, van Nostrand C$^{\text{o}}$, Princeton (1953).
56. M. Lothaire, *Algebraic combinatorics on words*, Cambridge Univ. Press, Cambridge (2002).
57. I.G. MacDonald, *Symmetric functions and Hall polynomials* (2nd edition), Oxford Univ. Press, New York (1995).
58. C. Malvenuto and C. Reutenauer, Duality between quasi-symmetric functions and the Solomon descent algebra, *J. Algebra* **177** (1995), 967-982.
59. J.W. Milnor and J.C. Moore, On the structure of Hopf algebras, *Ann. of Math.* **81** (1965), 211-264.
60. F. Patras, L'algèbre des descentes d'une bigèbre graduée, *J. Algebra* **170** (1994), 547-566.
61. H. Poincaré, Analysis Situs, *Journ. Ecole Polyt.* **1** (1895), 1-121. Reprinted in *Œuvres*, vol. VI, pp. 193-288, Gauthier-Villars, Paris (1953).
62. H. Poincaré, Sur les groupes continus, *Camb. Phil. Trans.* **18** (1899), 220-255. Reprinted in *Œuvres*, vol. III, pp. 173-212, Gauthier-Villars, Paris (1965).
63. L.S. Pontrjagin, Homologies in compact Lie groups (in Russian), *Math. Sbornik* **6** (1939), 389-422.
64. L.S. Pontrjagin, Über die topologische Struktur der Lie'schen Gruppen, *Comm. Math. Helv.* **13** (1940-1), 227-238.
65. D. Quillen, Rational homotopy theory, *Ann. of Math.* **90** (1969), 205-295.
66. C. Reutenauer, *Free Lie algebras*, Oxford Univ. Press, New York (1993).
67. M. Ronco, A Milnor-Moore theorem for dendriform Hopf algebras, *C.R. Acad. Sci. Paris* (série I) **332** (2000), 109-114.
68. M. Ronco, Eulerian idempotents and Milnor-Moore theorem for certain noncommutative Hopf algebras, *J. Algebra* **254** (2002), 152-172.
69. N. Saavedra, *Catégories tannakiennes*, Springer, Berlin (1972).
70. H. Samelson, Beiträge zur Topologie der Gruppen-Mannigfaltigkeiten, *Ann. of Math.* **42** (1941), 1091-1137.
71. H. Samelson, Topology of Lie groups, *Bull. Am. Math. Soc.* **58** (1952), 2-37.
72. J.-P. Serre, Gèbres, *Enseignement Math.* **39** (1993), 33-85. Reprinted in *Œuvres, Collected Papers*, vol. IV, pp. 272-324, Springer, Berlin (2000).
73. H. Weyl, Theorie der Darstellung kontinuierlichen halb-einfacher Gruppen durch lineare Transformationen, I, II, III, *Math. Zeit.* **23** (1925), 271-309; **24** (1926), 328-376 and 377-395. Reprinted in *Gesammelte Abhandlungen*, Band II, pp. 543-647, Springer, Berlin (1968).

74. H. Weyl, *The classical groups* (2nd edition), Princeton University Press, Princeton (1946).

Index