PURE AND APPLIED MATHEMATICS

A Series of Monographs and Textbooks

HOPF ALGEBRAS

An Introduction

Sorin Dăscălescu
Constantin Năstăsescu
Șerban Raianu

HOPF ALGEBRAS

PURE AND APPLIED MATHEMATICS

A Program of Monographs, Textbooks, and Lecture Notes

MONOGRAPHS AND TEXTBOOKS IN PURE AND APPLIED MATHEMATICS

1. *K. Yano,* Integral Formulas in Riemannian Geometry (1970)
2. *S. Kobayashi,* Hyperbolic Manifolds and Holomorphic Mappings (1970)
3. *V. S. Vladimirov,* Equations of Mathematical Physics (A. Jeffrey, ed.; A. Littlewood, trans.) (1970)
4. *B. N. Pshenichnyi,* Necessary Conditions for an Extremum (L. Neustadt, translation ed.; K. Makowski, trans.) (1971)
5. *L. Narici et al.,* Functional Analysis and Valuation Theory (1971)
6. *S. S. Passman,* Infinite Group Rings (1971)
7. *L. Dornhoff,* Group Representation Theory. Part A: Ordinary Representation Theory. Part B: Modular Representation Theory (1971, 1972)
8. *W. Boothby and G. L. Weiss, eds.,* Symmetric Spaces (1972)
9. *Y. Matsushima,* Differentiable Manifolds (E. T. Kobayashi, trans.) (1972)
10. *L. E. Ward, Jr.,* Topology (1972)
11. *A. Babakhanian,* Cohomological Methods in Group Theory (1972)
12. *R. Gilmer,* Multiplicative Ideal Theory (1972)
13. *J. Yeh,* Stochastic Processes and the Wiener Integral (1973)
14. *J. Barros-Neto,* Introduction to the Theory of Distributions (1973)
15. *R. Larsen,* Functional Analysis (1973)
16. *K. Yano and S. Ishihara,* Tangent and Cotangent Bundles (1973)
17. *C. Procesi,* Rings with Polynomial Identities (1973)
18. *R. Hermann,* Geometry, Physics, and Systems (1973)
19. *N. R. Wallach,* Harmonic Analysis on Homogeneous Spaces (1973)
20. *J. Dieudonné,* Introduction to the Theory of Formal Groups (1973)
21. *I. Vaisman,* Cohomology and Differential Forms (1973)
22. *B.-Y. Chen,* Geometry of Submanifolds (1973)
23. *M. Marcus,* Finite Dimensional Multilinear Algebra (in two parts) (1973, 1975)
24. *R. Larsen,* Banach Algebras (1973)
25. *R. O. Kujala and A. L. Vitter, eds.,* Value Distribution Theory: Part A; Part B: Deficit and Bezout Estimates by Wilhelm Stoll (1973)
26. *K. B. Stolarsky,* Algebraic Numbers and Diophantine Approximation (1974)
27. *A. R. Magid,* The Separable Galois Theory of Commutative Rings (1974)
28. *B. R. McDonald,* Finite Rings with Identity (1974)
29. *J. Satake,* Linear Algebra (S. Koh et al., trans.) (1975)
30. *J. S. Golan,* Localization of Noncommutative Rings (1975)
31. *G. Klambauer,* Mathematical Analysis (1975)
32. *M. K. Agoston,* Algebraic Topology (1976)
33. *K. R. Goodearl,* Ring Theory (1976)
34. *L. E. Mansfield,* Linear Algebra with Geometric Applications (1976)
35. *N. J. Pullman,* Matrix Theory and Its Applications (1976)
36. *B. R. McDonald,* Geometric Algebra Over Local Rings (1976)
37. *C. W. Groetsch,* Generalized Inverses of Linear Operators (1977)
38. *J. E. Kuczkowski and J. L. Gersting,* Abstract Algebra (1977)
39. *C. O. Christenson and W. L. Voxman,* Aspects of Topology (1977)
40. *M. Nagata,* Field Theory (1977)
41. *R. L. Long,* Algebraic Number Theory (1977)
42. *W. F. Pfeffer,* Integrals and Measures (1977)
43. *R. L. Wheeden and A. Zygmund,* Measure and Integral (1977)
44. *J. H. Curtiss,* Introduction to Functions of a Complex Variable (1978)
45. *K. Hrbacek and T. Jech,* Introduction to Set Theory (1978)
46. *W. S. Massey,* Homology and Cohomology Theory (1978)
47. *M. Marcus,* Introduction to Modern Algebra (1978)
48. *E. C. Young,* Vector and Tensor Analysis (1978)
49. *S. B. Nadler, Jr.,* Hyperspaces of Sets (1978)
50. *S. K. Segal,* Topics in Group Kings (1978)
51. *A. C. M. van Rooij,* Non-Archimedean Functional Analysis (1978)
52. *L. Corwin and R. Szczarba,* Calculus in Vector Spaces (1979)
53. *C. Sadosky,* Interpolation of Operators and Singular Integrals (1979)
54. *J. Cronin,* Differential Equations (1980)
55. *C. W. Groetsch,* Elements of Applicable Functional Analysis (1980)

56. *I. Vaisman,* Foundations of Three-Dimensional Euclidean Geometry (1980)
57. *H. I. Freedan,* Deterministic Mathematical Models in Population Ecology (1980)
58. *S. B. Chae,* Lebesgue Integration (1980)
59. *C. S. Rees et al.,* Theory and Applications of Fourier Analysis (1981)
60. *L. Nachbin,* Introduction to Functional Analysis (R. M. Aron, trans.) (1981)
61. *G. Orzech and M. Orzech,* Plane Algebraic Curves (1981)
62. *R. Johnsonbaugh and W. E. Pfaffenberger,* Foundations of Mathematical Analysis (1981)
63. *W. L. Voxman and R. H. Goetschel,* Advanced Calculus (1981)
64. *L. J. Corwin and R. H. Szczarba,* Multivariable Calculus (1982)
65. *V. I. Istrăţescu,* Introduction to Linear Operator Theory (1981)
66. *R. D. Järvinen,* Finite and Infinite Dimensional Linear Spaces (1981)
67. *J. K. Beem and P. E. Ehrlich,* Global Lorentzian Geometry (1981)
68. *D. L. Armacost,* The Structure of Locally Compact Abelian Groups (1981)
69. *J. W. Brewer and M. K. Smith, eds.,* Emmy Noether: A Tribute (1981)
70. *K. H. Kim,* Boolean Matrix Theory and Applications (1982)
71. *T. W. Wieting,* The Mathematical Theory of Chromatic Plane Ornaments (1982)
72. *D. B.Gauld,* Differential Topology (1982)
73. *R. L. Faber,* Foundations of Euclidean and Non-Euclidean Geometry (1983)
74. *M. Carmeli,* Statistical Theory and Random Matrices (1983)
75. *J. H. Carruth et al.,* The Theory of Topological Semigroups (1983)
76. *R. L. Faber,* Differential Geometry and Relativity Theory (1983)
77. *S. Barnett,* Polynomials and Linear Control Systems (1983)
78. *G. Karpilovsky,* Commutative Group Algebras (1983)
79. *F. Van Oystaeyen and A. Verschoren,* Relative Invariants of Rings (1983)
80. *I. Vaisman,* A First Course in Differential Geometry (1984)
81. *G. W. Swan,* Applications of Optimal Control Theory in Biomedicine (1984)
82. *T. Petrie and J. D. Randall,* Transformation Groups on Manifolds (1984)
83. *K. Goebel and S. Reich,* Uniform Convexity, Hyperbolic Geometry, and Nonexpansive Mappings (1984)
84. *T. Albu and C. Năstăsescu,* Relative Finiteness in Module Theory (1984)
85. *K. Hrbacek and T. Jech,* Introduction to Set Theory: Second Edition (1984)
86. *F. Van Oystaeyen and A. Verschoren,* Relative Invariants of Rings (1984)
87. *B. R. McDonald,* Linear Algebra Over Commutative Rings (1984)
88. *M. Namba,* Geometry of Projective Algebraic Curves (1984)
89. *G. F. Webb,* Theory of Nonlinear Age-Dependent Population Dynamics (1985)
90. *M. R. Bremner et al.,* Tables of Dominant Weight Multiplicities for Representations of Simple Lie Algebras (1985)
91. *A. E. Fekete,* Real Linear Algebra (1985)
92. *S. B. Chae,* Holomorphy and Calculus in Normed Spaces (1985)
93. *A. J. Jerri,* Introduction to Integral Equations with Applications (1985)
94. *G. Karpilovsky,* Projective Representations of Finite Groups (1985)
95. *L. Narici and E. Beckenstein,* Topological Vector Spaces (1985)
96. *J. Weeks,* The Shape of Space (1985)
97. *P. R. Gribik and K. O. Kortanek,* Extremal Methods of Operations Research (1985)
98. *J.-A. Chao and W. A. Woyczynski, eds.,* Probability Theory and Harmonic Analysis (1986)
99. *G. D. Crown et al.,* Abstract Algebra (1986)
100. *J. H. Carruth et al.,* The Theory of Topological Semigroups, Volume 2 (1986)
101. *R. S. Doran and V. A. Belfi,* Characterizations of C*-Algebras (1986)
102. *M. W. Jeter,* Mathematical Programming (1986)
103. *M. Altman,* A Unified Theory of Nonlinear Operator and Evolution Equations with Applications (1986)
104. *A. Verschoren,* Relative Invariants of Sheaves (1987)
105. *R. A. Usmani,* Applied Linear Algebra (1987)
106. *P. Blass and J. Lang,* Zariski Surfaces and Differential Equations in Characteristic $p > 0$ (1987)
107. *J. A. Reneke et al.,* Structured Hereditary Systems (1987)
108. *H. Busemann and B. B. Phadke,* Spaces with Distinguished Geodesics (1987)
109. *R. Harte,* Invertibility and Singularity for Bounded Linear Operators (1988)
110. *G. S. Ladde et al.,* Oscillation Theory of Differential Equations with Deviating Arguments (1987)
111. *L. Dudkin et al.,* Iterative Aggregation Theory (1987)
112. *T. Okubo,* Differential Geometry (1987)

113. *D. L. Stancl and M. L. Stancl,* Real Analysis with Point-Set Topology (1987)
114. *T. C. Gard,* Introduction to Stochastic Differential Equations (1988)
115. *S. S. Abhyankar,* Enumerative Combinatorics of Young Tableaux (1988)
116. *H. Strade and R. Farnsteiner,* Modular Lie Algebras and Their Representations (1988)
117. *J. A. Huckaba,* Commutative Rings with Zero Divisors (1988)
118. *W. D. Wallis,* Combinatorial Designs (1988)
119. *W. Więsław,* Topological Fields (1988)
120. *G. Karpilovsky,* Field Theory (1988)
121. *S. Caenepeel and F. Van Oystaeyen,* Brauer Groups and the Cohomology of Graded Rings (1989)
122. *W. Kozlowski,* Modular Function Spaces (1988)
123. *E. Lowen-Colebunders,* Function Classes of Cauchy Continuous Maps (1989)
124. *M. Pavel,* Fundamentals of Pattern Recognition (1989)
125. *V. Lakshmikantham et al.,* Stability Analysis of Nonlinear Systems (1989)
126. *R. Sivaramakrishnan,* The Classical Theory of Arithmetic Functions (1989)
127. *N. A. Watson,* Parabolic Equations on an Infinite Strip (1989)
128. *K. J. Hastings,* Introduction to the Mathematics of Operations Research (1989)
129. *B. Fine,* Algebraic Theory of the Bianchi Groups (1989)
130. *D. N. Dikranjan et al.,* Topological Groups (1989)
131. *J. C. Morgan II,* Point Set Theory (1990)
132. *P. Biler and A. Witkowski,* Problems in Mathematical Analysis (1990)
133. *H. J. Sussmann,* Nonlinear Controllability and Optimal Control (1990)
134. *J.-P. Florens et al.,* Elements of Bayesian Statistics (1990)
135. *N. Shell,* Topological Fields and Near Valuations (1990)
136. *B. F. Doolin and C. F. Martin,* Introduction to Differential Geometry for Engineers (1990)
137. *S. S. Holland, Jr.,* Applied Analysis by the Hilbert Space Method (1990)
138. *J. Okniński,* Semigroup Algebras (1990)
139. *K. Zhu,* Operator Theory in Function Spaces (1990)
140. *G. B. Price,* An Introduction to Multicomplex Spaces and Functions (1991)
141. *R. B. Darst,* Introduction to Linear Programming (1991)
142. *P. L. Sachdev,* Nonlinear Ordinary Differential Equations and Their Applications (1991)
143. *T. Husain,* Orthogonal Schauder Bases (1991)
144. *J. Foran,* Fundamentals of Real Analysis (1991)
145. *W. C. Brown,* Matrices and Vector Spaces (1991)
146. *M. M. Rao and Z. D. Ren,* Theory of Orlicz Spaces (1991)
147. *J. S. Golan and T. Head,* Modules and the Structures of Rings (1991)
148. *C. Small,* Arithmetic of Finite Fields (1991)
149. *K. Yang,* Complex Algebraic Geometry (1991)
150. *D. G. Hoffman et al.,* Coding Theory (1991)
151. *M. O. González,* Classical Complex Analysis (1992)
152. *M. O. González,* Complex Analysis (1992)
153. *L. W. Baggett,* Functional Analysis (1992)
154. *M. Sniedovich,* Dynamic Programming (1992)
155. *R. P. Agarwal,* Difference Equations and Inequalities (1992)
156. *C. Brezinski,* Biorthogonality and Its Applications to Numerical Analysis (1992)
157. *C. Swartz,* An Introduction to Functional Analysis (1992)
158. *S. B. Nadler, Jr.,* Continuum Theory (1992)
159. *M. A. Al-Gwaiz,* Theory of Distributions (1992)
160. *E. Perry,* Geometry: Axiomatic Developments with Problem Solving (1992)
161. *E. Castillo and M. R. Ruiz-Cobo,* Functional Equations and Modelling in Science and Engineering (1992)
162. *A. J. Jerri,* Integral and Discrete Transforms with Applications and Error Analysis (1992)
163. *A. Charlier et al.,* Tensors and the Clifford Algebra (1992)
164. *P. Biler and T. Nadzieja,* Problems and Examples in Differential Equations (1992)
165. *E. Hansen,* Global Optimization Using Interval Analysis (1992)
166. *S. Guerre-Delabrière,* Classical Sequences in Banach Spaces (1992)
167. *Y. C. Wong,* Introductory Theory of Topological Vector Spaces (1992)
168. *S. H. Kulkarni and B. V. Limaye,* Real Function Algebras (1992)
169. *W. C. Brown,* Matrices Over Commutative Rings (1993)
170. *J. Loustau and M. Dillon,* Linear Geometry with Computer Graphics (1993)
171. *W. V. Petryshyn,* Approximation-Solvability of Nonlinear Functional and Differential Equations (1993)

172. *E. C. Young*, Vector and Tensor Analysis: Second Edition (1993)
173. *T. A. Bick*, Elementary Boundary Value Problems (1993)
174. *M. Pavel*, Fundamentals of Pattern Recognition: Second Edition (1993)
175. *S. A. Albeverio et al.*, Noncommutative Distributions (1993)
176. *W. Fulks*, Complex Variables (1993)
177. *M. M. Rao*, Conditional Measures and Applications (1993)
178. *A. Janicki and A. Weron*, Simulation and Chaotic Behavior of α-Stable Stochastic Processes (1994)
179. *P. Neittaanmäki and D. Tiba*, Optimal Control of Nonlinear Parabolic Systems (1994)
180. *J. Cronin*, Differential Equations: Introduction and Qualitative Theory, Second Edition (1994)
181. *S. Heikkilä and V. Lakshmikantham*, Monotone Iterative Techniques for Discontinuous Nonlinear Differential Equations (1994)
182. *X. Mao*, Exponential Stability of Stochastic Differential Equations (1994)
183. *B. S. Thomson*, Symmetric Properties of Real Functions (1994)
184. *J. E. Rubio*, Optimization and Nonstandard Analysis (1994)
185. *J. L. Bueso et al.*, Compatibility, Stability, and Sheaves (1995)
186. *A. N. Michel and K. Wang*, Qualitative Theory of Dynamical Systems (1995)
187. *M. R. Damel*, Theory of Lattice-Ordered Groups (1995)
188. *Z. Naniewicz and P. D. Panagiotopoulos*, Mathematical Theory of Hemivariational Inequalities and Applications (1995)
189. *L. J. Corwin and R. H. Szczarba*, Calculus in Vector Spaces: Second Edition (1995)
190. *L. H. Erbe et al.*, Oscillation Theory for Functional Differential Equations (1995)
191. *S. Agaian et al.*, Binary Polynomial Transforms and Nonlinear Digital Filters (1995)
192. *M. I. Gil'*, Norm Estimations for Operation-Valued Functions and Applications (1995)
193. *P. A. Grillet*, Semigroups: An Introduction to the Structure Theory (1995)
194. *S. Kichenassamy*, Nonlinear Wave Equations (1996)
195. *V. F. Krotov*, Global Methods in Optimal Control Theory (1996)
196. *K. I. Beidar et al.*, Rings with Generalized Identities (1996)
197. *V. I. Arnautov et al.*, Introduction to the Theory of Topological Rings and Modules (1996)
198. *G. Sierksma*, Linear and Integer Programming (1996)
199. *R. Lasser*, Introduction to Fourier Series (1996)
200. *V. Sima*, Algorithms for Linear-Quadratic Optimization (1996)
201. *D. Redmond*, Number Theory (1996)
202. *J. K. Beem et al.*, Global Lorentzian Geometry: Second Edition (1996)
203. *M. Fontana et al.*, Prüfer Domains (1997)
204. *H. Tanabe*, Functional Analytic Methods for Partial Differential Equations (1997)
205. *C. Q. Zhang*, Integer Flows and Cycle Covers of Graphs (1997)
206. *E. Spiegel and C. J. O'Donnell*, Incidence Algebras (1997)
207. *B. Jakubczyk and W. Respondek*, Geometry of Feedback and Optimal Control (1998)
208. *T. W. Haynes et al.*, Fundamentals of Domination in Graphs (1998)
209. *T. W. Haynes et al.*, Domination in Graphs: Advanced Topics (1998)
210. *L. A. D'Alotto et al.*, A Unified Signal Algebra Approach to Two-Dimensional Parallel Digital Signal Processing (1998)
211. *F. Halter-Koch*, Ideal Systems (1998)
212. *N. K. Govil et al.*, Approximation Theory (1998)
213. *R. Cross*, Multivalued Linear Operators (1998)
214. *A. A. Martynyuk*, Stability by Liapunov's Matrix Function Method with Applications (1998)
215. *A. Favini and A. Yagi*, Degenerate Differential Equations in Banach Spaces (1999)
216. *A. Illanes and S. Nadler, Jr.*, Hyperspaces: Fundamentals and Recent Advances (1999)
217. *G. Kato and D. Struppa*, Fundamentals of Algebraic Microlocal Analysis (1999)
218. *G. X.-Z. Yuan*, KKM Theory and Applications in Nonlinear Analysis (1999)
219. *D. Motreanu and N. H. Pavel*, Tangency, Flow Invariance for Differential Equations, and Optimization Problems (1999)
220. *K. Hrbacek and T. Jech*, Introduction to Set Theory, Third Edition (1999)
221. *G. E. Kolosov*, Optimal Design of Control Systems (1999)
222. *N. L. Johnson*, Subplane Covered Nets (2000)
223. *B. Fine and G. Rosenberger*, Algebraic Generalizations of Discrete Groups (1999)
224. *M. Väth*, Volterra and Integral Equations of Vector Functions (2000)
225. *S. S. Miller and P. T. Mocanu*, Differential Subordinations (2000)

226. *R. Li et al.*, Generalized Difference Methods for Differential Equations: Numerical Analysis of Finite Volume Methods (2000)
227. *H. Li and F. Van Oystaeyen*, A Primer of Algebraic Geometry (2000)
228. *R. P. Agarwal*, Difference Equations and Inequalities: Theory, Methods, and Applications, Second Edition (2000)
229. *A. B. Kharazishvili*, Strange Functions in Real Analysis (2000)
230. *J. M. Appell et al.*, Partial Integral Operators and Integro-Differential Equations (2000)
231. *A. I. Prilepko et al.*, Methods for Solving Inverse Problems in Mathematical Physics (2000)
232. *F. Van Oystaeyen*, Algebraic Geometry for Associative Algebras (2000)
233. *D. L. Jagerman*, Difference Equations with Applications to Queues (2000)
234. *D. R. Hankerson et al.*, Coding Theory and Cryptography: The Essentials, Second Edition, Revised and Expanded (2000)
235. *S. Dăscălescu et al.*, Hopf Algebras: An Introduction (2001)
236. *R. Hagen et al.*, C^*-Algebras and Numerical Analysis (2001)
237. *Y. Talpaert*, Differential Geometry: With Applications to Mechanics and Physics (2001)

Additional Volumes in Preparation

HOPF ALGEBRAS

An Introduction

Sorin Dăscălescu
Constantin Năstăsescu
Şerban Raianu
University of Bucharest
Bucharest, Romania

MARCEL
DEKKER

MARCEL DEKKER, INC. NEW YORK • BASEL

Library of Congress Cataloging-in-Publication Data

Dascalescu, Sorin.
Hopf algebras : an introduction / Sorin Dascalescu, Constantin Nastasescu, Serban Raianu.
p. cm. – (Monographs and textbooks in pure and applied mathematics ; 235)
Includes index.
ISBN 0-8247-0481-9 (alk. paper)
1. Hopf algebras. I. Nastasescu, C. (Constantin). II. Raianu, Serban. III. Title.
IV. Series

QA613.8 .D37 2000
512'.55—dc21 00-059025

This book is printed on acid-free paper.

Headquarters
Marcel Dekker, Inc.
270 Madison Avenue, New York, NY 10016
tel: 212-696-9000; fax: 212-685-4540

Eastern Hemisphere Distribution
Marcel Dekker AG
Hutgasse 4, Postfach 812, CH-4001 Basel, Switzerland
tel: 41-61-261-8482; fax: 41-61-261-8896

World Wide Web
http://www.dekker.com

The publisher offers discounts on this book when ordered in bulk quantities. For more information, write to Special Sales/Professional Marketing at the headquarters address above.

Current printing (last digit)
10 9 8 7 6 5 4 3 2 1

PRINTED IN THE UNITED STATES OF AMERICA

Preface

A bialgebra is, roughly speaking, an algebra on which there exists a dual structure, called a coalgebra structure, such that the two structures satisfy a compatibility relation. A Hopf algebra is a bialgebra with an endomorphism satisfying a condition which can be expressed using the algebra and coalgebra structures.

The first example of such a structure was observed in algebraic topology by H. Hopf in 1941. This was the homology of a connected Lie group, which is even a graded Hopf algebra. Starting with the late 1960s, Hopf algebras became a subject of study from a strictly algebraic point of view, and by the end of the 1980s, research in this field was given a strong boost by the connections with quantum mechanics (the so-called quantum groups are in fact examples of noncommutative noncocommutative Hopf algebras).

Perhaps one of the most striking aspect of Hopf algebras is their extraordinary ubiquity in virtually all fields of mathematics: from number theory (formal groups), to algebraic geometry (affine group schemes), Lie theory (the universal enveloping algebra of a Lie algebra is a Hopf algebra), Galois theory and separable field extensions, graded ring theory, operator theory, locally compact group theory, distribution theory, combinatorics, representation theory and quantum mechanics, and the list may go on.

This text is mainly addressed to beginners in the field, graduate or even undergraduate students. The prerequisites are the notions usually contained in the first two year courses in algebra: some elements of linear algebra, tensor products, injective and projective modules. Some elementary notions of category theory are also required, such as equivalences of categories, adjoint functors, Morita equivalence, abelian and Grothendieck categories. The style of the exposition is mainly categorical.

The main subjects are the notions of a coalgebra and comodule over a coalgebra, together with the corresponding categories, the notion of a bialgebra and Hopf algebra, categories of Hopf modules, integrals, actions and coactions of Hopf algebras, some Hopf-Galois theory and some classification results for finite dimensional Hopf algebras. Special emphasis is put upon special classes of coalgebras, such as semiperfect, co-Frobenius, quasi-co-Frobenius, and cosemisimple or pointed coalgebras. Some torsion theory for coalgebras is also discussed. These classes of coalgebras are then investigated in the particular case of Hopf algebras, and the results are used, for example, in the chapters concerning integrals, actions and Galois extensions. The notions of a coalgebra and comodule are dualizations of the usual notions of an algebra and module. Beyond the formal aspect of dualization, it is worth keeping in mind that the introduction of these structures is motivated by natural constructions in classical fields of algebra, for example from representation theory. Thus, the notion of comultiplication in a coalgebra may be already seen in the definition of the tensor product of representations of groups or Lie algebras, and a comodule is, in the given context, just a linear representation of an affine group scheme.

As often happens, dual notions can behave quite differently in given dual situations. Coalgebras (and comodules) differ from their dual notions by a certain finiteness property they have. This can first be seen in the fact that the dual of a coalgebra is always an algebra in a functorial way, but not conversely. Then the same aspect becomes evident in the fundamental theorems for coalgebras and comodules. The practical result is that coalgebras and comodules are suitable for the study of cases involving infinite dimensions. This will be seen mainly in the chapter on actions and coactions.

The notion of an action of a Hopf algebra on an algebra unifies situations such as: actions of groups as automorphisms, rings graded by a group, and Lie algebras acting as derivations. The chapter on actions and coactions has as main application the characterization of Hopf-Galois extensions in the case of co-Frobenius Hopf algebras. We do not treat here the dual situation, namely actions and coactions on coalgebras.

Among other subjects which are not treated are: generalizations of Hopf modules, such as Doi-Koppinen modules or entwining modules, quasitriangular Hopf algebras and solutions of the quantum Yang-Baxter equation, and braided categories.

The last chapter contains some fundamental theorems on finite dimensional Hopf algebras, such as the Nichols-Zoeller theorem, the Taft-Wilson theorem, and the Kac-Zhu theorem.

We tried to keep the text as self-contained as possible. In the exposition we have indulged our taste for the language of category theory, and we use this language quite freely. A sort of "phrase-book" for this language is included in an appendix. Exercises are scattered throughout the text, with complete solutions at the end of each chapter. Some of them are very easy, and some of them not, but the reader is encouraged to try as hard as possible to solve them without looking at the solution. Some of the easier results can also be treated as exercises, and proved independently after a quick glimpse at the solution. We also tried to explain why the names for some notions sound so familar (e.g. convolution, integral, Galois extension, trace).

This book is not meant to supplant the existing monographs on the subject, such as the books of M. Sweedler [218], E. Abe [1], or S. Montgomery [149] (which were actually our main source of inspiration), but rather as a first contact with the field. Since references in the text are few, we include a bibliographical note at the end of each chapter.

It is usually difficult to thank people who helped without unwittingly leaving some out, but we shall try. So we thank our friends Nicolás Andruskiewitsch, Margaret Beattie, Stefaan Caenepeel, Bill Chin, Miriam Cohen (who sort of founded the Hopf algebra group in Bucharest with her talk in 1989), Yukio Doi, José Gomez Torrecillas, Luzius Grünenfelder, Andrei Kelarev, Akira Masuoka, Claudia Menini, Susan Montgomery, Declan Quinn, David Radford, Angel del Río, Manolo Saorín, Peter Schauenburg, Hans-Jürgen Schneider, Blas Torrecillas, Fred Van Oystaeyen, Leon Van Wyk, Sara Westreich, Robert Wisbauer, Yinhuo Zhang, our students and colleagues from the University of Bucharest, for the many things that we have learned from them. Florin Nichita and Alexandru Stănculescu took course notes for part of the text, and corrected many errors. Special thanks go to the editor of this series, Earl J. Taft, for encouraging us (and making us write this material). Finally, we thank our families, especially our wives, Crina, Petruţa and Andreea, for loving and understanding care during the preparation of the book.

Sorin Dăscălescu, Constantin Năstăsescu, Şerban Raianu

Contents

Chapter 1

Algebras and coalgebras

1.1 Basic concepts

Let k be a field. All unadorned tensor products are over k. The following alternative definition for the classical notion of a k-algebra sheds a new light on this concept, the ingredients of the new definition being objects (vector spaces), morphisms (linear maps), tensor products and commutative diagrams.

Definition 1.1.1 *A* k-algebra *is a triple* (A, M, u), *where* A *is a* k*-vector space,* $M : A \otimes A \longrightarrow A$ *and* $u : k \longrightarrow A$ *are morphisms of* k*-vector spaces such that the following diagrams are commutative:*

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{I \otimes M} & A \otimes A \\ {\scriptstyle M \otimes I}\downarrow & & \downarrow{\scriptstyle M} \\ A \otimes A & \xrightarrow{M} & A \end{array}$$

$$\begin{tikzcd}
 & A \otimes A \arrow[dd, "M"] & \\
k \otimes A \arrow[ur, "u \otimes I"] \arrow[dr, "\sim"'] & & A \otimes k \arrow[ul, "I \otimes u"'] \arrow[dl, "\sim"] \\
 & A &
\end{tikzcd}$$

We have denoted by I the identity map of A, and the unnamed arrows from the second diagram are the canonical isomorphisms. (In general we will denote by I (unadorned, if there is no danger of confusion, the identity map of a set, but sometimes also by Id.) ∎

Remark 1.1.2 *The definition is equivalent to the classical one, requiring A to be a unitary ring, and the existence of a unitary ring morphism $\phi : k \longrightarrow A$, with $Im\ \phi \subseteq Z(A)$. Indeed, the multiplication $a \cdot b = M(a \otimes b)$ defines on A a structure of unitary ring, with identity element $u(1)$; the role of ϕ is played by u itself. For the converse, we put $M(a \otimes b) = a \cdot b$ and $u = \phi$.*
Due to the above, the map M is called the multiplication of the algebra A, and u is called its unit. The commutativity of the first diagram in the definition is just the associativity of the multiplication of the algebra. ∎

The importance of the above definition resides in the fact that, due to its categorical nature, it can be dualized. We obtain in this way the notion of a *coalgebra.*

Definition 1.1.3 *A k-*coalgebra *is a triple (C, Δ, ε), where C is a k-vector space, $\Delta : C \longrightarrow C \otimes C$ and $\varepsilon : C \longrightarrow k$ are morphisms of k-vector spaces such that the following diagrams are commutative:*

$$\begin{tikzcd}
C \arrow[r, "\Delta"] \arrow[d, "\Delta"'] & C \otimes C \arrow[d, "I \otimes \Delta"] \\
C \otimes C \arrow[r, "\Delta \otimes I"] & C \otimes C \otimes C
\end{tikzcd}$$

$$
\begin{tikzcd}
& C \arrow[dl, "\sim"'] \arrow[dr, "\sim"] \arrow[dd, "\Delta"] & \\
k \otimes C & & C \otimes k \\
& C \otimes C \arrow[ul, "\varepsilon \otimes I"] \arrow[ur, "I \otimes \varepsilon"'] &
\end{tikzcd}
$$

The maps Δ *and* ε *are called* the comultiplication, *and* the counit, *respectively, of the coalgebra* C. *The commutativity of the first diagram is called* coassociativity. ∎

Example 1.1.4 *1) Let* S *be a nonempty set;* kS *is the* k*-vector space with basis* S. *Then* kS *is a coalgebra with comultiplication* Δ *and counit* ε *defined by* $\Delta(s) = s \otimes s$, $\varepsilon(s) = 1$ *for any* $s \in S$. *This shows that any vector space can be endowed with a* k*-coalgebra structure.*
2) Let H *be a* k*-vector space with basis* $\{c_m \mid m \in \mathbf{N}\}$. *Then* H *is a coalgebra with comultiplication* Δ *and counit* ε *defined by*

$$\Delta(c_m) = \sum_{i=0,m} c_i \otimes c_{m-i}, \quad \varepsilon(c_m) = \delta_{0,m}$$

for any $m \in \mathbf{N}$ *(*δ_{ij} *will denote throughout the Kronecker symbol). This coalgebra is called the divided power coalgebra, and we will come back to it later.*
3) Let $(S, \leq)$ *be a partially ordered locally finite set (i.e. for any* $x, y \in S$, *with* $x \leq y$, *the set* $\{z \in S \mid x \leq z \leq y\}$ *is finite). Let* $T = \{(x,y) \in S \times S \mid x \leq y\}$ *and* V k*-vector space with basis* T. *Then* V *is a coalgebra with*

$$\Delta(x,y) = \sum_{x \leq z \leq y} (x,z) \otimes (z,y)$$

$$\varepsilon(x,y) = \delta_{x,y}$$

for any $(x,y) \in T$.
4) The field k *is a* k*-coalgebra with comultiplication* $\Delta : k \to k \otimes k$ *the canonical isomorphism,* $\Delta(\alpha) = \alpha \otimes 1$ *for any* $\alpha \in k$, *and the counit* $\varepsilon : k \to k$ *the identity map. We remark that this coalgebra is a particular case of the example in 1), for* S *a set with only one element.*
5) Let $n \geq 1$ *be a positive integer, and* $M^c(n,k)$ *a* k*-vector space of dimension* n^2. *We denote by* $(e_{ij})_{1 \leq i,j \leq n}$ *a basis of* $M^c(n,k)$. *We define on* $M^c(n,k)$ *a comultiplication* Δ *by*

$$\Delta(e_{ij}) = \sum_{1 \leq p \leq n} e_{ip} \otimes e_{pj}$$

for any i, j, and a counit ε by

$$\varepsilon(e_{ij}) = \delta_{ij}$$

In this way, $M^c(n, k)$ becomes a coalgebra, which is called the matrix coalgebra.
6) Let C be a vector space with basis $\{ g_i, d_i \mid i \in \mathbf{N}^* \}$. We define $\Delta : C \to C \otimes C$ and $\varepsilon : C \to k$ by

$$\begin{aligned} \Delta(g_i) &= g_i \otimes g_i \\ \Delta(d_i) &= g_i \otimes d_i + d_i \otimes g_{i+1} \\ \varepsilon(g_i) &= 1 \\ \varepsilon(d_i) &= 0 \end{aligned}$$

Then (C, Δ, ε) is a coalgebra. ∎

The following exercise deals with a coalgebra called the trigonometric coalgebra. The reason for the name, as well as what really makes it a coalgebra, will be discussed later, after the introduction of the representative coalgebra of a semigroup (the same applies to the divided power coalgebra in the second example above).

Exercise 1.1.5 *Let C be a k-space with basis $\{s, c\}$. We define $\Delta : C \to C \otimes C$ and $\varepsilon : C \to k$ by*

$$\begin{aligned} \Delta(s) &= s \otimes c + c \otimes s \\ \Delta(c) &= c \otimes c - s \otimes s \\ \varepsilon(s) &= 0 \\ \varepsilon(c) &= 1. \end{aligned}$$

Show that (C, Δ, ε) is a coalgebra.

Exercise 1.1.6 *Show that on any vector space V one can introduce an algebra structure.*

Let (C, Δ, ε) be a coalgebra. We recurrently define the sequence of maps $(\Delta_n)_{n \geq 1}$, as follows:

$$\Delta_1 = \Delta, \quad \Delta_n : C \longrightarrow C \otimes \ldots \otimes C \quad (C \text{ appearing } n+1 \text{ times })$$

$$\Delta_n = (\Delta \otimes I^{n-1}) \circ \Delta_{n-1}, \quad \text{for any } n \geq 2.$$

(Throughout the text, the composition of the maps f and g will be denoted by $f \circ g$, or simply fg when there is no danger of confusion.)
As we know, in an algebra we have a property called generalized associativity. The dual property in the case of coalgebras is called generalized coassociativity, and is given in the following proposition.

Proposition 1.1.7 *Let (C,Δ,ε) be a coalgebra. Then for any $n \geq 2$ and any $p \in \{0,\ldots,n-1\}$ the following equality holds*

$$\Delta_n = (I^p \otimes \Delta \otimes I^{n-1-p}) \circ \Delta_{n-1}.$$

Proof: We show by induction on n that the equality holds for any $p \in \{0,\ldots,n-1\}$. For $n=2$ we have to show that $(\Delta \otimes I) \circ \Delta = (I \otimes \Delta) \circ \Delta$, which is the coassociativity of the comultiplication.
We assume that the relation holds for n. Let then $p \in \{1,\ldots,n\}$. We have

$$\begin{aligned}
& (I^p \otimes \Delta \otimes I^{n-p}) \circ \Delta_n = \\
= \ & (I^p \otimes \Delta \otimes I^{n-p}) \circ (I^{p-1} \otimes \Delta \otimes I^{n-p}) \circ \Delta_{n-1} \\
= \ & (I^{p-1} \otimes ((I \otimes \Delta) \circ \Delta) \otimes I^{n-p}) \circ \Delta_{n-1} \\
= \ & (I^{p-1} \otimes ((\Delta \otimes I) \circ \Delta) \otimes I^{n-p}) \circ \Delta_{n-1} \\
= \ & (I^{p-1} \otimes \Delta \otimes I^{n+1-p}) \circ (I^{p-1} \otimes \Delta \otimes I^{n-p}) \circ \Delta_{n-1} \\
= \ & (I^{p-1} \otimes \Delta \otimes I^{n-p+1}) \circ \Delta_n
\end{aligned}$$

Since for $p=0$ we have by definition that $\Delta_{n+1} = (I^p \otimes \Delta \otimes I^{n-p}) \circ \Delta_n$, by the above relation it follows, by induction on p, that the equality holds for any $p \in \{0,\ldots,n\}$. ∎

Unlike the case of algebras, where the multiplication "diminishes" the number of elements, from two elements obtaining only one after applying the multiplication, in a coalgebra, the comultiplication produces an opposite effect, from one element obtaining by comultiplication a finite family of pairs of elements. Due to this fact, computations in a coalgebra are harder than the ones in an algebra. The following notation for the comultiplication, usually called the "Sweedler notation", but also known as the "Heyneman-Sweedler notation", proved itself to be very effective.

1.1.8 The Sigma Notation. *Let (C,Δ,ε) be a coalgebra. For an element $c \in C$ we denote*

$$\Delta(c) = \sum c_1 \otimes c_2.$$

With the usual summation conventions we should have written

$$\Delta(c) = \sum_{i=1,n} c_{i1} \otimes c_{i2}.$$

The sigma notation supresses the index "i". It is a way to emphasize the form of $\Delta(c)$, and it is very useful for writing long compositions involving the comultiplication in a compressed way.
In a similar way, for any $n \geq 1$ we write

$$\Delta_n(c) = \sum c_1 \otimes \ldots \otimes c_{n+1}.$$

∎

The above notation provides an easy way for writing commutative diagrams, the first examples being the diagrams in the definition of a coalgebra, i.e. the coassociativity and the counit property:

1.1.9 Formulas. *Let (C, Δ, ε) be a coalgebra and $c \in C$. Then:*

$$\Delta_2(c) = \sum \Delta(c_1) \otimes c_2 = \sum c_1 \otimes \Delta(c_2) = \sum c_1 \otimes c_2 \otimes c_3$$

$$(\text{or } \Delta_2(c) = \sum c_{1_1} \otimes c_{1_2} \otimes c_2 = \sum c_1 \otimes c_{2_1} \otimes c_{2_2} = \sum c_1 \otimes c_2 \otimes c_3).$$

Note that

$$\sum c_{1_1} \otimes c_{1_2} \otimes c_2 = \sum c_1 \otimes c_{2_1} \otimes c_{2_2},$$

$\forall c \in C$ is just the equality $(\Delta \otimes I) \circ \Delta = (I \otimes \Delta) \circ \Delta$, the commutativity of the first diagram in Definition 1.1.3. The commutativity of the second diagram in the same definition may be written as

$$Id_C = \phi_l \circ (\varepsilon \otimes I) \circ \Delta = \phi_r \circ (I \otimes \varepsilon) \circ \Delta,$$

where $\phi_r : C \otimes k \xrightarrow{\sim} C$ and $\phi_l : k \otimes C \xrightarrow{\sim} C$ are the canonical isomorphisms. Using the sigma notation, the same equalities are written as

$$\sum \varepsilon(c_1)c_2 = \sum c_1\varepsilon(c_2) = c.$$

The advantage of using the sigma notation will become clear later, when we will deal with very complicated commutative diagrams or very long compositions. ∎

We are going to explain now how to operate with the sigma notation. For this we will need some more formulas.

Lemma 1.1.10 *Let (C, Δ, ε) be a coalgebra. Then:*
1) For any $i \geq 2$ we have $\Delta_i = (\Delta_{i-1} \otimes I) \circ \Delta$.
2) For any $n \geq 2$, $i \in \{1, \ldots, n-1\}$ and $m \in \{0, \ldots, n-i\}$ we have

$$\Delta_n = (I^m \otimes \Delta_i \otimes I^{n-i-m}) \circ \Delta_{n-i}.$$

Proof: 1) By induction on i. For $i = 2$ this is the definition of Δ_2. We assume that the assertion is true for i, and then

$$\begin{aligned}
\Delta_{i+1} &= (\Delta \otimes I^i) \circ \Delta_i \\
&= (\Delta \otimes I^i) \circ (\Delta_{i-1} \otimes I) \circ \Delta \\
&= (((\Delta \otimes I^{i-1}) \circ \Delta_{i-1}) \otimes I) \circ \Delta \\
&= (\Delta_i \otimes I) \circ \Delta.
\end{aligned}$$

2) We fix $n \geq 2$, and we prove by induction on $i \in \{1, \ldots, n-1\}$ that for any $m \in \{0, \ldots, n-i\}$ the required relation holds.
For $i = 1$ this is the generalized coassociativity proved in Proposition 1.1.7. We assume the assertion is true for $i-1$ ($i \geq 2$) and we prove it for i. We pick $m \in \{0, \ldots, n-i\} \subset \{0, \ldots, n-i+1\}$ and we have

$$\begin{aligned}
\Delta_n &= (I^m \otimes \Delta_{i-1} \otimes I^{n-i-m+1}) \circ \Delta_{n-i+1} \\
&\qquad\qquad \text{(by the induction hypothesis)} \\
&= (I^m \otimes \Delta_{i-1} \otimes I^{n-i-m+1}) \circ (I^m \otimes \Delta \otimes I^{n-i-m}) \circ \Delta_{n-i} \\
&\qquad\qquad \text{(by generalized coassociativity)} \\
&= (I^m \otimes ((\Delta_{i-1} \otimes I) \circ \Delta) \otimes I^{n-i-m}) \circ \Delta_{n-i} \\
&= (I^m \otimes \Delta_i \otimes I^{n-i-m}) \circ \Delta_{n-i} \\
&\qquad\qquad \text{(using 1))}
\end{aligned}$$

∎

These formulas allow us to give the following computation rule, which is essential for computations in colagebras, and which will be used throughout in the sequel.

1.1.11 Computation rule. *Let (C, Δ, ε) be a coalgebra, $i \geq 1$,*

$$f : C \otimes \ldots \otimes C \longrightarrow C$$

(in the preceding tensor product C appearing $i+1$ times) and

$$\overline{f} : C \longrightarrow C$$

linear maps such that $f \circ \Delta_i = \overline{f}$.
Then, if $n \geq i$, V is a k-vector space, and

$$g : C \otimes \ldots \otimes C \longrightarrow V$$

(here C appearing $n+1$ times in the tensor product) is a k-linear map, for any $1 \leq j \leq n+1$ and $c \in C$ we have

$$\sum g(c_1 \otimes \ldots \otimes c_{j-1} \otimes f(c_j \otimes \ldots \otimes c_{j+i}) \otimes c_{j+i+1} \otimes \ldots \otimes c_{n+i+1}) =$$

$$= \sum g(c_1 \otimes \ldots \otimes c_{j-1} \otimes \overline{f}(c_j) \otimes c_{j+1} \otimes \ldots \otimes c_{n+1})$$

This happens because

$$\sum g(c_1 \otimes \ldots \otimes c_{j-1} \otimes f(c_j \otimes \ldots \otimes c_{j+i}) \otimes$$

$$\begin{aligned}
&\otimes c_{j+i+1} \otimes \ldots \otimes c_{n+i+1}) = \\
= \;& g \circ (I^{j-1} \otimes f \otimes I^{n-j+1}) \circ \Delta_{n+i}(c) \\
= \;& g \circ (I^{j-1} \otimes f \otimes I^{n-j+1}) \circ (I^{j-1} \otimes \Delta_i \otimes I^{n-j+1}) \circ \Delta_n(c) \\
= \;& g \circ (I^{j-1} \otimes (f \circ \Delta_i) \otimes I^{n-j+1}) \circ \Delta_n(c) \\
= \;& g \circ (I^{j-1} \otimes \overline{f} \otimes I^{n-j+1}) \circ \Delta_n(c) \\
= \;& \sum g(c_1 \otimes \ldots \otimes c_{j-1} \otimes \overline{f}(c_j) \otimes c_{j+1} \otimes \ldots \otimes c_{n+1})
\end{aligned}$$

This rule may be formulated as follows: if we have a formula (*) in which an expression in $c_1, \ldots, c_{i+1}$ *(from* $\Delta_i(c)$*) has as result an element in* C *(*$f \circ \Delta_i = \overline{f}$*), then in an expression depending on* $c_1, \ldots, c_{n+i+1}$ *(from* $\Delta_{n+i}(c)$*) in which the expression in the formula (*) appears for* $c_j, \ldots, c_{j+i}$ *(*$i+1$ *consecutive positions), we can replace the expression depending on* $c_j, \ldots, c_{j+i}$ *by* $\overline{f}(c_j)$*, leaving unchanged* $c_1, \ldots, c_{j-1}$ *and transforming* $c_{j+i+1}, \ldots, c_{n+i+1}$ *in* $c_{j+1}, \ldots, c_{n+1}$. ∎

Example 1.1.12 *If* (C, Δ, ε) *is a coalgebra, then for any* $c \in C$ *we have*

$$\sum \varepsilon(c_1)\varepsilon(c_2)c_3 = c.$$

This is because having in mind the formula $\sum \varepsilon(c_1)c_2 = c$*, we can replace in the left hand side* $\varepsilon(c_2)c_3$ *by* c_2*, leaving* c_1 *unchanged. Therefore,* $\sum \varepsilon(c_1)\varepsilon(c_2)c_3 = \sum \varepsilon(c_1)c_2$*, and this is exactly* c. ∎

We end this section by giving some definitions allowing the introduction of some categories.

Definition 1.1.13 *An algebra* (A, M, u) *is said to be* commutative *if the diagram*

$$\begin{tikzcd}
A \otimes A \arrow[rr, "T"] \arrow[dr, "M"'] & & A \otimes A \arrow[dl, "M"] \\
& A &
\end{tikzcd}$$

is commutative, where $T : A \otimes A \longrightarrow A \otimes A$ *is the twist map, defined by* $T(a \otimes b) = b \otimes a$.
ii) A coalgebra (C, Δ, ε) *is called* cocommutative *if the diagram*

$$\begin{tikzcd} & C \arrow[dl, "\Delta"'] \arrow[dr, "\Delta"] & \\ C \otimes C \arrow[rr, "T"'] & & C \otimes C \end{tikzcd}$$

is commutative, which may be written as $\sum c_1 \otimes c_2 = \sum c_2 \otimes c_1$ *for any* $c \in C$. ∎

Definition 1.1.14 *Let* (A, M_A, u_A), (B, M_B, u_B) *be two* k*-algebras. The* k*-linear map* $f : A \longrightarrow B$ *is a morphism of algebras if the following diagrams are commutative*

$$\begin{tikzcd} A \otimes A \arrow[r, "f \otimes f"] \arrow[d, "M_A"'] & B \otimes B \arrow[d, "M_B"] \\ A \arrow[r, "f"] & B \end{tikzcd} \qquad \begin{tikzcd} A \arrow[rr, "f"] & & B \\ & k \arrow[ul, "u_A"] \arrow[ur, "u_B"'] & \end{tikzcd}$$

ii) Let $(C, \Delta_C, \varepsilon_C)$, $(D, \Delta_D, \varepsilon_D)$ *be two* k*-coalgebras. The* k*-linear map* $g : C \longrightarrow D$ *is a morphism of coalgebras if the following diagrams are commutative*

$$\begin{tikzcd} C \arrow[r, "g"] \arrow[d, "\Delta_C"'] & D \arrow[d, "\Delta_D"] \\ C \otimes C \arrow[r, "g \otimes g"] & D \otimes D \end{tikzcd} \qquad \begin{tikzcd} C \arrow[rr, "g"] \arrow[dr, "\varepsilon_C"'] & & D \arrow[dl, "\varepsilon_D"] \\ & k & \end{tikzcd}$$

The commutativity of the first diagram may be written in the sigma notation as:

$$\Delta_D(g(c)) = \sum g(c)_1 \otimes g(c)_2 = \sum g(c_1) \otimes g(c_2).$$

∎

In this way we can define the categories $k - Alg$ and $k - Cog$, in which the objects are the k-algebras, respectively the k-coalgebras, and the morphisms are the ones previously defined.

Exercise 1.1.15 *Show that in the category $k - Cog$, isomorphisms (i.e. morphisms of coalgebras having an inverse which is also a coalgebra morphism) are precisely the bijective morphisms.*

1.2 The finite topology

Let X and Y be non-empty sets and Y^X the set of all mappings from X to Y. It is clear that we can regard Y^X as the product of the sets $Y_x = Y$, where x ranges over the index set X. The *finite topology* of Y^X is obtained by taking the product space in the category of topological spaces, where each Y_x is regarded as a discrete space. A basis for the open sets in this topology is given by the sets of the form

$$\{g \in Y^X \mid g(x_i) = f(x_i), 1 \leq i \leq n\},$$

where $\{x_i \mid 1 \leq i \leq n\}$ is a finite set of elements of X, and f is a fixed element of Y^X, so that every open set is a union of open sets of this form.

Assume now that k is a field, and X and Y are two k-vector spaces. The set $Hom_k(X, Y)$ of all k-homomorphisms from X to Y, which is also a k-vector space, is a subset of Y^X. Thus we can consider on $Hom_k(X, Y)$ the topology induced by the finite topology on Y^X. This topology on $Hom_k(X, Y)$ is also called the *finite topology*.

If $f \in Hom_k(X, Y)$, the the sets

$$\mathcal{O}(f, x_1, \ldots, x_n) = \{g \in Hom_k(X, Y) \mid g(x_i) = f(x_i), 1 \leq i \leq n\}$$

form a basis for the filter of neighbourhoods of f, where $\{x_i \mid 1 \leq i \leq n\}$ ranges over the finite subsets of X. Note that $\mathcal{O}(f, x_1, \ldots, x_n) = \bigcap_{i=1}^{n} \mathcal{O}(f, x_i)$, and $\mathcal{O}(f, x_1, \ldots, x_n) = f + \mathcal{O}(0, x_1, \ldots, x_n)$.

Proposition 1.2.1 *With the above notation we have the following results.*
a) $Hom_k(X, Y)$ is a closed subspace of Y^X (in the finite topology).
b) $Hom_k(X, Y)$, with the finite topology, is a topological k-vector space (the topology of k is the discrete topology).
c) If $dim_k(X) < \infty$, then the finite topology on $Hom_k(X, Y)$ is discrete.

Proof: a) Pick f in the closure of $Hom_k(X, Y)$, and let $x_1, x_2 \in X$, and $\lambda, \mu \in k$. The open set $U = \{g \in Y^X \mid g(x_1) = f(x_1), g(x_2) = f(x_2), g(\lambda x_1 + \mu x_2) = f(\lambda x_1 + \mu x_2)\}$ is a neighbourhood of f, and therefore

$U \bigcap Hom_k(X,Y) \neq \emptyset$. If $h \in U \bigcap Hom_k(X,Y)$, then $h(x_1) = f(x_1)$, $h(x_2) = f(x_2)$, and $h(\lambda x_1 + \mu x_2) = f(\lambda x_1 + \mu x_2)$. Since $h(\lambda x_1 + \mu x_2) = \lambda h(x_1) + \mu h(x_2) = \lambda f(x_1) + \mu f(x_2)$, we obtain that $f(\lambda x_1 + \mu x_2) = \lambda f(x_1) + \mu f(x_2)$, so $f \in Hom_k(X,Y)$.
b) If $\lambda, \mu \in k$, we have to show that the map $\alpha : (f,g) \longmapsto \lambda f + \mu g$ is a continuous mapping from the product space $Hom_k(X,Y) \times Hom_k(X,Y)$ into $Hom_k(X,Y)$. Indeed, we can consider the open neighbourhoods of $\lambda f + \mu g$ of the form $N = \lambda f + \mu g + \mathcal{O}(0, x_1, \ldots, x_n)$. If we put $N_1 = f + \mathcal{O}(0, x_1, \ldots, x_n)$ and $N_2 = g + \mathcal{O}(0, x_1, \ldots, x_n)$, then N_1 (resp. N_2) is a neighbourhood of f (resp. g). Since $\mathcal{O}(0, x_1, \ldots, x_n)$ is a k-subspace, it is clear that $\alpha(N_1 \times N_2) \subseteq N$, so α is continuous.
c) is obvious.

Exercise 1.2.2 *An open subspace in a topological vector space is also closed.*

If k is a field, we can consider the particular case when $X = V$ is a k-vector space, and $Y = k$. In this case, the vector space $Hom_k(V, k)$ is the dual V^*. We introduce now some notation. If S is a subset of V^*, then we denote

$$S^\perp = \{x \in V \mid u(x) = 0, \forall u \in S\} = \bigcap_{u \in S} Ker(u).$$

Similarly, if S is a subset of V, then we set

$$S^\perp = \{u \in V^* \mid u(S) = 0\} = \{u \in V^* \mid S \subseteq Ker(u)\}.$$

If $S = \{u\}$ (where $u \in V$ or $u \in V^*$), we denote $S^\perp = u^\perp$.

Exercise 1.2.3 *When S is a subset of V^* (or V), $S^\perp$ is a subspace of V (or V^*). In fact $S^\perp = \langle S \rangle^\perp$, where $\langle S \rangle$ is the subspace spanned by S. Moreover, we have $S^\perp = ((S^\perp)^\perp)^\perp$, for any subset S of V^* (or V).*

Exercise 1.2.4 *The set of all $f + W^\perp$, where W ranges over the finite dimensional subspaces of V, form a basis for the filter of neighbourhoods of $f \in V^*$ in the finite topology.*

The following result is the key fact in the study of the finite topology in V^*.

Proposition 1.2.5 *i) If S is a subspace of V^* and $\{e_1, \ldots, e_n\}$ is a finite subset of V, then*

$$S^\perp + \sum_{i=1}^{n} k e_i = (S \cap \bigcap_{i=1}^{n} e_i^\perp)^\perp.$$

ii) (the dual version of i)) If S is a k-linear subspace of V and $\{u_1, \dots, u_n\}$ is a finite subset of V^*, then

$$S^\perp + \sum_{i=1}^{n} ku_i = (S \cap \bigcap_{i=1}^{n} u_i^\perp)^\perp.$$

Proof: i) The inclusion

$$S^\perp + \sum_{i=1}^{n} ke_i \subseteq (S \cap \bigcap_{i=1}^{n} e_i^\perp)^\perp.$$

is clear. We show the converse inclusion by induction on n. Let $n = 1$ and denote in this case e_1 by e. Let $x \in (S \cap e^\perp)^\perp$. If $S \cap e^\perp = S$, then $x \in S^\perp$ and so $x \in S^\perp + ke$. Hence we can assume that $S \cap e^\perp \subset S$, $S \cap e^\perp \neq S$. Since $V^*/e^\perp \simeq (ke)^*$, and $(ke)^*$ has dimension one, it follows that $S/(S \cap e^\perp)$ is also 1-dimensional. Hence $S = (S \cap e^\perp) \oplus ku$, for some $u \in V^*$, with $u \in S$ and $u \notin S \cap e^\perp$. So $u \notin e^\perp$, and therefore $u(e) \neq 0$. We put $\lambda = u(x)u(e)^{-1}$. If $y = x - \lambda e$, then for any $v \in S$ we have $v(y) = v(x) - \lambda v(e)$. But $v = w + au$, where $w \in S \cap e^\perp$. So $v(x) = w(x) + au(x) = au(x)$. On the other hand, $\lambda v(e) = \lambda w(e) + \lambda au(e) = \lambda au(e) = au(x)u(e)^{-1}u(e) = au(x)$. Hence $v(y) = au(x) - au(x) = 0$, and since $v \in S$ is arbitrary, we obtain that $y \in S^\perp$. Thus $x = y + \lambda e \in S^\perp + ke$.

Assume that the assertion is true for $n-1$ $(n > 1)$. We have $S^\perp + \sum\limits_{i=1}^{n} ke_i = S^\perp + \sum\limits_{i=1}^{n-1} ke_i + ke_n = (S \cap \bigcap\limits_{i=1}^{n-1} e_i^\perp)^\perp + ke_n = (S \cap \bigcap\limits_{i=1}^{n} e_i^\perp \cap e_n^\perp)^\perp = (S \cap \bigcap\limits_{i=1}^{n} e_i^\perp)^\perp$.

ii) Since the proof is similar to the one of assertion i), we only sketch the case $n = 1$. We put $u = u_1$. We clearly have $S^\perp + ku \subseteq (S \cap u^\perp)^\perp$. For the reverse inclusion, we can assume $S \cap u^\perp \neq S$. Clearly in this case we have $u \neq 0$. Since $u^\perp = Ker(u)$, we have that $V/u^\perp = V/Ker(u)$ has dimension one. So $S/(S \cap u^\perp) \simeq (S + u^\perp)/u^\perp \leq V/u^\perp$ also has dimension one. There exists $e \in S$, $e \notin S \cap u^\perp$, such that $S = (S \cap u^\perp) \oplus ke$. So $u(e) \neq 0$. If now $f \in (S \cap u^\perp)^\perp$, we put $g = f - f(e)u(e)^{-1}u$. If $x \in S$, then $x = y + \lambda e$, with $y \in S \cap u^\perp$. But $f(x) = f(y) + \lambda f(e) = \lambda f(e)$, and $(f(e)u(e)^{-1}u)(x) = f(e)u(e)^{-1}u(y) + \lambda f(e)u(e)^{-1}u(e) = \lambda f(e)$. So $g(x) = \lambda f(e) - \lambda f(e) = 0$, and therefore $g \in S^\perp$. Since $f = g + f(e)u(e)^{-1}u$, we obtain $f \in S^\perp + ku$.

Theorem 1.2.6 *i) If S is subspace of V, then $(S^\perp)^\perp = S$.*
ii) If S is a subspace of V^*, then $(S^\perp)^\perp = \overline{S}$, where $\overline{S}$ is the closure of S in the finite topology.

Proof: i) We have clearly that $S \subseteq (S^\perp)^\perp$. Assume now that there exists $x \in (S^\perp)^\perp$, $x \notin S$. Since S is a subspace, then $kx \cap S = 0$. Thus there

exists $f \in V^*$ such that $f(x) = 1$ and $f(S) = 0$. But $f \in S^\perp$, and since $x \in (S^\perp)^\perp$, we have $f(x) = 0$, a contradiction. Hence $(S^\perp)^\perp = S$.
ii) $S^\perp$ is a subspace of V. Hence $(S^\perp)^\perp = \cap W^\perp$, where W ranges over the finite dimensional subspaces of $S^\perp$. Since $W^\perp$ is an open subspace of V^*, it follows that $W^\perp$ is also closed (see Exercise 1.2.2). Hence $\cap W^\perp$ is closed, so $(S^\perp)^\perp$ is closed in the finite topology (see also Exercise 1.2.7 below). Since $S \subseteq (S^\perp)^\perp$, it follows that $\overline{S} \subseteq (S^\perp)^\perp$. Let $f \in (S^\perp)^\perp$ and $W \subset V$ a k-subspace of finite dimension. We show that $(f + W^\perp) \cap S \neq \emptyset$. Clearly if $f \in W^\perp$ then $f + W^\perp = W^\perp$ (because $W^\perp$ is a subspace), and therefore $(f + W^\perp) \cap S = W^\perp \cap S \neq \emptyset$ (because it contains the zero morphism). Also if $W \subseteq S^\perp$, then $(S^\perp)^\perp \subseteq W^\perp$, and therefore $f \in W^\perp$. Hence we can assume that $f \notin W^\perp$ and so it follows that $W \not\subset S^\perp$. Thus we can write $W = (W \cap S^\perp) \oplus W'$, where $W' \neq 0$ and $dim_k(W') < \infty$. Also since $f(S^\perp) = 0$ and $f(W) \neq 0$ it follows that $f(W') \neq 0$. Let $\{e_1, \ldots, e_n\}$ $(n \geq 1)$ be a basis for W'. We denote by $a_i = f(e_i)$ $(1 \leq i \leq n)$, hence not all the a_i's are zero. By Proposition 1.2.5 i), we have

$$S^\perp \oplus \sum_{j \neq i} k e_j = (S \cap \bigcap_{j \neq i} e_j^\perp)^\perp.$$

Since $e_i \notin S^\perp \oplus \sum_{j \neq i} k e_j$, then $e_i \notin (S \cap \bigcap_{j \neq i} e_j^\perp)^\perp$. Hence there exists $g_i \in S \cap \bigcap_{j \neq i} e_j^\perp$ such that $g_i(e_i) = 1$. So we have $g_i \in S$, and $g_i(e_k) = \delta_{ik}$. We denote by $g = \sum_{i=1}^{n} a_i g_i$. Hence $g \in S$ and $g(e_k) = a_k$ $(1 \leq k \leq n)$.
Let now $h = g - f$. Clearly $h(e_i) = 0$ $(1 \leq i \leq n)$, and hence $h(W') = 0$. Since $h \in (S^\perp)^\perp$, then $h(S^\perp) = 0$, and thus $h(W \cap S^\perp) = 0$. So $h(W) = 0$, and hence $h \in W^\perp$. In conclusion, $g \in S \cap (f + W^\perp)$, and therefore $f \in \overline{S}$.

Exercise 1.2.7 *If S is a subspace of V^*, then prove that $(S^\perp)^\perp$ is closed in the finite topology by showing that its complement is open.*

We give now some consequences of Theorem 1.2.6.

Corollary 1.2.8 *There exists a bijective correspondence between the subspaces of V and the closed subspaces of V^*, given by $S \longmapsto S^\perp$.* ∎

Corollary 1.2.9 *If $S \subseteq V^*$ is a subspace, then S is dense in V^* if and only if $S^\perp = \{0\}$.*

Proof: If S is dense in V^*, i.e. $\overline{S} = V^*$, then since $\overline{S} = (S^\perp)^\perp$, it is necessary that $S^\perp = \{0\}$. The converse is obvious, since $\{0\}^\perp = V^*$. ∎

Exercise 1.2.10 *If V is a k-vector space, we have the canonical k-linear map*

$$\phi_V : V \longrightarrow (V^*)^*, \quad \phi_V(x)(f) = f(x), \ \forall x \in V, \ f \in V^*.$$

Then the following assertions hold:
a) The map ϕ_V is injective.
b) $Im(\phi_V)$ is dense in $(V^*)^*$.

Exercise 1.2.11 *Let $V = V_1 \oplus V_2$ be a vector space, and $X = X_1 \oplus X_2$ a subspace of V^* ($X_i \subseteq V_i^*$, $i = 1, 2$). If X is dense in V^*, then X_i is dense in V_i^*, $i = 1, 2$.*

Corollary 1.2.12 *Let X, Y be two subspaces of V^* such that X is closed and $dim_k(Y) < \infty$. Then $X + Y$ is closed.*
In particular, every finite dimensional subspace of V^* is closed.

Proof: Since X is closed, we have $X = (X^\perp)^\perp$. Then by Proposition 1.2.5 ii), we have $X + Y = (X^\perp)^\perp + Y = (X^\perp \cap Y')^\perp$, for some subspace Y' of V, and therefore $X + Y$ is also closed, by Exercise 1.2.3. ∎

Corollary 1.2.13 *i) There is a bijective correspondence between the finite dimensional subspaces of V^* and the subspaces of V of finite codimension, given by $X \longmapsto X^\perp$. Moreover, for any finite dimensional subspace X of V^* we have $dim_k(X) = codim_k(X^\perp)$.*
ii) There is a bijective correspondence between the closed subspaces of V^* of finite codimension and the finite dimensional subspaces of V, given by $X \longmapsto X^\perp$. Moreover, for any closed subspace X of V^* of finite codimension, we have $codim_k(X) = dim_k(X^\perp)$.

Proof: i) Let $X \subseteq V^*$ be a finite dimensional subspace and let $\{u_1, \dots, u_n\}$ be a basis of X. Then $X^\perp = \bigcap_{i=1}^n u_i^\perp = \bigcap_{i=1}^n Ker(u_i)$. But there exists a monomorphism $0 \longrightarrow V/X^\perp \longrightarrow \bigoplus_{i=1}^n V/Ker(u_i)$. Since $dim_k(V/Ker(u_i)) = 1$, we have that $dim_k(V/X^\perp) \leq n = dim_k(X)$, so $X^\perp$ has finite codimension.
Conversely, if $W \subseteq V$ has finite codimension, then $W^\perp \simeq (V/W)^*$, and so $dim_k(W^\perp) = codim_k(W) < \infty$. We can now apply Corollary 1.2.8.
ii) Let $X \subseteq V^*$ be a subspace of finite codimension. There exist $f_1 \dots, f_n \in V^*$ such that $V^* = X \oplus \sum_{i=1}^n k f_i$. Then $0 = V^{*\perp} = X^\perp \cap \bigcap_{i=1}^n Ker(f_i)$, so

$$0 \longrightarrow X^\perp \longrightarrow V/(\bigcap_{i=1}^n Ker(f_i)).$$

But

$$0 \longrightarrow V/(\bigcap_{i=1}^{n} Ker(f_i)) \longrightarrow \bigoplus_{i=1}^{n} V/Ker(f_i) \simeq k^n,$$

so $0 \longrightarrow X^{\perp} \longrightarrow k^n$, and therefore $dim_k(X^{\perp}) \leq n = codim_k(X)$..
Conversely, if $W \subseteq V$ is a finite dimensional subspace, we have $V^*/W^{\perp} \simeq W^*$, so $dim_k(V^*/W^{\perp}) = dim_k(W^*) = dim_k(W)$. ∎

Exercise 1.2.14 *Let $X \subseteq V^*$ be a subspace of finite dimension n. Prove that X is closed in the finite topology of V^* by showing that $dim_k((X^{\perp})^{\perp}) \leq n$.*

Exercise 1.2.15 *If X is a finite codimensional k-linear subspace of V^*, then X is closed in the finite topology if and only if $X^{\perp} = X^{\bar{\perp}}$, where $X^{\bar{\perp}}$ is the orthogonal of X in V^{**}.*

We denote by ${}_k\mathcal{M}$ the category of k-vector spaces. If $u : V \longrightarrow V'$ is a map in this category (i.e. u is k-linear) then we have the dual map $u^* : V'^* \longrightarrow V^*$, where $u^*(f) = f \circ u$, $f \in V'^*$.
Let $W \subseteq V$ be a subspace. Then

$$\begin{aligned} u^{*-1}(W^{\perp}) &= \{f \mid u^*(f) \in W^{\perp}\} \\ &= \{f \in V'^* \mid f \circ u \in W^{\perp}\} \\ &= \{f \in V'^* \mid f(u(W)) = 0\} = u(W)^{\perp}. \end{aligned}$$

Moreover, if W is finite dimensional, then $u(W)$ has finite dimension as a subspace of V', and so it follows that the map $u^* : V'^* \longrightarrow V^*$ is continuous in the finite topology. We have thus the following result:

Corollary 1.2.16 *The mapping $V \longmapsto V^*$ defines a contravariant functor from the category ${}_k\mathcal{M}$ to the category of topological k-vector spaces (k is considered with the discrete topology).* ∎

Exercise 1.2.17 *If V is a k-vector space such that $V = \bigoplus_{i \in I} V_i$, where $\{V_i \mid i \in I\}$ is a family of subspaces of V, then $\bigoplus_{i \in I} V_i^*$ is dense in V^* in the finite topology.*

Exercise 1.2.18 *Let $u : V \longrightarrow V'$ be a k-linear map, and $u^* : V'^* \longrightarrow V^*$ the dual morphism of u. The following assertions hold:*
i) If T is a subspace of V', then $u^*(T^{\perp}) = u^{-1}(T)^{\perp}$.
ii) If X is a subspace of V'^*, then $u^*(X)^{\perp} = u^{-1}(X^{\perp})$.
iii) The image of a closed subspace through u^* is a closed subspace.
iv) If u is injective, and $Y \subseteq V'^*$ is a dense subspace, it follows that $u^*(Y)$ is dense in V^*.

1.3 The dual (co)algebra

We will often use the following simple fact: if X and Y are k-vector spaces, and t is an element of $X \otimes Y$, then t can be represented as $t = \sum_{i=1}^{n} x_i \otimes y_i$ for some positive integer n, some linearly independent $(x_i)_{i=1,n}$ in X, and some $(y_i)_{i=1,n} \subset Y$. Similarly, t can be written as a sum of tensor monomials with the elements appearing on the second tensor position being linearly independent.

Exercise 1.3.1 *Let t be a non-zero element of $X \otimes Y$. Show that there exist a positive integer n, some linearly independent $(x_i)_{i=1,n} \subset X$, and some linearly independent $(y_i)_{i=1,n} \subset Y$ such that $t = \sum_{i=1}^{n} x_i \otimes y_i$*

The following lemma is well known from linear algebra.

Lemma 1.3.2 *Let k be a field, M, N, V three k-vector spaces, and the linear maps $\phi : M^* \otimes V \to Hom(M, V), \phi' : Hom(M, N^*) \to (M \otimes N)^*, \rho : M^* \otimes N^* \to (M \otimes N)^*$ defined by*

$$\phi(f \otimes v)(m) = f(m)v \text{ for } f \in M^*, v \in V, m \in M,$$

$$\phi'(g)(m \otimes n) = g(m)(n) \text{ for } g \in Hom(M, N^*), m \in M, n \in N,$$

$$\rho(f \otimes g)(m \otimes n) = f(m)g(n) \text{ for } f \in M^*, g \in N^*, m \in M, n \in N.$$

Then:
i) ϕ is injective. If moreover V is finite dimensional, then ϕ is an isomorphism.
ii) ϕ' is an isomorphism.
iii) ρ is injective. If moreover N is finite dimensional, then ρ is an isomorphism.

Proof: i) Let $x \in M^* \otimes V$ with $\phi(x) = 0$. Let $x = \sum_i f_i \otimes v_i$ (finite sum), with $f_i \in M^*, v_i \in V$ and $(v_i)_i$ are linearly independent. Then $0 = \phi(x)(m) = \sum_i f_i(m)v_i$ for any $m \in M$, whence $f_i(m) = 0$ for any i and m. It follows that $f_i = 0$ for any i, and then $x = 0$. Thus ϕ is injective. Assume now that V is finite dimensional. For $V = k$ it is clear that ϕ is an isomorphism. Since the functors $M^* \otimes (-)$ and $Hom(M, -)$ commute with finite direct sums, there exist isomorphisms $\phi_1 : M^* \otimes V \to (M^* \otimes k)^n$ and $\phi_2 : (Hom(M, k))^n \to Hom(M, V)$, where $n = dim(V)$. We also have an isomorphism $\phi_3 : (M^* \otimes k)^n \to (Hom(M, k))^n$, the direct sum of n isomorphisms obtained for $V = k$. Moreover, $\phi = \phi_2\phi_3\phi_1$, thus ϕ is an isomorphism too (also see Exercise 1.3.3 below).

ii) If $(X_i)_{i\in I}$ and Y are k-vector spaces, then there exists a canonical isomorphism $Hom(\oplus_{i\in I}X_i, Y) \simeq \prod_{i\in I} Hom(X_i, Y)$. In particular, if I is a basis of M, then $M \simeq k^{(I)}$ and we obtain the canonical isomorphisms

$$u_1 : Hom(M, N^*) \to (Hom(k, N^*))^I$$

$$u_2 : ((k \otimes N)^*)^I \to (M \otimes N)^*.$$

Since clearly for $M = k$ the associated map ϕ' is an isomorphism, we obtain a canonical isomorphism

$$u_3 : (Hom(k, N^*))^I \to ((k \otimes N)^*)^I,$$

and moreover $\phi' = u_2u_3u_1$, so ϕ' is an isomorphism too.
iii) We note that $\rho = \phi'\phi_0$, where ϕ_0 is the morphism obtained as ϕ for $V = N^*$. Then everything follows from the preceding assertions. ∎

Exercise 1.3.3 *Show that if M is a finite dimensional vector space, then the linear map*

$$\phi : M^* \otimes V \to Hom(M, V),$$

defined by $\phi(f \otimes v)(m) = f(m)v$ for $f \in M^*$, $v \in V$, $m \in M$, is an isomorphism.

Exercise 1.3.4 *Let M and N be k-vector spaces. Let the k-linear map:*

$$\rho : V^* \otimes W^* \longrightarrow (V \otimes W)^*, \quad \rho(f \otimes g)(x \otimes y) = f(x)g(y),$$

$\forall f \in M^*, g \in N^*, x \in M, y \in N$. Then the following assertions hold:
a) $Im(\rho)$ is dense in $(M \otimes N)^*$.
b) If M or N is finite dimensional, then ρ is bijective.

Corollary 1.3.5 *For any k-vector spaces $M_1, \ldots, M_n$ the map $\theta : M_1^* \otimes \ldots \otimes M_n^* \to (M_1 \otimes \ldots \otimes M_n)^*$ defined by $\theta(f_1 \otimes \ldots \otimes f_n)(m_1 \otimes \ldots \otimes m_n) = f_1(m_1)\ldots f_n(m_n)$ is injective. Moreover, if all the spaces M_i are finite dimensional, then θ is an isomorphism.*

Proof: The assertion follows immediately by induction from asertion iii) of the lemma. ∎

If X, Y are k-vector spaces and $v : X \to Y$ is a k-linear map, we will denote by $v^* : Y^* \to X^*$ the map defined by $v^*(f) = fv$ for any $f \in Y^*$. We made all the necessary preparations for constructing the dual algebra of a coalgebra. Let then (C, Δ, ε) be a coalgebra. We define the maps $M : C^* \otimes C^* \to C^*, M = \Delta^*\rho$, where ρ is defined as in Lemma 1.3.2, and $u : k \to C^*, u = \varepsilon^*\phi$, where $\phi : k \to k^*$ is the canonical isomorphism.

Proposition 1.3.6 *(C^*, M, u) is an algebra.*

Proof: Denoting $M(f \otimes g)$ by $f * g$, from the definition we obtain that

$$(f * g)(c) = (\Delta^* \rho)(f \otimes g)(c) = \rho(f \otimes g)(\Delta(c)) = \sum f(c_1)g(c_2)$$

for $f, g \in C^*$ and $c \in C$. From this it follows that for $f, g, h \in C^*$ and $c \in C$ we have

$$\begin{aligned} ((f * g) * h)(c) &= \sum (f * g)(c_1)h(c_2) \\ &= \sum f(c_1)g(c_2)h(c_3) \\ &= \sum f(c_1)(g * h)(c_2) \\ &= (f * (g * h))(c) \end{aligned}$$

hence the associativity is checked.
We remark now that for $\alpha \in k$ and $c \in C$ we have $u(\alpha)(c) = \alpha\varepsilon(c)$. The second condition from the definition of an algebra is equivalent to the fact that $u(1)$ is an identity element for the multiplication defined by M, that is $u(1) * f = f * u(1) = f$ for any $f \in C^*$, and this follows directly from $\sum \varepsilon(c_1)c_2 = \sum c_1\varepsilon(c_2) = c$. ∎

Remark 1.3.7 *The algebra C^* defined above is called the dual algebra of the coalgebra C. The multiplication of C^* is called* convolution. *Most of the times (if there is no danger of confusion), we will simply write fg instead of $f * g$ for the convolution product of f and g.* ∎

Example 1.3.8 *1) Let S be a nonempty set, and kS the coalgebra defined in 1.1.4 1). Then the dual algebra is $(kS)^* = Hom(kS, k)$ with multiplication defined by*

$$(f * g)(s) = f(s)g(s)$$

for $f, g \in (kS)^*, s \in S$. Denoting by $Map(S, k)$ the algebra of functions from S to k, the map $\theta : (kS)^* \to Map(S, k)$ associating to a morphism $f \in (kS)^*$ its restriction to S is an algebra isomorphism.
2) Let H be the coalgebra defined in 1.1.4 2). Then the algebra H^* has multiplication defined by

$$(f * g)(c_n) = \sum_{i=0,n} f(c_i)g(c_{n-i})$$

for $f, g \in H^*, n \in \mathbf{N}$, and unit $u : k \to H^*, u(\alpha)(c_n) = \alpha\delta_{0,n}$ for $\alpha \in k$ and $n \in \mathbf{N}$.

H^* is isomorphic to the algebra of formal power series $k[[X]]$, a canonical isomorphism being given by

$$\phi : H^* \to k[[X]],\ \phi(f) = \sum_{n\geq 0} f(c_n)X^n.$$

∎

The dual problem is the following: having an algebra (A, M, u) can one introduce a canonical structure of a coalgebra on A^*? We remark that is is not possible to perform a construction similar to the one of the dual algebra, due to the inexistence of a canonical morphism $(A\otimes A)^* \to A^*\otimes A^*$. However, if A is finite dimensional, the canonical morphism $\rho : A^* \otimes A^* \to (A \otimes A)^*$ is bijective and we can use ρ^{-1}.
Thus, if the algebra (A, M, u) is finite dimensional, we define the maps $\Delta : A^* \to A^* \otimes A^*$ and $\varepsilon : A^* \to k$ by $\Delta = \rho^{-1}M^*$ and $\varepsilon = \psi u^*$, where $\psi : k^* \to k$ is the canonical isomorphism, $\psi(f) = f(1)$ for $f \in k^*$.
We remark that if $\Delta(f) = \sum_i g_i \otimes h_i$, where $g_i, h_i \in A^*$, then $f(ab) = \sum_i g_i(a)h_i(b)$ for any $a, b \in A$. Also if $(g'_j, h'_j)_j$ is a finite family of elements in A^* such that $f(ab) = \sum_j g'_j(a)h'_j(b)$ for any $a, b \in A$, then $\sum_i g_i \otimes h_i = \sum_j g'_j \otimes h'_j$, following from the injectivity of ρ.
In conclusion, we can define $\Delta(f) = \sum g_i \otimes h_i$ for any $(g_i, h_i) \in A^*$ with the property that $f(ab) = \sum_i g_i(a)h_i(b)$ for any $a, b \in A$.

Proposition 1.3.9 *If (A, M, u) is a finite dimensional algebra, then we have that $(A^*, \Delta, \varepsilon)$ is a coalgebra.*

Proof: Let $f \in A^*$ and $\Delta(f) = \sum_i g_i \otimes h_i$. We let $\Delta(g_i) = \sum_j g'_{i,j} \otimes g''_{i,j}$ and $\Delta(h_i) = \sum_j h'_{i,j} \otimes h''_{i,j}$. Then

$$(\Delta \otimes I)\Delta(f) = \sum_{i,j} g'_{i,j} \otimes g''_{i,j} \otimes h_i$$

$$(I \otimes \Delta)\Delta(f) = \sum_{i,j} g_i \otimes h'_{i,j} \otimes h''_{i,j}.$$

We consider the map $\theta : A^* \otimes A^* \otimes A^* \to (A \otimes A \otimes A)^*$ defined by $\theta(u \otimes v \otimes w)(a \otimes b \otimes c) = u(a)v(b)w(c)$ for $u, v, w \in A^*, a, b, c \in A$. This map is injective by Corollary 1.3.5. But

$$\begin{aligned}
\theta(\sum_{i,j} g'_{i,j} \otimes g''_{i,j} \otimes h_i)(a \otimes b \otimes c) &= \sum_{i,j} g'_{i,j}(a)g''_{i,j}(b)h_i(c) \\
&= \sum_i g_i(ab)h_i(c) \\
&= f(abc)
\end{aligned}$$

and

$$\begin{aligned}\theta(\sum_{i,j} g_i \otimes h'_{i,j} \otimes h''_{i,j})(a \otimes b \otimes c) &= \sum_{i,j} g_i(a)h'_{i,j}(b)h''_{i,j}(c) \\ &= \sum_i g_i(a)h_i(bc) \\ &= f(abc)\end{aligned}$$

and then due to the injectivity of θ we obtain that

$$\sum_{i,j} g'_{i,j} \otimes g''_{i,j} \otimes h_i = \sum_{i,j} g_i \otimes h'_{i,j} \otimes h''_{i,j},$$

i.e. Δ is coassociative.
We also have

$$(\sum_i \varepsilon(g_i)h_i)(a) = \sum_i g_i(1)h_i(a) = f(a)$$

hence $\sum_i \varepsilon(g_i)h_i = f$, and similarly $\sum_i \varepsilon(h_i)g_i = f$, so the counit property is also checked. ∎

Remark 1.3.10 *It is possible to express the comultiplication of the dual coalgebra of an algebra A using a basis of A and its dual basis in A^*. Let then $(e_i)_i$ be a basis of the finite dimensional algebra A and $e_i^* \in A^*$ defined by $e_i^*(e_j) = \delta_{i,j}$ (Kronecker symbol). Then $(e_i^*)_i$ is a basis of A^*, called the dual basis, and $(e_j^* \otimes e_l^*)_{j,l}$ is a basis of $A^* \otimes A^*$. It follows that for an element $f \in A^*$ there exist scalars $(a_{j,l})_{j,l}$ such that $\Delta(f) = \sum_{j,l} a_{j,l}e_j^* \otimes e_l^*$. Taking into account the definition of the comultiplication, it follows that for fixed s, t we have*

$$f(e_se_t) = \sum_{j,l} a_{j,l}e_j^*(e_s)e_l^*(e_t) = a_{s,t}.$$

We have obtained that

$$\Delta(f) = \sum_{j,l} f(e_je_l)e_j^* \otimes e_l^*.$$

∎

Exercise 1.3.11 *Let $A = M_n(k)$ be the algebra of $n \times n$ matrices. Then the dual coalgebra of A is isomorphic to the matrix coalgebra $M^c(n, k)$.*

The construction of the dual (co)algebra described above behaves well with respect to morphisms.

Proposition 1.3.12 *i) If $f : C \to D$ is a coalgebra morphism, then $f^* : D^* \to C^*$ is an algebra morphism.*
ii) If $f : A \to B$ is a morphism of finite dimensional algebras, then $f^* : B^* \to A^*$ is a morphism of coalgebras.

Proof: i) Let $d^*, e^* \in D^*$ and $c \in C$. Then

$$(f^*(d^* * e^*))(c) = (d^* * e^*)(f(c))$$

$$= \sum d^*(f(c_1))e^*(f(c_2)) \quad (f \text{ is a coalgebra morphism})$$

$$= \sum (f^*(d^*))(c_1)(f^*(e^*))(c_2)$$

$$= (f^*(d^*) * f^*(e^*))(c)$$

and hence $f^*(d^*e^*) = f^*(d^*)f^*(e^*)$. Moreover, $f^*(\varepsilon_D) = \varepsilon_D f = \varepsilon_C$, so f^* is an algebra morphism.
ii) We have to show that the following diagram is commutative.

$$\begin{tikzcd}
B^* \arrow[r, "f^*"] \arrow[d, "\Delta_{B^*}"'] & A^* \arrow[d, "\Delta_{A^*}"] \\
B^* \otimes B^* \arrow[r, "f^* \otimes f^*"] & A^* \otimes A^*
\end{tikzcd}$$

Let $b^* \in B^*$, $(\Delta_{A^*} f^*)(b^*) = \Delta_{A^*}(b^* f) = \sum_i g_i \otimes h_i$ şi $\Delta_{B^*}(b^*) = \sum_j p_j \otimes q_j$. Denoting by $\rho : A^* \otimes A^* \to (A \otimes A)^*$ the canonical injection, for any $a \in A, b \in B$ we have

$$\rho((\Delta_{A^*} f^*)(b^*))(a \otimes b) = \sum_i g_i(a)h_i(b) = (b^* f)(ab)$$

and

$$\begin{aligned}
\rho((f^* \otimes f^*)\Delta_{B^*}(b^*))(a \otimes b) &= \rho(\sum_j p_j f \otimes q_j f)(a \otimes b) \\
&= \sum (p_j f)(a)(q_j f)(b) \\
&= \sum_j p_j(f(a))q_j(f(b)) \\
&= b^*(f(a)f(b)) \\
&= b^*(f(ab))
\end{aligned}$$

which proves the commutativity of the diagram. Also

$$(\varepsilon_{A^*}f^*)(b^*) = \varepsilon_{A^*}(b^*f) = (b^*f)(1) = b^*(f(1)) = b^*(1) = \varepsilon_{B^*}(b^*),$$

so f^* is a morphism of coalgebras. ∎

Corollary 1.3.13 *The correspondences $C \mapsto C^*$ and $f \mapsto f^*$ define a contravariant functor $(-)^* : k - Cog \to k - Alg$.* ∎

Denoting by $k - f.d.Cog$ and $k - f.d.Alg$ the full subcategories of the categories $k - Cog$ and $k - Alg$ consisting of all finite dimensional objects in these categories, the preceding results define the contravariant functors $(-)^* : k - f.d.Cog \to k - f.d.Alg$ and $(-)^* : k - f.d.Alg \to k - f.d.Cog$ which associate the dual (co)algebra (there is no danger of confusion if we denote both functors by $(-)^*$). We will show that these functors define a duality of categories.
We recall first that if V is a finite dimensional vector space, then the map $\theta_V : V \to V^{**}, \theta_V(v)(v^*) = v^*(v)$ for any $v \in V, v^* \in V^*$ is an isomorphism of vector spaces.

Proposition 1.3.14 *Let A be a finite dimensional algebra and C a finite dimensional coalgebra. Then:*
i) $\theta_A : A \to A^{**}$ is an isomorphism of algebras.
ii) $\theta_C : C \to C^{**}$ is an isomorphism of coalgebras.

Proof: i) We have to prove only that θ_A is an algebra morphism. Let $a, b \in A$ and $a^* \in A^*$. Denote by Δ the comultiplication of A^* and let $\Delta(a^*) = \sum_i f_i \otimes g_i \in A^* \otimes A^*$. Then

$$\begin{aligned}(\theta_A(a) * \theta_A(b))(a^*) &= \sum_i \theta_A(a)(f_i)\theta_A(b)(g_i) \\ &= \sum_i f_i(a)g_i(b) \\ &= a^*(ab) \\ &= \theta_A(ab)(a^*)\end{aligned}$$

so θ_A is multiplicative. We also have that $\theta_A(1)(a^*) = a^*(1) = \varepsilon_{A^*}(a^*)$, so $\theta_A(1) = \varepsilon_{A^*}$, i.e. θ_A preserves the unit.
ii) We denote by Δ and $\overline{\Delta}$ the comultiplications of C and C^{**}. We have to show that the following diagram is commutative.

$$\begin{CD}
C @>{\theta_C}>> C^{**} \\
@V{\Delta}VV @VV{\overline{\Delta}}V \\
C \otimes C @>{\theta_C \otimes \theta_C}>> C^{**} \otimes C^{**}
\end{CD}$$

If $\rho : C^{**} \otimes C^{**} \to (C^* \otimes C^*)^*$ is the canonical isomorphism and $c \in C, c^*, d^* \in C^*$ then putting $\overline{\Delta}(\theta_C(c)) = \sum_i f_i \otimes g_i$ we have

$$\begin{aligned}
\rho((\overline{\Delta}\theta_C)(c))(c^* \otimes d^*) &= \sum_i \rho(f_i \otimes g_i)(c^* \otimes d^*) \\
&= \sum_i f_i(c^*)g_i(d^*) \\
&= \theta_C(c^* * d^*) \\
&= (c^* * d^*)(c)
\end{aligned}$$

and

$$\begin{aligned}
\rho((\theta_C \otimes \theta_C)\Delta(c))(c^* \otimes d^*) &= \sum \rho(\theta_C(c_1) \otimes \theta_C(c_2))(c^* \otimes d^*) \\
&= \sum c^*(c_1)d^*(c_2) = (c^* * d^*)(c)
\end{aligned}$$

proving the commutativity of the diagram.
We also have that

$$(\varepsilon_{C^{**}}\theta_C)(c) = \varepsilon_{C^{**}}(\theta_C(c)) = \theta_C(c)(\varepsilon_C) = \varepsilon_C(c)$$

showing that $\varepsilon_{C^{**}}\theta_C = \varepsilon_C$ and the proof is complete. ∎

Example 1.3.15 *By Exercise 1.3.11 that $M_n(k)^* \simeq M^c(n,k)$. The preceding proposition shows that $M^c(n,k)^* \simeq M_n(k)$.* ∎

1.4 Constructions in the category of coalgebras

Definition 1.4.1 *Let (C, Δ, ε) be a coalgebra. A k-subspace D of C is called a* subcoalgebra *if $\Delta(D) \subseteq D \otimes D$.* ∎

It is clear that if D is a subcoalgebra, then D together with the map $\Delta_D : D \to D \otimes D$ induced by Δ and with the restriction ε_D of ε to D is a coalgebra.

Proposition 1.4.2 *If $(C_i)_{i\in I}$ a family of subcoalgebras of C, then $\sum_{i\in I} C_i$ is a subcoalgebra.*

Proof: $\Delta(\sum_{i\in I} C_i) = \sum_{i\in I} \Delta(C_i) \subseteq \sum_{i\in I} C_i \otimes C_i \subseteq (\sum_{i\in I} C_i) \otimes (\sum_{i\in I} C_i)$. ∎

In the category $k-Cog$ the notion of subcoalgebra coincides with the notion of subobject. We describe now the factor objects in this category.

Definition 1.4.3 *Let (C, Δ, ε) be a coalgebra and I a k-subspace of C. Then I is called:*
i) a left (right) coideal *if $\Delta(I) \subseteq C \otimes I$ (respectively $\Delta(I) \subseteq I \otimes C$).*
ii) a coideal *if $\Delta(I) \subseteq I \otimes C + C \otimes I$ and $\varepsilon(I) = 0$.* ∎

Exercise 1.4.4 *Show that if I is a coideal it does not follow that I is a left or right coideal.*

Lemma 1.4.5 *Let V and W two k-vector spaces, and $X \subseteq V$, $Y \subseteq W$ vector subspaces. Then $(V \otimes Y) \cap (X \otimes W) = X \otimes Y$.*

Proof: Let $(x_j)_{j\in J}$ be a basis in X which we complete with $(x_j)_{j\in J'}$ up to a basis of V. Also consider $(y_p)_{p\in P}$ a basis of Y, which we complete with $(y_p)_{p\in P}$ to get a basis of W. Consider an element

$$q = \sum_{j\in J, p\in P} a_{jp} x_j \otimes y_p + \sum_{j\in J, p\in P'} b_{jp} x_j \otimes y_p +$$

$$+ \sum_{j\in J', p\in P} c_{jp} x_j \otimes y_p + \sum_{j\in J', p\in P'} d_{jp} x_j \otimes y_p$$

in $(V \otimes Y) \cap (X \otimes W)$, where $a_{jp}, b_{jp}, c_{jp}, d_{jp}$ are scalars. Fix $j_0 \in J, p_0 \in P$ and choose $f \in V^*, g \in W^*$ such that $f(x_{j_0}) = 1, f(x_j) = 0$ for any $j \in J \cup J', j \neq j_0$, and $g(y_{p_0}) = 1, g(y_p) = 0$ for any $p \in P \cup P', p \neq p_0$. Since $q \in V \otimes Y$, it follows that $(f \otimes g)(q) = 0$. But then denoting by $\phi : k \otimes k \to k$ the canonical isomorphism, we have $\phi(f \otimes g)(q) = b_{j_0 p_0}$, hence $b_{j_0 p_0} = 0$.
Similarly, we obtain that all of the b_{jp}, c_{jp}, d_{jp} are zero, and thus $q = 0$. It follows that $(V \otimes Y) \cap (X \otimes W) \subseteq X \otimes Y$. The reverse inclusion is clear. ∎

Remark 1.4.6 *If I is a left and right coideal, then, by the preceding lemma $\Delta(I) \subseteq (C \otimes I) \cap (I \otimes C) = I \otimes I$, hence I is a subcoalgebra.* ∎

The following simple, but important result is a first illustration of a certain finiteness property which is intrinsic for coalgebras.

Theorem 1.4.7 *(The Fundamental Theorem of Coalgebras) Every element of a coalgebra C is contained in a finite dimensional subcoalgebra.*

Proof: Let $c \in C$. Write $\Delta_2(c) = \sum_{i,j} c_i \otimes x_{ij} \otimes d_j$, with linearly independent c_i's and d_j's. Denote by X the subspace spanned by the x_{ij}'s, which is finite dimensional. Since $c = (\varepsilon \otimes I \otimes \varepsilon)(\Delta_2(c))$, it follows that $c \in X$. Now

$$(\Delta \otimes I \otimes I)(\Delta_2(c)) = (I \otimes \Delta \otimes I)(\Delta_2(c)),$$

and since the d_j's are linearly independent, it follows that

$$\sum_i c_i \otimes \Delta(x_{ij}) = \sum_i \Delta(c_i) \otimes x_{ij} \in C \otimes C \otimes X.$$

Since the c_i's are linearly independent, it follows that $\Delta(x_{ij}) \in C \otimes X$. Similarly, $\Delta(x_{ij}) \in X \otimes C$, and by the preceding remark X is a subcoalgebra. ∎

The following lemma from linear algebra will also be useful.

Lemma 1.4.8 *Let $f : V_1 \to V_2$ and $g : W_1 \to W_2$ morphisms of k-vector spaces. Then $Ker(f \otimes g) = Ker(f) \otimes W_1 + V_1 \otimes Ker(g)$.*

Proof: Let $(v_\alpha)_{\alpha \in A_1}$ be a basis of $Ker(f)$, which we complete with $(v_\alpha)_{\alpha \in A_2}$ to form a basis of V_1. Then $(f(v_\alpha))_{\alpha \in A_2}$ is a linearly independent subset of V_2. Analogously, let $(w_\beta)_{\beta \in B_1}$ be a basis of $Ker(g)$ which we complete with $(w_\beta)_{\beta \in B_2}$ to a basis of W_1. Again $(g(w_\beta))_{\beta \in B_2}$ is a linearly independent family in W_2. Let

$$q = \sum_{\substack{\alpha \in A_1 \cup A_2 \\ \beta \in B_1 \cup B_2}} c_{\alpha\beta} v_\alpha \otimes w_\beta \in Ker(f \otimes g).$$

Then

$$\sum_{\substack{\alpha \in A_1 \cup A_2 \\ \beta \in B_1 \cup B_2}} c_{\alpha\beta} f(v_\alpha) \otimes g(w_\beta) = 0.$$

By the linearly independence of the family $(f(v_\alpha) \otimes g(w_\beta))_{\alpha \in A_2, \beta \in B_2}$ it follows that $c_{\alpha\beta} = 0$ for any $\alpha \in A_2, \beta \in B_2$.
Then $q \in Ker(f) \otimes W_1 + V_1 \otimes Ker(g)$ and we obtain that

$$Ker(f \otimes g) \subseteq Ker(f) \otimes W_1 + V_1 \otimes Ker(g)$$

The reverse inclusion is clear. ∎

Proposition 1.4.9 *Let $f : C \to D$ be a coalgebra morphism. Then $Im(f)$ is a subcoalgebra of D and $Ker(f)$ is a coideal in C.*

Proof: Since f is a coalgebra map, the following diagram is commutative.

$$\begin{tikzcd} C \arrow[r, "f"] \arrow[d, "\Delta_C"'] & D \arrow[d, "\Delta_D"] \\ C \otimes C \arrow[r, "f \otimes f"] & D \otimes D \end{tikzcd}$$

Then $\Delta_D(Im(f)) = \Delta_D(f(C)) = (f \otimes f)\Delta_C(C) \subseteq (f \otimes f)(C \otimes C) = f(C) \otimes f(C) = Im(f) \otimes Im(f)$, so $Im(f)$ is a subcoalgebra in D.
Also $\Delta_D f(Ker(f)) = 0$, so $(f \otimes f)\Delta_C(Ker(f)) = 0$ and then

$$\Delta_C(Ker(f)) \subseteq Ker(f \otimes f) = Ker(f) \otimes C + C \otimes Ker(f)$$

by Lemma 1.4.8, hence $Ker(f)$ is a coideal. ∎

The construction of factor objects, as well as the universal property they have, are given in the next theorem.

Theorem 1.4.10 *Let C be a coalgebra, I a coideal and $p : C \to C/I$ the canonical projection of k-vector spaces. Then:*
i) There exists a unique coalgebra structure on C/I (called the factor coalgebra) such that p is a morphism of coalgebras.
ii) If $f : C \to D$ is a morphism of coalgebras with $I \subseteq Ker(f)$, then there exists a unique morphism of coalgebras $\overline{f} : C/I \to D$ for which $\overline{f}p = f$.

Proof: i) Since $(p \otimes p)\Delta(I) \subseteq (p \otimes p)(I \otimes C + C \otimes I) = 0$, by the universal property of the factor vector space it follows that there exists a unique linear map $\overline{\Delta} : C/I \to C/I \otimes C/I$ for which the following diagram is commutative.

$$\begin{tikzcd} C \arrow[r, "p"] \arrow[d, "\Delta"'] & C/I \arrow[d, "\overline{\Delta}"] \\ C \otimes C \arrow[r, "p \otimes p"] & C/I \otimes C/I \end{tikzcd}$$

This map is defined by $\overline{\Delta}(\overline{c}) = \sum \overline{c_1} \otimes \overline{c_2}$, where $\overline{c} = p(c)$ is the coset of c modulo I. It is clear that

$$(\overline{\Delta} \otimes I)\overline{\Delta}(\overline{c}) = (I \otimes \overline{\Delta})\overline{\Delta}(\overline{c}) = \sum \overline{c_1} \otimes \overline{c_2} \otimes \overline{c_3}$$

hence $\overline{\Delta}$ is coassociative. Moreover, since $\varepsilon(I) = 0$, by the universal property of the factor vector space it follows that there exists a unique linear map $\overline{\varepsilon} : C/I \to k$ such that the following diagram is commutative.

$$\begin{tikzcd} C \arrow[rr, "p"] \arrow[dr, "\varepsilon"'] & & C/I \arrow[dl, "\overline{\varepsilon}"] \\ & k & \end{tikzcd}$$

We have $\overline{\varepsilon}(\overline{c}) = \varepsilon(c)$ for any $c \in C$, and then

$$\sum \overline{\varepsilon}(\overline{c_1})\overline{c_2} = p(\sum \varepsilon(c_1)c_2) = p(c) = \overline{c}$$

It follows that $(C/I, \overline{\Delta}, \overline{\varepsilon})$ is a coalgebra, and the commutativity of the two diagrams above shows that p is a coalgebra map.
The uniqueness of the coalgebra structure on C/I for which p is a coalgebra morphism follows from the uniqueness of $\overline{\Delta}$ and $\overline{\varepsilon}$.
ii) From the universal property of the factor vector space it follows that there exists a unique morphism of k-vector spaces $\overline{f} : C/I \to D$ such that $\overline{f}p = f$, defined by $\overline{f}(\overline{c}) = f(c)$ for any $c \in C$. Since

$$(\Delta_D\overline{f})(\overline{c}) = \Delta_D(f(c)) = \sum f(c_1) \otimes f(c_2) =$$

$$= \sum \overline{f}(\overline{c_1}) \otimes \overline{f}(\overline{c_2}) = (\overline{f} \otimes \overline{f})(\overline{\Delta}(\overline{c}))$$

and

$$\varepsilon_D\overline{f}(\overline{c}) = \varepsilon_D(f(c)) = \varepsilon_C(c) = \overline{\varepsilon}(c)$$

it follows that $\overline{f}$ is a morphism of coalgebras. ∎

Corollary 1.4.11 *(The fundamental isomorphism theorem for coalgebras) Let $f : C \to D$ be a morphism of coalgebras. Then there exists a canonical isomorphism of coalgebras between $C/Ker(f)$ and $Im(f)$.* ∎

Exercise 1.4.12 *Show that the category $k - Cog$ has coequalizers, i.e. if $f, g : C \to D$ are two morphisms of coalgebras, there exists a coalgebra E and a morphism of coalgebras $h : D \to E$ such that $h \circ f = h \circ g$.*

We describe now a special class of elements of a coalgebra C.

Definition 1.4.13 *An element g of the coalgebra C is called a* grouplike *element if $g \neq 0$ and $\Delta(g) = g \otimes g$. The set of grouplike elements of the coalgebra C is denoted by $G(C)$.* ∎

The counit property shows that $\varepsilon(g) = 1$ for any $g \in G(C)$. Moreover, we show that they are linearly independent.

Proposition 1.4.14 *Let C be a coalgebra. Then the elements of $G(C)$ are linearly independent.*

Proof: We assume that $G(C)$ is not a linearly independent family, and look for a contradiction. Let then n be the smallest natural number for which there exist $g, g_1, \ldots, g_n \in G(C)$, distinct elements such that $g = \sum_{i=1,n} \alpha_i g_i$ for some scalars α_i. If $n = 1$, then $g = \alpha_1 g_1$ and applying ε we obtain $\alpha_1 = 1$ and hence $g_1 = g$, a contradiction. Thus $n \geq 2$. Then all α_i are non-zero (otherwise we would have such a linear combination for a smaller n). We apply Δ to the relation $g = \sum_{i=1,n} \alpha_i g_i$ and we obtain

$$g \otimes g = \sum_{i=1,n} \alpha_i g_i \otimes g_i$$

Replacing g, it follows that

$$\sum_{i,j=1,n} \alpha_i \alpha_j g_i \otimes g_j = \sum_{i=1,n} \alpha_i g_i \otimes g_i.$$

Since the elements $g_1, \ldots, g_n$ are linearly independent (otherwise again we would obtain one of them as a linear combination of less then n grouplike elements), it follows that for $i \neq j$ we have $\alpha_i \alpha_j = 0$, a contradiction. ∎

If A is a finite dimensional algebra, then the grouplike elements of the dual coalgebra have a special meaning.

Proposition 1.4.15 *Let A be a finite dimensional algebra and A^* the dual coalgebra of A. Then $G(A^*) = Alg(A, k)$, the algebra maps from A to k.*

Proof: Let $f \in A^*$. Then f is a grouplike element if $\Delta(f) = f \otimes f$, and taking into account the definition of the dual coalgebra, this implies that $f(ab) = f(a)f(b)$ for any $a, b \in A$. Moreover, $f(1) = \varepsilon(f) = 1$, so f is a morphism of algebras. ∎

Exercise 1.4.16 *Let S be a set, and kS the grouplike coalgebra (see Example 1.1.4, 1). Show that $G(kS) = S$.*

We can now give an example of a coalgebra which has no grouplike elements.

Example 1.4.17 *Let $n > 1$ and $C = M^c(n,k)$ the matrix coalgebra from Example 1.1.4.5). Then C is the dual of the matrix algebra $M_n(k)$ (from Example 1.3.11), hence $G(C) = Alg(M_n(k), k)$. On the other hand, there are no algebra maps $f : M_n(k) \longrightarrow k$, since for such a morphism $Ker(f)$ would be an ideal (we will use sometimes this terminology for a two-sided ideal) of $M_n(k)$, so it would be either 0 or $M_n(k)$. But $Ker(f) = 0$ would imply f injective, which is impossible because of dimensions, and $Ker(f) = M_n(k)$ is again impossible because $f(1) = 1$. Therfore $G(C) = \emptyset$.* ∎

Exercise 1.4.18 *Check directly that there are no grouplike elements in $M^c(n,k)$ if $n > 1$.*

We study now products and coproducts in categories of coalgebras.

Proposition 1.4.19 *The category $k - Cog$ has coproducts.*

Proof: Let $(C_i)_{i\in I}$ be a family of k-coalgebras, $\oplus_{i\in I} C_i$ the direct sum of this family in ${}_k\mathcal{M}$ and $q_j : C_j \rightarrow \oplus_{i\in I} C_i$ the canonical injections. Then there exists a unique morphism Δ in ${}_k\mathcal{M}$ such that the diagram

$$\begin{tikzcd}
C_j \arrow[r, "q_j"] \arrow[d, "\Delta_j"'] & \oplus_{i\in I} C_i \arrow[d, "\Delta"] \\
C_j \otimes C_j \arrow[r, "q_j \otimes q_j"] & (\oplus_{i\in I} C_i) \otimes (\oplus_{i\in I} C_i)
\end{tikzcd}$$

is commutative. Also there exists a unique morphism of vector spaces ε for which the diagram

$$\begin{tikzcd}
C_j \arrow[rr, "q_j"] \arrow[dr, "\varepsilon_j"'] & & \oplus_{i\in I} C_i \arrow[dl, "\varepsilon"] \\
& k &
\end{tikzcd}$$

is commutative. It can be checked immediately, looking at each component, that $(\oplus_{i\in I}C_i, \Delta, \varepsilon)$ is a coalgebra, and that this is the coproduct of the family $(C_i)_{i\in I}$ in the category $k - Cog$. ∎

Before discussing the products in the category $k-Cog$ we need the concept of tensor product of coalgebras. Let then $(C, \Delta_C, \varepsilon_C)$ and $(D, \Delta_D, \varepsilon_D)$ two coalgebras and $\Delta : C\otimes D \to C\otimes D\otimes C\otimes D$, $\varepsilon : C\otimes D \to k$ the maps defined by $\Delta = (I\otimes T\otimes I)(\Delta_C\otimes\Delta_D)$, $\varepsilon = \phi(\varepsilon_C\otimes\varepsilon_D)$, where $T(c\otimes d) = d\otimes c$ and $\phi : k\otimes k \to k$ is the canonical isomorphism. Using the sigma notation we have

$$\Delta(c\otimes d) = \sum c_1\otimes d_1\otimes c_2\otimes d_2$$

$$\varepsilon(c\otimes d) = \varepsilon_C(c)\varepsilon_D(d)$$

for any $c \in C, d \in D$. We also define the maps $\pi_C : C\otimes D \to C, \pi_D : C\otimes D \to D$ by $\pi_C(c\otimes d) = c\varepsilon_D(d), \pi_D(c\otimes d) = \varepsilon_C(c)d$ for any $c \in C, d \in D$.

Proposition 1.4.20 *$(C\otimes D, \Delta, \varepsilon)$ is a coalgebra and the maps π_C and π_D are morphisms of coalgebras.*

Proof: From the definition of Δ it follows that

$$(\Delta\otimes I)\Delta(c\otimes d) = (\Delta\otimes I_{C\otimes D})(\sum c_1\otimes d_1\otimes c_2\otimes d_2)$$

$$= \sum (c_1)_1\otimes(d_1)_1\otimes(c_1)_2\otimes(d_1)_2\otimes c_2\otimes d_2$$

$$= \sum c_1\otimes d_1\otimes c_2\otimes d_2\otimes c_3\otimes d_3$$

and

$$(I\otimes\Delta)\Delta(c\otimes d) = (I_{C\otimes D}\otimes\Delta)(\sum c_1\otimes d_1\otimes c_2\otimes d_2)$$

$$= \sum c_1\otimes d_1\otimes(c_2)_1\otimes(d_2)_1\otimes(c_2)_2\otimes(d_2)_2$$

$$= \sum c_1\otimes d_1\otimes c_2\otimes d_2\otimes c_3\otimes d_3,$$

showing that Δ is coassociative. We also have

$$\begin{aligned}\sum(c_1\otimes d_1)\varepsilon(c_2\otimes d_2) &= \sum(c_1\otimes d_1)\varepsilon_C(c_2)\varepsilon_D(d_2)\\ &= (\sum c_1\varepsilon_C(c_2))\otimes(\sum d_1\varepsilon_D(d_2))\\ &= c\otimes d\end{aligned}$$

and analogously $\sum\varepsilon(c_1\otimes d_1)(c_2\otimes d_2) = c\otimes d$, showing that $C\otimes D$ is a coalgebra. The fact that π_C is a morphism of coalgebras follows from the relations

$$\begin{aligned}(\pi_C \otimes \pi_C)\Delta(c \otimes d) &= \sum c_1 \varepsilon_D(d_1) \otimes c_2 \varepsilon_D(d_2) \\ &= \sum c_1 \varepsilon_D(d_1 \varepsilon_D(d_2)) \otimes c_2 \\ &= \varepsilon_D(d)\Delta_C(c) \\ &= \Delta_C(\pi_C(c \otimes d))\end{aligned}$$

and

$$\varepsilon_C \pi_C(c \otimes d) = \varepsilon_C(c)\varepsilon_D(d) = \varepsilon(c \otimes d).$$

Similarly, π_D is a morphism of coalgebras. ∎

We can now prove that products exist, not in the category $k - Cog$, but in the full subcategory of all cocommutative coalgebras $k - CCog$. This result is dual to the one saying that in the category of commutative k-algebras, the tensor product of two such algebras is their coproduct.

Proposition 1.4.21 *Let C and D be two cocommutative coalgebras. Then $C \otimes D$, together with the maps π_C and π_D is the product of the objects C and D in the category $k - CCog$.*

Proof: Let E be a coalgebra, and $f : E \to C, g : E \to D$ two morphisms of coalgebras. We prove that there exists a unique morphism of coalgebras $\phi : E \to C \otimes D$ such that the following diagram is commutative.

$$\begin{tikzcd} & E \arrow[dl, "f"'] \arrow[dr, "g"] \arrow[dd, "\phi"] & \\ C & & D \\ & C \otimes D \arrow[ul, "\pi_C"] \arrow[ur, "\pi_D"'] & \end{tikzcd}$$

We define $\phi : E \to C \otimes D$ by $\phi(x) = \sum f(x_1) \otimes g(x_2)$ for any $x \in E$. Then

$$\pi_C \phi(x) = \sum f(x_1)\varepsilon_D(g(x_2)) = \sum f(x_1)\varepsilon_E(x_2) = f(x)$$

hence $\pi_C \phi = f$, and analogously $\pi_D \phi = g$. We show now that ϕ is a coalgebra map. We have

$$\begin{aligned}\Delta\phi(x) &= \Delta(\sum f(x_1) \otimes g(x_2)) \\ &= \sum f((x_1)_1) \otimes g((x_2)_1) \otimes f((x_1)_2) \otimes g((x_2)_2) \\ &= \sum f(x_1) \otimes g(x_3) \otimes f(x_2) \otimes g(x_4)\end{aligned}$$

and

$$
\begin{aligned}
(\phi\otimes\phi)\Delta_E(x) &= \sum \phi(x_1)\otimes\phi(x_2)\\
&= \sum f((x_1)_1)\otimes g((x_1)_2)\otimes f((x_2)_1)\otimes g((x_2)_2)\\
&= \sum f(x_1)\otimes g(x_2)\otimes f(x_3)\otimes g(x_4)
\end{aligned}
$$

But E is cocommutative, hence

$$\sum x_1\otimes x_2\otimes x_3\otimes x_4 = \sum x_1\otimes (x_2)_1\otimes (x_2)_2\otimes x_3$$

$$= \sum x_1\otimes (x_2)_2\otimes (x_2)_1\otimes x_3 = \sum x_1\otimes x_3\otimes x_2\otimes x_4$$

and from here it follows that $\Delta\phi(x) = (\phi\otimes\phi)\Delta_E(x)$.
Moreover,

$$
\begin{aligned}
(\varepsilon\phi)(x) &= \varepsilon(\sum f(x_1)\otimes g(x_2))\\
&= \sum \varepsilon_C(f(x_1))\varepsilon_D(g(x_2))\\
&= \sum \varepsilon_E(x_1)\varepsilon_E(x_2)\\
&= \varepsilon_E(\sum x_1\varepsilon_E(x_2))\\
&= \varepsilon_E(x)
\end{aligned}
$$

thus $\varepsilon\phi = \varepsilon_E$.
It remains to prove that ϕ is unique. For this, note that if $\phi' : E \to C\otimes D$ is a morphism of coalgebras with $\pi_C\phi' = f$ and $\pi_D\phi' = g$, then

$$
\begin{aligned}
(f\otimes g)\Delta_E &= (\pi_C\phi'\otimes\pi_D\phi')\Delta_E\\
&= (\pi_C\otimes\pi_D)(\phi'\otimes\phi')\Delta_E\\
&= (\pi_C\otimes\pi_D)\Delta\phi'\\
&= \phi'
\end{aligned}
$$

since clearly $(\pi_C\otimes\pi_D)\Delta$ is the identity. Therefore $\phi' = (f\otimes g)\Delta_E = \phi$. ∎

Another frequently used construction in the theory of coalgebras is the one of co-opposite coalgebra. Let (C,Δ,ε) be a k-coalgebra and the map $\Delta^{cop} : C \to C\otimes C$, $\Delta^{cop} = T\Delta$, where $T : C\otimes C \to C\otimes C$ is the map defined by $T(a\otimes b) = b\otimes a$.

Proposition 1.4.22 *$(C,\Delta^{cop},\varepsilon)$ is a coalgebra.*

Proof: Immediate. ∎

Remark 1.4.23 *The coalgebra defined in the previous proposition is called the co-opposite coalgebra of C and it is denoted by C^{cop}. This concept is dual to the one of opposite algebra of an algebra. We recall that if (A, M, u) is a k-algebra, then the multiplication $MT : A \otimes A \to A$ and the unit u define an algebra structure on the space A, called the opposite algebra of A. This is denoted by A^{op}.* ∎

Proposition 1.4.24 *Let C be a coalgebra. Then the algebras $(C^{cop})^*$ and $(C^*)^{op}$ are equal.*

Proof: Denote by M_1 and M_2 the multiplications in $(C^{cop})^*$ and $(C^*)^{op}$. Then for any $c^*, d^* \in C^*$ and $c \in C$ we have

$$M_1(c^* \otimes d^*)(c) = (c^* \otimes d^*)(T\Delta(c)) = \sum c^*(c_2)d^*(c_1)$$

$$M_2(c^* \otimes d^*)(c) = \sum d^*(c_1)c^*(c_2)$$

which ends the proof. ∎

We close this section by giving the dual version for coalgebras of the extension of scalars for algebras. Let (C, Δ, ε) be a k-coalgebra and $\phi : k \to K$ a morphism of fields. We define $\Delta' : K \otimes_k C \to (K \otimes_k C) \otimes_K (K \otimes_k C)$ and $\varepsilon' : K \otimes_k C \to K$ by $\Delta'(\alpha \otimes c) = \sum (\alpha \otimes c_1) \otimes (1 \otimes c_2)$ and $\varepsilon'(\alpha \otimes c) = \alpha\phi(\varepsilon(c))$ for any $\alpha \in K, c \in C$. The following result is again easily checked

Proposition 1.4.25 *$(K \otimes_k C, \Delta', \varepsilon')$ is a K-coalgebra.* ∎

1.5 The finite dual of an algebra

We saw in Proposition 1.3.9 that for any finite dimensional algebra A, one can introduce a canonical coalgebra structure on the dual space A^*. In this section we show that to any algebra A we can associate in a natural way a coalgebra, which is not defined on the entire dual space A^*, but on a certain subspace of it.

Let then A be an algebra with multiplication $M : A \otimes A \to A$. We consider the following set

$$A^\circ = \{f \in A^* \mid Ker(f) \text{ contains an ideal of finite codimension}\}$$

We recall that a subspace X of the vector space V has finite codimension if $dim(V/X)$ is finite. It is clear that if X and Y are subspaces of finite codimension in V, then $X \cap Y$ also has finite codimension, since there exists an injective morphism $V/(X \cap Y) \to V/X \times V/Y$. Then if $f, g \in A^\circ$

it follows that $Ker(f) \cap Ker(g) \subseteq Ker(f+g)$ and so $f+g \in A^\circ$. Also for $f \in A^\circ, \alpha \in k$ we have $Ker(f) \subseteq Ker(\alpha f)$, so $\alpha f \in A^\circ$ too. Thus A° is a k-subspace in A^*. It is on this subspace that we will introduce a coalgebra structure associated to the algebra A.

Lemma 1.5.1 *Let $f : A \to B$ be a morphfism of algebras and I an ideal of finite codimension in B. Then the ideal $f^{-1}(I)$ has finite codimension in A.*

Proof: Let $p : B \to B/I$ be the canonical projection. Then the map $pf : A \to B/I$ is a morphism of algebras and $Ker(pf) = f^{-1}(I)$. Then $A/f^{-1}(I) \simeq Im(pf) \leq B/I$ which has finite dimension. ∎

Lemma 1.5.2 *Let A, B be algebras and $f : A \to B$ a morphism of algebras. Then:*
i) $f^*(B^\circ) \subseteq A^\circ$, where f^* is the dual map of f.
ii) If we denote by $\phi : A^* \otimes B^* \to (A \otimes B)^*$ the canonical injection, we have $\phi(A^\circ \otimes B^\circ) = (A \otimes B)^\circ$.
iii) $M^*(A^\circ) \subseteq \psi(A^\circ \otimes A^\circ)$, where M is the multiplication of A and $\psi : A^* \otimes A^* \to (A \otimes A)^*$ is the canonical injection.

Proof: i) Let $b^* \in B^\circ$ and I be an ideal of finite codimension in B which is contained in $Ker(b^*)$. Then $f^{-1}(I)$ is an ideal of finite codimension in A by Lemma 1.5.1 and $f^{-1}(I) \subseteq Ker(b^* f) = Ker(f^*(b^*))$. It follows that $f^*(b^*) \in A^\circ$.
ii) Let $a^* \in A^\circ, b^* \in B^\circ$ and I, J ideals of finite codimension in A, respectively B, with $I \subseteq Ker(a^*), J \subseteq Ker(b^*)$. Then $A \otimes J + I \otimes B \subseteq Ker(\phi(a^* \otimes b^*))$, and since $A \otimes J + I \otimes B$ is an ideal in $A \otimes B$ and $(A \otimes B)/(A \otimes J + I \otimes B) \simeq A/I \otimes B/J$, which is finite dimensional, it follows that $\phi(a^* \otimes b^*) \in (A \otimes B)^\circ$, so $\phi(A^\circ \otimes B^\circ) \subseteq (A \otimes B)^\circ$.
Let now $h \in (A \otimes B)^\circ$ and K an ideal of finite codimension of $A \otimes B$ with $K \subseteq Ker(h)$. We define $I = \{a \in A | a \otimes 1 \in K\}$, which is an ideal of A, and $J = \{b \in B | 1 \otimes b \in K\}$, which is an ideal of B. Since I is the inverse image of K via the canonical algebra map $A \to A \otimes B$, sending a to $a \otimes 1$, from Lemma 1.5.1 we deduce that I has finite codimension in A. Analogously, J has finite codimension in B, and moreover $A \otimes J + I \otimes B$ is an ideal of finite codimension in $A \otimes B$. Clearly $A \otimes J + I \otimes B \subseteq K$, so $h(A \otimes J + I \otimes B) = 0$. Then since $(A \otimes B)/(A \otimes J + I \otimes B) \simeq A/I \otimes B/J$, there exits an $\overline{h}$ making the following diagram commutative

$$\begin{tikzcd}
A \otimes B \arrow[rr, "p_I \otimes p_J"] \arrow[dr, "h"'] & & A/I \otimes B/J \arrow[dl, "\overline{h}"] \\
& k &
\end{tikzcd}$$

where p_I şi p_J are the canonical projections.
Since A/I and B/J have both finite codimension, there exists a canonical isomorphism $\theta : (A/I)^* \otimes (B/J)^* \to (A/I \otimes B/J)^*$. Then there exist $(\gamma_i)_i \subseteq (A/I)^*, (\delta_i)_i \subseteq (B/J)^*$, with $\overline{h} = \theta(\sum_i \gamma_i \otimes \delta_i)$. Then

$$\begin{aligned}
h(a \otimes b) &= \overline{h}(p_I(a) \otimes p_J(b)) \\
&= \sum_i \theta(\gamma_i \otimes \delta_i)(p_I(a) \otimes p_J(b)) \\
&= \sum_i \gamma_i(p_I(a))\delta_i(p_J(b)) \\
&= \phi(\sum_i \gamma_i p_I \otimes \delta_i p_J)(a \otimes b)
\end{aligned}$$

and so $h = \phi(\sum_i \gamma_i p_I \otimes \delta_i p_J)$. But $\gamma_i p_I \in A^*$ şi $I \subseteq Ker(\gamma_i p_I)$, hence $\gamma_i p_I \in A^\circ$, and analogously $\gamma_i p_J \in B^\circ$. We have obtained that $h \in \phi(A^\circ \otimes B^\circ)$. Consequently, we also have that $(A \otimes B)^\circ \subseteq \phi(A^\circ \otimes B^\circ)$, and the equality is proved.
iii) Let $a^* \in A^\circ$ and I a finite codimensional ideal of A with $I \subseteq Ker(a^*)$. Then $A \otimes I + I \otimes A$ is a finite codimensional ideal of $A \otimes A$ and $A \otimes I + I \otimes A \subseteq Ker(a^* M)$, hence $a^* M = M(a^*) \in (A \otimes A)^\circ = \psi(A^\circ \otimes A^\circ)$ by assertion ii). ∎

We are now in a position to define the coalgebra structure on A°. With the notation of the preceding proposition we know that $M^*(A^\circ) \subseteq (A \otimes A)^\circ = \psi(A^\circ \otimes A^\circ)$, where $\psi : A^* \otimes A^* \to (A \otimes A)^*$ is the canonical injection. By Lemma 1.5.2 the map ψ can be regarded as an isomorphism between $A^\circ \otimes A^\circ$ and $(A \otimes A)^\circ$. Let then $\Delta : A^\circ \to A^\circ \otimes A^\circ, \Delta = \psi^{-1} M^*$. We also define the map $\varepsilon : A^\circ \to k$ by $\varepsilon(a^*) = a^*(1)$.

Proposition 1.5.3 $(A^\circ, \Delta, \varepsilon)$ *is a coalgebra.*

Proof: Consider the following diagram

$$
\begin{tikzcd}
 & (A\otimes A)^* \arrow[rr, "(I\otimes M)^*"] & & (A\otimes A\otimes A)^* \\
A^* \arrow[ur, "M^*"] \arrow[rr, "M^*"] & & (A\otimes A)^* \arrow[ur, "(M\otimes I)^*"] & \\
 & A^\circ\otimes A^\circ \arrow[uu, "\psi"] \arrow[rr, "I\otimes\Delta"] & & A^\circ\otimes A^\circ\otimes A^\circ \arrow[uu, "\psi_1"'] \\
A^\circ \arrow[uu, "j"] \arrow[ur, "\Delta"] \arrow[rr, "\Delta"'] & & A^\circ\otimes A^\circ \arrow[uu, "\psi"] \arrow[ur, "\Delta\otimes I"'] &
\end{tikzcd}
$$

We have denoted again by ψ the restriction to $A^\circ\otimes A^\circ$ of the map defined above, by ψ_1 the canonical injection, and by j the inclusion. We prove step by step the commutativity of some subdiagrams. First, $(\psi\Delta)(a^*) = (\psi\psi^{-1}M^*)(a^*) = M^*(a^*) = M^*j(a^*)$ for any $a^* \in A^*$, hence $\psi\Delta = M^*j$. In order to show that $\psi_1(\Delta\otimes I) = (M\otimes I)^*\psi$ we note first that if $a^* \in A^\circ$ and $\Delta(a^*) = \sum_i a_i^*\otimes b_i^*$, then $\psi^{-1}M^*(a^*) = \sum_i a_i^*\otimes b_i^*$, so $a^*M = M^*(a^*) = \sum_i \psi(a_i^*\otimes b_i^*)$ and then for any $a,b\in A$ we have $a^*(ab) = \sum_i a_i^*(a)b_i^*(b)$. Then if $a^*,b^*\in A^\circ$ şi $a,b,c\in A$ we have

$$
\begin{aligned}
& (\psi_1(\Delta\otimes I)(a^*\otimes b^*))(a\otimes b\otimes c) = \\
= \;& \psi_1(\sum_i a_i^*\otimes b_i^*\otimes b^*)(a\otimes b\otimes c) \\
= \;& \sum_i a_i^*(a)b_i^*(b)b^*(c) \\
= \;& a^*(ab)b^*(c) \\
= \;& ((M\otimes I)^*\psi(a^*\otimes b^*))(a\otimes b\otimes c)
\end{aligned}
$$

hence $\psi_1(\Delta\otimes I) = (M\otimes I)^*\psi$. Similarly $\psi_1(I\otimes\Delta) = (I\otimes M)^*\psi$. Also

$$(I\otimes M)^*M^* = (M(I\otimes M))^* = (M(M\otimes I))^* = (M\otimes I)^*M^*.$$

Then

$$
\begin{aligned}
\psi_1(\Delta\otimes I)\Delta &= (M\otimes I)^*\psi\Delta \\
&= (M\otimes I)^*M^*j \\
&= (I\otimes M)^*M^*j \\
&= (I\otimes M)^*\psi\Delta \\
&= \psi_1(I\otimes\Delta)\Delta
\end{aligned}
$$

and since ψ_1 is injective, we obtain $(\Delta\otimes I)\Delta = (I\otimes\Delta)\Delta$, the coassociativity of A°.
Let now $a^* \in A^\circ$ and $\Delta(a^*) = \sum_i a_i^* \otimes b_i^*$. Then

$$(\sum_i \varepsilon(a_i^*)b_i^*)(a) = \sum_i a_i^*(1)b_i^*(a) = a^*(1\cdot a) = a^*(a)$$

for any $a \in A$, and therefore $\sum_i \varepsilon(a_i^*)b_i^* = a^*$. Similarly, $\sum_i \varepsilon(b_i^*)a_i^* = a^*$ and the proof is complete. ∎

Proposition 1.5.4 *Let $f : A \to B$ be a morphism of algebras. Then $f^*(B^\circ) \subseteq A^\circ$ and the induced map $f^\circ : B^\circ \to A^\circ$ is a morphism of coalgebras.*

Proof: We already saw in Lemma 1.5.2 that $f^*(B^\circ) \subseteq A^\circ$. In order to show that f° is a morphism of coalgebras, we have to prove that the following two diagrams are commutative.

$$\begin{tikzcd} B^\circ \arrow[r, "f^\circ"] \arrow[d, "\Delta_{B^\circ}"'] & A^\circ \arrow[d, "\Delta_{A^\circ}"] \\ B^\circ\otimes B^\circ \arrow[r, "f^\circ\otimes f^\circ"] & A^\circ\otimes A^\circ \end{tikzcd} \qquad \begin{tikzcd} B^\circ \arrow[rr, "f^\circ"] \arrow[dr, "\varepsilon_{B^\circ}"'] & & A^\circ \arrow[dl, "\varepsilon_{A^\circ}"] \\ & k & \end{tikzcd}$$

The commutativity of the second diagram is immediate, since

$$\varepsilon_{A^\circ} f^\circ(b^*) = (f^\circ(b^*))(1) = b^*(f(1)) = b^*(1) = \varepsilon_{B^\circ}(b^*)$$

for any $b^* \in B^\circ$.
As for the first diagram, let $b^* \in B^\circ$, $\Delta_{B^\circ}(b^*) = \sum_i b_i^* \otimes c_i^*$. Since $\psi : A^\circ \otimes A^\circ \to (A\otimes A)^*$ is injective, in order to show that $(f^\circ\otimes f^\circ)\Delta_{B^\circ} = \Delta_{A^\circ} f^\circ$ it is enough to show that $\psi(f^\circ\otimes f^\circ)\Delta_{B^\circ} = \psi\Delta_{A^\circ} f^\circ$. But for $x, y \in A$ we have

$$\begin{aligned} ((\psi(f^\circ\otimes f^\circ)\Delta_{B^\circ})(b^*))(x\otimes y) &= \sum_i (f^\circ(b_i^*))(x)(f^\circ(c_i^*))(y) \\ &= \sum_i b_i^*(f(x))c_i^*(f(y)) \\ &= b^*(f(x)f(y)) \end{aligned}$$

the last equality following directly from the definition of Δ_{B° ($\Delta = \psi^{-1}M^*$, hence $\psi\Delta = M^*$, then apply it to b^* and then to $f(x) \otimes f(y)$). Further on, we have

$$\begin{aligned}((\psi\Delta_{A^\circ} f^\circ)(b^*))(x \otimes y) &= ((\psi\Delta_{A^\circ})(b^* f))(x \otimes y) \\ &= (M^*(b^* f))(x \otimes y) = (b^* f M)(x \otimes y) \\ &= b^*(f(xy)) \\ &= b^*(f(x)f(y))\end{aligned}$$

and the proof is complete. ∎

The following result is a consequence of the last two propositions.

Corollary 1.5.5 *The mappings $A \mapsto A^\circ$ and $f \mapsto f^\circ$ define a contravariant functor $(-)^\circ : k - Alg \to k - Cog$.* ∎

We are going to give now a characterization of the elements of A° which will be useful for computations. To this end, we first remark that $A^* = Hom(A, k)$, and since A is an A-left, A-right bimodule, it follows that A^* is an A-left, A-right bimodule, with actions given as follows. If $a \in A$ and $a^* \in A^*$, then:
- the left action of A on A^* by $(a \rightharpoonup a^*)(b) = a^*(ba)$ for any $b \in A$.
- the right action of A on A^* by $(a^* \leftharpoonup a)(b) = a^*(ab)$ for any $b \in A$. [1]

Proposition 1.5.6 *Let A be a k-algebra and $f \in A^*$. Then the following assertions are equivalent:*
1) $f \in A^\circ$.
2) $M^*(f) \in \psi(A^\circ \otimes A^\circ)$.
3) $M^*(f) \in \psi(A^* \otimes A^*)$.
4) $A \rightharpoonup f$ is finite dimensional.
5) $f \leftharpoonup A$ is finite dimensional.
6) $A \rightharpoonup f \leftharpoonup A$ is finite dimensional.

Proof: 1) $\Rightarrow$ 2) was proved in Lmma 1.5.2.
2) $\Rightarrow$ 3) is clear.
3) $\Rightarrow$ 4) Let $M^*(f) = \psi(\sum_i a_i^* \otimes b_i^*)$ with $a_i^*, b_i^* \in A^*$. Then for $a, b \in A$ we have $f(ab) = \sum_i a_i^*(a)b_i^*(b)$, hence $(b \rightharpoonup f)(a) = (\sum_i b_i^*(b)a_i^*)(a)$, that is $b \rightharpoonup f = \sum_i b_i^*(b)a_i^*$. This shows that $A \rightharpoonup f$ is contained in the subspace of A^* generated by $(a_i^*)_i$, and this is finite dimensional.

[1]$(a \rightharpoonup a^*)$ should be read as "a hits a^*", and $(a^* \leftharpoonup a)$ as "a^* hit by a". These conventions were proposed by W. Nichols, and are known as the "Nichols dictionary". They also include "$\rightharpoondown$ = twhits" and "$\leftharpoondown$ = twhit by".

4) $\Rightarrow$ 1) We assume that $A \rightharpoonup f$ is finite dimensional. Since $A \rightharpoonup f$ is a left A-submodule of A^*, we have a morphism of k-algebras induced by this structure $\pi : A \to End(A \rightharpoonup f)$ defined by $\pi(a)(m) = a \rightharpoonup m$ for any $a \in A, m \in A \rightharpoonup f$. Since $End(A \rightharpoonup f)$ has also finite dimension, it follows that $I = Ker(\pi)$ is an ideal of finite codimension in A. But for $a \in I$ we have $f(a) = (a \rightharpoonup f)(1) = 0$, so $I \subseteq Ker(f)$ and $f \in A^\circ$.
3) $\Rightarrow$ 5) and 5) $\Rightarrow$ 1) are proved in the same way as 3) $\Rightarrow$ 4) and 4) $\Rightarrow$ 1), working with the right hand structure.
1) $\Rightarrow$ 6) If $f \in A^\circ$, let I be an ideal of finite codimension in A with $I \subseteq Ker(f)$. Then for $a, b \in A$ we have $(a \rightharpoonup f \leftharpoonup b)(I) = f(bIa) \subseteq f(I) = 0$, hence $A \rightharpoonup f \leftharpoonup A \subseteq \{g \in A^* | g(I) = 0\}$. But I has finite codimension, so there exist $(a_i)_{i=1,n} \subseteq A$ completing a basis of I to a basis of A. Denoting by $a_i^* \in A^*$ the map for which $a_i^*(I) = 0, a_i^*(a_j) = \delta_{i,j}$, it follows immediately that the subspace $\{g \in A^* | g(I) = 0\}$ is generated by $(a_i^*)_{i=1,n}$ and so it has finite dimension.
6) $\Rightarrow$ 4) is clear. ∎

Remarks 1.5.7 *1) The preceding proposition shows that A° is the biggest coalgebra contained in A^* and induced by M. Indeed, we have $M^* : A^* \to (A \otimes A)^*$ and if $X \subseteq A^*$ is a coalgebra induced by M, then $M^*(X) \subseteq \psi(X \otimes X)$. But then $M^*(X) \subseteq \psi(A^* \otimes A^*)$, hence $X \subseteq M^{*\,-1}(\psi(A^* \otimes A^*)) = A^\circ$.*
2) It may happen that $A^\circ = 0$. For example, let A be a simple k-algebra of infinite dimension over k (e.g. an infinite field extension of k). Then A does not contain any proper ideals of finite codimension, and hence $A^\circ = 0$.
∎

We recall now another result from linear algebra.

Lemma 1.5.8 *If $f_1, \ldots, f_n$ be linearly independent elements of V^*, then there exist $v_1, \ldots, v_n \in V$ with $f_i(v_j) = \delta_{i,j}$ for any $i, j = 1, \ldots, n$. Moreover, the v_i's are also linearly independent.*

Proof: We proceed by induction on n. For $n = 1$ the result is clear. Let now $f_1, \ldots, f_{n+1}$ be linearly independent in V^*, and appplying the induction hypothesis we find $v_1, \ldots, v_n \in V$ such that $f_i(v_j) = \delta_{i,j}$ for any $i, j = 1, \ldots, n$. Since $f_1, \ldots, f_{n+1}$ are linearly independent, we have $f_{n+1} - \sum_{i=1,n} f_{n+1}(v_i) f_i \neq 0$, hence there exists a $v \in V$ with $f_{n+1}(v) \neq \sum_{i=1,n} f_{n+1}(v_i) f_i(v)$. Then $f_{n+1}(v - \sum_{i=1,n} v_i f_i(v)) \neq 0$ and

$$f_j(v - \sum_{i=1,n} v_i f_i(v)) = f_j(v) - f_j(v) = 0.$$

Multiplying then $v - \sum_{i=1,n} v_i f_i(v)$ by a scalar, we obtain a $w_{n+1} \in V$ with $f_j(w_{n+1}) = \delta_{j,n+1}$ for $j = 1, \ldots, n+1$. Let $w_j = v_j - f_{n+1}(v_j) w_{n+1}$

for $j = 1, \dots, n$. We have $f_i(w_j) = f_i(v_j) = \delta_{i,j}$ for any $i, j = 1, \dots, n$ and $f_{n+1}(w_j) = 0$ for $j = 1, \dots, n$, hence $w_1, \dots, w_{n+1}$ satisfy the required conditions.
The last assertion follows by applying the f_i's to a linear combination of the v_i's which is equal to zero, in order to deduce that all the coefficients are zero. ∎

Remark 1.5.9 *We have that*

$$A^\circ = \{f \in A^* \mid \exists f_i, g_i \in A^* \; : \; f(xy) = \sum f_i(x) g_i(y), \; \forall x, y \in A\} \quad (1.1)$$

From this we see that A° is a subbimodule of A^* with respect to $\rightharpoonup$ and $\leftharpoonup$. If we use Exercise 1.3.1 and assume the f_i's and g_i's are linearly independent, then by Lemma 1.5.8 we obtain that $f_i \in A \rightharpoonup f \subset A^\circ$ and $g_i \in f \leftharpoonup A \subset A^\circ$. Hence we remark that if we use (1.1) as the definition for A°, the fact that it is a coalgebra follows exactly as in the finite dimensional case treated in Proposition 1.3.9.
The above show that for all $f \in A^\circ$, $A \rightharpoonup f \leftharpoonup A$ is a subcoalgebra of A°, and it is finite dimensional. This means that the Fundamental Theorem of Coalgebras (Theorem 1.4.7) holds in A°. Another consequence is that subcoalgebras of A° are subbimodules of A°, and the intersection of a family of subcoalgebras of A° is a subcoalgebra (it contains the subbimodule generated by each of its elements). Thus the smallest subcoalgebra containing $f \in A^\circ$ is $A \rightharpoonup f \leftharpoonup A$.
Finally, we remark that we have the description of the grouplikes in A° exactly as in the finite dimensional case (Proposition 1.4.15):

$$G(A^\circ) = \{f : A \to k \mid \; f \textit{ is an algebra map}\}.$$

∎

An important particular case of a finite dual is obtained for the case the algebra A is a semigroup algebra kG, for some monoid G (kG has basis G as a k-vector space and multiplication given by $(ax)(by) = (ab)(xy)$ for $a, b \in k$, $x, y \in G$). As it is well known, there exists an isomorphism of vector spaces

$$\phi : k^G \longrightarrow (kG)^* = Hom(kG, k), \quad \phi(f)(\sum_i a_i x_i) = \sum_i a_i f(x_i).$$

Consequently, k^G becomes a kG-bimodule by transport of structures via ϕ:

$$(xf)(y) = f(yx), \quad (fx)(y) = f(xy), \;\; \forall x, y \in G, \;\; f \in k^G.$$

Definition 1.5.10 *If G is a monoid, we call*

$$R_k(G) := \phi^{-1}((kG)^\circ)$$

the representative coalgebra *of the monoid G.* ∎

Note that the coalgebra structure on $R_k(G)$ is also transported via ϕ. $R_k(G)$ is a kG-subbimodule of k^G, and consists of the functions (which are called representative) generating a finite dimensional kG-subbimodule (or, equivalently, a left or right kG-submodule). We have

$$R_k(G) = \{f \in k^G \mid \exists f_i, g_i \in k^G,\ \ f(xy) = \sum f_i(x)g_i(y)\ \ \forall x, y \in G\},$$

and the coalgebra structure on $R_k(G)$ is given as follows: if $f \in R_k(G)$, and $f_i, g_i \in k^G$ are such that $f(xy) = \sum f_i(x)g_i(y)$, then $\Delta(f) = \sum f_i \otimes g_i$. Note also that for any k-algebra A we have

$$A^\circ = R_k(A_m) \cap A^*$$

where A_m denotes the multiplicative monoid of A.

The following exercise explains the name of representative functions.

Exercise 1.5.11 *Let G be a group, and $\rho : G \to GL_n(k)$ a representation of G. If we denote $\rho(x) = (f_{ij}(x))_{i,j}$, let $V(\rho)$ be the k-subspace of k^G spanned by the $\{f_{ij}\}_{i,j}$. Then the following assertions hold:*
i) $V(\rho)$ is a finite dimensional subbimodule of k^G.
ii) $R_k(G) = \sum\limits_{\rho} V(\rho)$, where ρ ranges over all finite dimensional representations of G.

We now go back to Exercise 1.1.5 to give the promised explanation of the name "trigonometric coalgebra". The functions sin and cos : $\mathbf{R} \to \mathbf{R}$ satisfy the equalities

$$\sin(x+y) = \sin(x)\cos(y) + \sin(y)\cos(x),$$

and

$$\cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y).$$

These equalities show that sin and cos are representative functions on the group $(\mathbf{R}, +)$. The subspace generated by them in the space of the real functions is then a subcoalgebra of $R_{\mathbf{R}}((\mathbf{R}, +))$, isomorphic to the trigonometric coalgebra.

Other examples of representative functions include:

1) The exponential function $\exp : \mathbf{R} \to \mathbf{R}$, because $e^{x+y} = e^x e^y$, hence $\Delta(\exp) = \exp \otimes \exp$.

In general, if G is a group, then $f \in R_k(G)$ is grouplike if and only if f is a group morphism from G to $(k^*, \cdot)$.
2) The logarithmic function $\lg : (0, \infty) \to \mathbf{R}$, because $\lg(xy) = \lg(x) + \lg(y)$, hence $\Delta(\lg) = \lg \otimes \mathbf{1} + \mathbf{1} \otimes \lg$, where $\mathbf{1}$ denotes the constant function taking the value 1. Such a function is called primitive.
It is also easy to see that in general, if G is a group, then $f \in R_k(G)$ is primitive if and only if f is a group morphism from G to $(k, +)$.
3) Let $d_n : \mathbf{R} \to \mathbf{R}$ be defined by $d_n(x) = \frac{x^n}{n!}$. Since $d_n(x+y) = \sum\limits_i d_i(x) d_{n-i}(y)$ (by the binomial formula), it follows that the d_n's are representative functions on the group $(\mathbf{R}, +)$, and the subspace they span is a subcoalgebra of $R_{\mathbf{R}}((\mathbf{R}, +))$, isomorphic to the divided power coalgebra from Example 1.1.4 2. This explains the name of this coalgebra.

We saw in Proposition 1.3.14 that a finite dimensional (co)algebra is isomorphic to the dual of the dual. We study now the connection between a (co)algebra and dual of the dual in the case of arbitrary dimensions.

Proposition 1.5.12 *Let C be a coalgebra and $\phi : C \to C^{**}$ the canonical injection. Then $Im(\phi) \subseteq C^{*\,\circ}$ and the corestriction $\phi_C : C \to C^{*\,\circ}$ of ϕ is a morphism of coalgebras.*

Proof: Let $c \in C$ and $c^*, d^* \in C^*$. Then

$$\begin{aligned}(c^* \rightharpoonup \phi(c))(d^*) &= \phi(c)(d^*c^*) = (d^*c^*)(c) \\ &= \sum d^*(c_1)c^*(c_2) \\ &= \sum c^*(c_2)\phi(c_1)(d^*)\end{aligned}$$

and hence $c^* \rightharpoonup \phi(c) = \sum c^*(c_2)\phi(c_1)$. It follows that $C^* \rightharpoonup \phi(c)$ is finite dimensional, being contained in the subspace generated by all $\phi(c_1)$. This shows that $\phi(c) \in C^{*\,\circ}$.
We prove now that the following diagrams are commutative.

$$\begin{tikzcd} C \arrow[r, "\phi_C"] \arrow[d, "\Delta"'] & C^{*\,\circ} \arrow[d, "\Delta_0"] \\ C \otimes C \arrow[r, "\phi_C \otimes \phi_C"] & C^{*\,\circ} \otimes C^{*\,\circ} \end{tikzcd} \qquad \begin{tikzcd} C \arrow[rr, "\phi_C"] \arrow[dr, "\varepsilon_C"'] & & C^{*\,\circ} \arrow[dl, "\varepsilon_0"] \\ & k & \end{tikzcd}$$

For the second diagram this is clear, since

$$(\varepsilon_0 \phi_C)(c) = \phi_C(c)(1_{C^*}) = \phi_C(c)(\varepsilon) = \varepsilon(c).$$

For the first diagram we will show taht $\psi\Delta_0\phi_C = \psi(\phi_C \otimes \phi_C)\Delta$, where $\psi : C^{**} \otimes C^{**} \to (C^* \otimes C^*)^*$ is the canonical injection. If $c \in C$ and $c^*, d^* \in C^*$ we have

$$\begin{aligned}
(\psi(\phi_C \otimes \phi_C)\Delta(c))(c^* \otimes d^*) &= (\psi(\sum \phi_C(c_1) \otimes \phi_C(c_2)))(c^* \otimes d^*) \\
&= \sum c^*(c_1)d^*(c_2) \\
&= (c^* \cdot d^*)(c) \\
&= (M(c^* \otimes d^*))(c) \\
&= \phi_C(c)(M(c^* \otimes d^*)) \\
&= (\phi_C(c)M)(c^* \otimes d^*) \\
&= (M^*(\phi_C(c)))(c^* \otimes d^*) \\
&= (\psi\Delta_0(\phi_C(c)))(c^* \otimes d^*) \\
&= ((\psi\Delta_0\phi_C)(c))(c^* \otimes d^*)
\end{aligned}$$

As ψ is injective, it follows that $\Delta_0\phi_C = (\phi_C \otimes \phi_C)\Delta$. ∎

Definition 1.5.13 *A coalgebra C is called* coreflexive *if ϕ_C is an isomorphism.* ∎

Exercise 1.5.14 *The coalgebra C is coreflexive if and only if every ideal of finite codimension in C^* is closed in the finite topology.*

Exercise 1.5.15 *Give another proof for Proposition 1.5.3 using the representative coalgebra. Deduce that any coalgebra is a subcoalgebra of a representative coalgebra.*

Remark 1.5.16 *The above exercise, combined with Remark 1.5.9, shows that the intersection of a family of subcoalgebras of a coalgebra is a subcoalgebra (see Corollary 1.5.29 below).*
The same argument provides a new proof for the Fundamental Theorem of Coalgebras (Theorem 1.4.7). ∎

Exercise 1.5.17 *If C is a coalgebra, show that C is cocommutative if and only if C^* is commutative.*

Proposition 1.5.18 *Let A be an algebra. Then the map $i_A : A \to A^{\circ *}$, defined by $i_A(a)(a^*) = a^*(a)$ for any $a \in A, a^* \in A^\circ$, is a morphism of algebras.*

Proof: We have first that $i_A(1)(a^*) = a^*(1) = \varepsilon_{A^\circ}(a^*)$, so $i_A(1) = \varepsilon_{A^\circ}$, which is the identity of $A^{\circ *}$. Then for any $a, b \in A, a^* \in A^\circ$ we have

$i_A(ab)(a^*) = a^*(ab)$, and

$$\begin{aligned}
(i_A(a)i_A(b))(a^*) &= \sum_p i_A(a)(a_p^*)i_A(b)(b_p^*) \\
&= \sum_p a_p^*(a)b_p^*(b) \\
&= (\psi\Delta(a^*))(a \otimes b) \\
&= M^*(a^*)(a \otimes b) \\
&= (a^*M)(a \otimes b) \\
&= a^*(ab)
\end{aligned}$$

where we have denoted $\Delta(a^*) = \sum_p a_p^* \otimes b_p^*$, and from here it follows that $i_A(ab) = i_A(a) \cdot i_A(b)$. ∎

Exercise 1.5.19 *If A is an algebra, then the algebra map $i_A : A \rightarrow A^{\circ *}$ defined by $i_A(a)(a^*) = a^*(a)$ for any $a \in A, a^* \in A^{\circ}$, is not injective in general.*

Definition 1.5.20 *An algebra A is called* proper *(or* residually finite dimensional*) if i_A is injective, it is called* weakly reflexive *if i_A is injective, and it is called* reflexive *if i_A is bijective.* ∎

Exercise 1.5.21 *If A is a k-algebra, the following assertions are equivalent:*
a) A is proper.
b) A° is dense in A^* in the finite topology.
c) The intersection of all ideals of finite codimension in A is zero.

We now have the following contravariant functors

$$(-)^{\circ} : k - Alg \rightarrow k - Cog$$

$$(-)^* : k - Cog \rightarrow k - Alg$$

In order to work with covariant functors, we will regard these two functors as covariant functors $(-)^{\circ} : k - Alg \rightarrow (k - Cog)^0$ and $(-)^* : (k - Cog)^0 \rightarrow k - Alg$, where by $\mathcal{C}^0$ we have denoted the dual of the category $\mathcal{C}$.

Theorem 1.5.22 $(-)^{\circ}$ *is a left adjoint for* $(-)^*$.

Proof: Let C be a coalgebra and A an algebra. We define the maps

$$u : Hom_{k-Cog}(C, A^{\circ}) \rightarrow Hom_{k-Alg}(A, C^*)$$

$$v : Hom_{k-Alg}(A, C^*) \to Hom_{k-Cog}(C, A^\circ)$$

by $u(f) = f^* i_A$ for $f : C \to A^\circ$ a morphism of coalgebras and $v(g) = g^\circ \phi_C$ for $g : A \to C^*$ a morphism of algebras. We prove that the maps u and v are inverse one to each other. For $f \in Hom_{k-Cog}(C, A^\circ), c \in C$ and $a \in A$ we have

$$\begin{aligned}
(((vu)(f))(c))(a) &= (((f^* i_A)^\circ \phi_C)(c))(a) \\
&= ((f^* i_A)^\circ(\phi_C(c)))(a) \\
&= (\phi_C(c) f^* i_A)(a) \\
&= (\phi_C(c))(f^* i_A(a)) \\
&= (f^* i_A(a))(c) \\
&= (i_A(a) f)(c) \\
&= i_A(a)(f(c)) \\
&= (f(c))(a)
\end{aligned}$$

which shows that $vu = Id$.
For $g \in Hom_{k-Alg}(A, C^*), a \in A$ and $c \in C$ we have

$$\begin{aligned}
(((uv)(g))(a)(c) &= (((g^\circ \phi_C)^* i_A)(a))(c) \\
&= ((g^\circ \phi_C)^*(i_A(a)))(c) \\
&= (i_A(a) g^\circ \phi_C)(c) \\
&= (i_A(a))((g^\circ \phi_C)(c)) \\
&= (g^\circ(\phi_C(c)))(a) \\
&= (\phi_C(c) g)(a) \\
&= \phi_C(c)(g(a)) \\
&= (g(a))(c)
\end{aligned}$$

hence also $uv = Id$. Since the maps u and v are natural, it follows that the claimed adjunction holds. ∎

We remark that if we restrict and corestrict these two functors to the subcategories of (co)-algebras of finite dimension, we obtain the duality of categories described in Section 1.3. In the general case, the above adjunction suggests that many phenomena occur in a dual manner in the categories $k - Alg$ and $k - Cog$.

We show now that there exists a correspondence between the subcoalgebras of a coalgebra and the ideals of the dual algebra. This correspondence is in the spirit of the duality discussed above, since subcoalgebras are subobjects, ideals are subspaces allowing the construction of factor objects, and the notions of subobject and factor object are dual notions.

Proposition 1.5.23 *Let C be a coalgebra and C^* the dual algebra. Then:*
i) If I is an ideal in C^*, it follows that $I^\perp$ is a subcoalgebra in C.
ii) If D is a k-subspace of C, then D is a subcoalgebra in C if and only if $D^\perp$ is an ideal in C^*. In this case the algebras $C^*/D^\perp$ and D^* are isomorphic.

Proof: i) Let $(e_j)_{j\in J}$ be a basis in C and let $c \in I^\perp$. Then there exist $(c_j)_{j\in J} \subseteq C$ with $\Delta(c) = \sum_{j\in J} c_j \otimes e_j$. We show that $c_j \in I^\perp$ for any $j \in J$. Choose $j_0 \in J$ and $h \in C^*$ with $h(e_j) = \delta_{j,j_0}$ for any $j \in J$. If $f \in I$ then $fh \in I$, so $(fh)(c) = 0$. But $(fh)(c) = \sum_{j\in J} f(c_j)h(e_j) = f(c_{j_0})$. It follows that $f(c_{j_0}) = 0$ for any $f \in I$, hence $c_{j_0} \in I^\perp$.
Thus we have that $\Delta(c) \in I^\perp \otimes C$. Similarly, one can prove that $\Delta(c) \in C \otimes I^\perp$. Then $\Delta(c) \in (I^\perp \otimes C) \cap (C \otimes I^\perp) = I^\perp \otimes I^\perp$ by Lemma 1.4.5, and so $I^\perp$ is a subcoalgebra of C.
ii) If $D^\perp$ is an ideal in C^*, then it follows from i) that $D^{\perp\perp}$ is a subcoalgebra in C. But $D^{\perp\perp} = D$ from Theorem 1.2.6. Conversely, if D is a subcoalgebra, let $i : D \to C$ be the inclusion, which is an injective coalgebra map. Then $i^* : C^* \to D^*$ is a surjective algebra map, and it is clear that $Ker(i^*) = D^\perp$. It follows that $D^\perp$ is an ideal, and the required isomorphism follows from the fundamental isomorphism theorem for algebras.
∎

A similar duality holds when we consider the ideals of an algebra and the subcoalgebras of the finite dual.

Proposition 1.5.24 *Let A be an algebra, and A° its finite dual. Then:*
i) If I is an ideal of A, it follows that $I^\perp \cap A^\circ$ is a subcoalgebra in A°.
ii) If D is a subcoalgebra in A°, it follows that $D^\perp$ is an ideal in A.

Proof: i) Let $f \in I^\perp \cap A^\circ$ and $\Delta(f) = \sum_i u_i \otimes v_i$ with $u_i, v_i \in A^\circ$ such that $(v_i)_i$ are linearly independent. From the preceding lemma it follows that there exist $(a_i)_i \subseteq A$ with $v_i(a_j) = \delta_{i,j}$ for any i, j. Then for any j and any $a \in I$ we have $aa_j \in I$, hence $0 = f(aa_j) = \sum_i u_i(a)v_i(a_j) = u_j(a)$, so $u_j \in I^\perp$. It follows that $\Delta(f) \in (I^\perp \cap A^\circ) \otimes A^\circ$. Similarly, $\Delta(f) \in A^\circ \otimes (I^\perp \cap A^\circ)$ and then from Lemma 1.4.5 it follows that $\Delta(f) \in (I^\perp \cap A^\circ) \otimes (I^\perp \cap A^\circ)$.
ii) Let $a \in D^\perp$ and $b \in A$. If $f \in D$ and $\Delta(f) = \sum_i u_i \otimes v_i$ with $u_i, v_i \in D$, then $f(ab) = \sum_i u_i(a)v_i(b) = 0$, hence also $ab \in D^\perp$. Analogously, $ba \in D^\perp$, so $D^\perp$ is an ideal in A. ∎

Dual results also hold if we look at the connection between the coideals of a coalgebra and the subalgebras of the dual algebra, respectively the subalgebras of an algebra and the coideals of the finite dual.

Proposition 1.5.25 *Let C be a coalgebra, and C^* the dual algebra. Then:*
i) If S is a subalgebra in C^*, then $S^\perp$ is a coideal in C.
ii) If I is a coideal in C, then $I^\perp$ is a subalgebra in C^*.

Proof: i) Let $i : S \to C^*$ be the inclusion, which is a morphism of algebras. Then $i^\circ : C^{*\circ} \to S^\circ$ is a morphism of coalgebras, and hence if $\phi_C : C \to C^{*\circ}$ is the canonical coalgebra map, we have a morphism of coalgebras $i^\circ \phi_C : C \to S^\circ$. If $c \in C$, then $c \in Ker(i^\circ \phi_C)$ if and only if $\phi_C(c)i = 0$, and this is equivalent to $f(c) = 0$ for any $f \in S$. Thus $Ker(i^\circ \phi_C) = S^\perp$. Since the kernel of a coalgebra map is a coideal, assertion i) is proved.
ii) Let $\pi : C \to C/I$ be the canonical projection, which is a coalgebra map. Then $\pi^* : (C/I)^* \to C^*$ is a morphism of algebras. If $f \in C^*$, then $f \in Im(\pi^*)$ if and only if there exists $g \in (C/I)^*$ with $f = g\pi$. But this is equivalent to the fact that $f(I) = 0$, or $f \in I^\perp$. It follows that $I^\perp = Im(\pi^*)$, which is a subalgebra in C^*. ∎

Proposition 1.5.26 *Let A be an algebra and A° its finite dual. Then:*
i) If S is a subalgebra in A, then $S^\perp \cap A^\circ$ is a coideal in A°.
ii) If I is a coideal in A°, then $I^\perp$ is a subalgebra in A.

Proof: i) Let $i : S \to A$ be the inclusion, which is a morphism of algebras, and $i^\circ : A^\circ \to S^\circ$ the induced coalgebra map. Then

$$Ker(i^\circ) = \{f \in A^\circ | i^\circ(f) = 0\} =$$

$$= \{f \in A^\circ | fi = 0\} = \{f \in A^\circ | f(S) = 0\} = A^\circ \cap S^\perp,$$

so $A^\circ \cap S^\perp$ is a coideal in A°.
ii) Let $a, b \in I^\perp$ and let $f \in I$. Let $\Delta(f) = \sum_i u_i \otimes v_i \in A^\circ \otimes I + I \otimes A^\circ$. Then $f(ab) = \sum_i u_i(a)v_i(b) = 0$, so $ab \in I^\perp$. Now $\varepsilon_{A^\circ}(f) = 0$ shows that $f(1) = 0$ for any $f \in I$, and hence $1 \in I^\perp$. ∎

We give now connections between the left (right) coideals of a coalgebra and the left (right) ideals of the dual algebra, respectively between the left (right) ideals of an algebra and the left (right) coideals of the finite dual.

Proposition 1.5.27 *Let C be a coalgebra, and C^* the dual algebra. Then:*
i) If I is a left (right) ideal in C^*, then $I^\perp$ is a left (right) coideal in C.
ii) If J is left (right) coideal in C, then $J^\perp$ is a left (right) ideal in C^*.

Proof: i) Assume that I is a left ideal. Let $c \in I^\perp$ and $\Delta(c) = \sum_i c_i \otimes d_i$ with $(c_i)_i$ linearly independent. Fix a j and choose $c^* \in C^*$ with $c^*(c_i) = \delta_{i,j}$ for any i. If $f \in I$ then $c^* f \in I$, hence $(c^* f)(c) = 0$. But $(c^* f)(c) = \sum_i c^*(c_i) f(d_i) = f(d_j)$, so $d_j \in I^\perp$. Consequently, $\Delta(c) \in C \otimes I^\perp$.
ii) Assume that J is a left coideal, so $\Delta(J) \subseteq C \otimes J$. Let $f \in J^\perp$, and $c^* \in C^*$. Then $(c^* f)(J) \subseteq c^*(C) f(J) = 0$, hence $c^* f \in J^\perp$. It follows that $J^\perp$ is a left ideal.
The right hand versions are proved similarly. ∎

Proposition 1.5.28 *Let A be an algebra, and A° its finite dual. Then:*
i) If I is a left (right) ideal in A, then $I^\perp \cap A^\circ$ is a left (right) coideal in A°.
ii) If J is a left (right) coideal in A°, then $J^\perp$ is a left (right) ideal in A.

Proof: i) We assume that I is a left ideal. If $f \in I^\perp \cap A^\circ$, let $\Delta(f) = \sum_i u_i \otimes v_i$ with $u_i, v_i \in A^\circ$ and $(u_i)_i$ linearly independent. By Lemma 1.5.8 it follows that there exist $(a_i)_i \subseteq A$ with $u_i(a_j) = \delta_{i,j}$ for any i, j. If $a \in I$, then $a_i a \in A$, hence $0 = f(a_i a) = v_i(a)$, and so $v_i \in I^\perp$ for any i. We obtained $\Delta(f) \in A^\circ \otimes (I^\perp \cap A^\circ)$.
ii) Assume that J is a left coideal, and let $a \in J^\perp, b \in A$. Since $\Delta(J) \subseteq A^\circ \otimes J$, we obtain that $f(ba) = 0$ for any $f \in J$, hence $ba \in J^\perp$. ∎

Corollary 1.5.29 *Let C be a coalgebra, and $(X_i)_i$ a family of subcoalgebras (left coideals, right coideals). Then $\cap_i X_i$ is a subcoalgebra (left coideal, right coideal).*

Proof: We have $\cap_i X_i = \cap_i X_i^{\perp\perp} = (\sum_i X_i^\perp)^\perp$. But $X_i^\perp$ are ideals (left ideals, right ideals) in C^*, thus $\sum_i X_i^\perp$ is also an ideal (left ideal, right ideal). Then $(\sum_i X_i^\perp)^\perp$ is a subcoalgebra (left coideal, right coideal) in C. ∎

Remark 1.5.30 *The above corollary allows the definition of the subcoalgebra (left coideal, right coideal) generated by a subset of a coalgebra as the smallest subcoalgebra (left coideal, right coideal) containing that set.* ∎

Example 1.5.31 *The finite dimensional subcoalgebra containing an element of a coalgebra constructed in Theorem 1.4.7 is actually the subcoalgebra generated by that element. For if $\Delta_2(c) = \sum_{i,j} c_i \otimes x_{ij} \otimes d_j$ are as in the proof of the fundamental theorem, and if D is any subcoalgebra containing c, then $\Delta_2(c) \in D \otimes D \otimes D$, and applying maps of the form $f_i \otimes I \otimes g_j$ to this (f_i is 1 on c_i and zero on any other $c_{i'}$, and g_j is 1 on d_j, and zero on any other $d_{j'}$), we obtain that the span of the x_{ij}'s is contained in D.* ∎

We give now an application of the fundamental theorem for coalgebras. The following definition is due to P. Gabriel [85].

Definition 1.5.32 *Let A be a k-algebra. A is called a* pseudocompact *algebra if A is a topological k-algebra, Hausdorff separated, complete, and satisfies the APC axiom:*
APC: The ring A has a basis of neighbourhoods of zero formed by the ideals I of finite codimension. ∎

Theorem 1.5.33 *If C is a k-coalgebra, then the dual algebra C^* is a pseudocompact topological algebra.*

Proof: We first prove that the multiplication $M : C^* \times C^* \longrightarrow C^*$ is continuous. If $f, g \in C^*$, let $fg + W^\perp$ be an open neighbourhood of fg (W is a finite dimensional subspace of C). It is easy to see that there exist two finite dimensional subspaces W_1, W_2 of C, such that $\Delta(W) \subseteq W_1 \otimes W_2$. So $f + W_1^\perp$ (resp. $g + W_2^\perp$) is an open neighbourhood of f (resp. g). We prove that

$$M(f + W_1^\perp, g + W_2^\perp) \subseteq fg + W^\perp. \tag{1.2}$$

Indeed, if $u \in W_1^\perp$, $v \in W_2^\perp$, we have

$$(f+u)(g+v) = fg + fv + ug + uv.$$

Now if $c \in W$, then $\Delta(c) = \sum c_1 \otimes c_2 \in W_1 \otimes W_2$. Therefore, $(fv)(c) = \sum f(c_1)v(c_2) = 0$ (since $v \in W_2^\perp$). Similarly, we have $ug(c) = 0$ and $(uv)(c) = 0$. Thus $fv + ug + uv \in W^\perp$, and (1.2) is proved, and M is continuous.

We show now that the set of all ideals I of C^* has the following properties:
i) all I's have finite codimension (i.e. $dim(C^*/I) < \infty$).
ii) they are open and closed in the finite topology, and they form a basis for the filter of neighbourhoods of zero in C^*.

Indeed, the set of $W^\perp$, where W ranges over the finite dimensional subspaces of C is a basis for the filter of neighbourhoods of zero in C^*. By Theorem 1.4.7, there exists a finite dimensional subcoalgebra D of C such that $W \subseteq D$. Then $D^\perp \subseteq W^\perp$, and $I = D^\perp$ is an ideal by Proposition 1.5.23, ii). Since $C^*/I \simeq D^*$, it follows that I is finite codimensional. Also since $I = D^\perp$ and $dim(D) < \infty$, then I is an open neighbourhood of zero in C^*. Since I is an ideal (in particular a subgroup) then I is also closed in the finite topology.

Now if $f, g \in C^*$, $f \neq g$, there exists $x \in C$ such that $f(x) \neq g(x)$. It is easy to see that $(f + x^\perp) \cap (g + x^\perp) = \emptyset$, so C^* is Hausdorff separated.

Finally, since C is the sum of its finite dimensional subcoalgebras D (by Theorem 1.4.7), we have

$$C^* = Hom(C,k) = Hom(\varinjlim D, k) =$$

$$= \varprojlim Hom(D,k) = \varprojlim D^* = \varprojlim (C^*/D^\perp),$$

and therefore C^* is complete. ∎

1.6 The cofree coalgebra

It is well known that the forgetful functor $U : k-Alg \to {}_k\mathcal{M}$ (associating to a k-algebra the underlying k-vector space) has a left adjoint T. The functor

T associates to the k-vector space V the free algebra, which is exactly the tensor algebra $T(V)$. We shall return to this object in Chapter 3, where we show that it has even a Hopf algebra structure. For the moment we will only need the existence of a natural bijection

$$Hom(A,V) \simeq Hom_{k-Alg}(A,T(V))$$

for any k-algebra A and any k-vector space V. This bijection follows from the adjunction property of T. Due to the duality between algebras and coalgebras, it is natural to expect the forgetful functor $U : k - Cog \to {}_k\mathcal{M}$ to have a right adjoint.

Definition 1.6.1 *Let V be a k-vector space. A* cofree coalgebra *over V is a pair (C,p), where C is a k-coalgebra, and $p : C \to V$ is a k-linear map such that for any k-coalgebra D, and any k-linear map $f : D \to V$ there exists a unique morphism of coalgebras $\overline{f} : D \to C$, with $f = p\overline{f}$.* ∎

Exercise 1.6.2 *Show that if (C,p) is a cofree coalgebra over the k-vector space V, then p is surjective.*

Standard arguments show that any two cofree coalgebras over V are isomorphic. The main problem is to show that such a cofree coalgebra always exists.

Lemma 1.6.3 *Let X and Y be two k-vector spaces. Then there exists a natural bijection between $Hom(X,Y^*)$ and $Hom(Y,X^*)$.*

Proof: Define

$$\phi : Hom(X,Y^*) \to Hom(Y,X^*)$$

by $\phi(u)(y)(x) = u(x)(y)$ for any $u \in Hom(X,Y^*), x \in X, y \in Y$ and

$$\psi : Hom(Y,X^*) \to Hom(X,Y^*)$$

by $\psi(v)(x)(y) = v(y)(x)$ for any $v \in Hom(Y,X^*), x \in X, y \in Y$. Then

$$\begin{aligned}(\psi\phi)(u)(x)(y) &= \psi(\phi(u))(x)(y)\\ &= \phi(u)(y)(x)\\ &= u(x)(y),\end{aligned}$$

hence $\psi\phi = Id$, and

$$\begin{aligned}(\phi\psi)(v)(y)(x) &= \phi(\psi(v))(y)(x)\\ &= \psi(v)(x)(y)\\ &= v(y)(x),\end{aligned}$$

hence also $\phi\psi = Id$. ∎

Lemma 1.6.4 *Let V be a k-vector space. Then there exists a cofree coalgebra over V^{**}.*

Proof: Let D be a coalgebra. From the preceding lemma there exists a bijection $\phi : Hom(D, V^{**}) \to Hom(V^*, D^*)$ defined by $\phi(u)(v^*)(d) = u(d)(v^*)$ for any $u \in Hom(D, V^{**}), d \in D, v^* \in V^*$. From the universal property of the tensor algebra it follows that there exists a bijection $\phi_1 : Hom(V^*, D^*) \to Hom_{k-Alg}(T(V^*), D^*)$. We denote by $\phi_1(f) = \overline{f}$ for any $f \in Hom(V^*, D^*)$.
From the adjunction described in Theorem 1.5.22 we have a bijection

$$\phi_2 : Hom_{k-Alg}(T(V^*), D^*) \to Hom_{k-Cog}(D, T(V^*)^\circ)$$

defined by $\phi_2(f) = f^\circ \phi_D$ for any $f \in Hom_{k_{Alg}}(T(V^*), D^*)$, where $\phi_D : D \to D^{*\circ}$ is the canonical morphism. Composing the above bijections we obtain a bijection

$$\phi_2\phi_1\phi : Hom(D, V^{**}) \longrightarrow Hom_{k-Cog}(D, T(V^*)^\circ),$$

$\phi_2\phi_1\phi(f) = (\overline{\phi(f)})^\circ \phi_D$. Let $i : V^* \to T(V^*)$ be the inclusion, and $p : T(V^*)^\circ \to V^{**}$, $p = i^* j$, where $j : T(V^*)^\circ \to T(V^*)^*$ is the inclusion. We show that $(T(V^*)^\circ, p)$ is a cofree coalgebra over V^{**}. Let $f : D \to V^{**}$ be a morphism of k-vector spaces. We show that there exists a unique morphism of coalgebras $\tilde{f} : D \to T(V^*)^\circ$ for which $f = p\tilde{f}$.
Let $\tilde{f} = \phi_2\phi_1\phi(f) = (\overline{\phi(f)})^\circ \phi_D$. Then for $d \in D$ şi $v^* \in V^*$ we have

$$\begin{aligned}
((p\tilde{f})(d))(v^*) &= ((i^* j(\overline{\phi(f)})^\circ \phi_D)(d))(v^*) \\
&= (i^* j(\overline{\phi(f)})^\circ (\phi_D(d)))(v^*) \\
&= (i^* j(\phi_D(d)\overline{\phi(f)}))(v^*) \\
&= (j(\phi_D(d)\overline{\phi(f)})i)(v^*) \\
&= (\phi_D(d)\overline{\phi(f)}i)(v^*) \\
&= \phi_D(d)\overline{\phi(f)}(i(v^*)) \\
&= \phi_D(d)\overline{\phi(f)}(v^*) \\
&= \phi_D(d)(\phi(f)(v^*)) \\
&= \phi(f)(v^*)(d) \\
&= f(d)(v^*),
\end{aligned}$$

hence $f = p\tilde{f}$, and so such $\tilde{f}$ exists.
As for the uniqueness, if $h \in Hom_{k-Cog}(D, T(V^*)^\circ)$ satisfies $ph = f$, let $h = \phi_2\phi_1\phi(f')$ with $f' \in Hom(D, V^{**})$. Then from the above computations it follows that $p\phi_2\phi_1\phi(f') = f'$, hence $ph = f'$. We obtain that $f' = f$ and so $h = \phi_2\phi_1\phi(f) = \tilde{f}$. ∎

Lemma 1.6.5 *Let (C, p) be a cofree coalgebra over the k-vector space V, and let W be a subspace of V. Then there exists a cofree coalgebra over W.*

Proof: Let $D = \sum\{E | E \subseteq C$ subcoalgebra with $p(E) \subseteq W\}$, and let $\pi : D \to W$ denote the restriction and corestriction of p. We show that (D, π) is a cofree coalgebra over W. Let F be a coalgebra, and $f : F \to W$ k-linear map. Then $if : F \to V$ is k-linear (i is the inclusion), hence there exists a unique $h : F \to C$, morphism of coalgebras with $if = ph$. But $ph(F) = if(F) \subseteq i(W) = W$, so $p(h(F)) \subseteq W$, and from the definition of D it follows that $h(F) \subseteq D$. Denoting by $h' : F \to D$ the corestriction of h, we have $\pi h'(x) = ph(x) = if(x) = f(x)$ for any $x \in F$, so $\pi h' = f$.
If $g : F \to D$ is another morphism of coalgebras with $\pi g = f$, then denoting by $g_1 : F \to C$ the morphism given by $g_1(x) = g(x)$ for any $x \in F$, we clearly have $pg_1 = if$, so $h = g_1$. This shows that $g = h'$ and the uniqueness is also proved. ∎

Theorem 1.6.6 *Let V be a k-vector space. Then there exists a cofree coalgebra over V.*

Proof: From Lemma 1.6.4 we know that a cofree coalgebra exists over V^{**}. Since V is isomorphic to a subspace of V^{**}, from Lemma 1.6.5 we obtain that a cofree coalgebra also exists over V. ∎

Corollary 1.6.7 *The forgetful functor $U : k - Cog \to {}_k\mathcal{M}$ has a right adjoint.*

Proof: For $V \in {}_k\mathcal{M}$ we denote by $FC(V)$ the cofree coalgebra over V constructed in Theorem 1.6.6. If $V, W \in {}_k\mathcal{M}$ and $f \in Hom(V, W)$, then there exists a unique morphism of coalgebras $FC(f) : FC(V) \to FC(W)$ for which $fp = \pi FC(f)$, where $p : FC(V) \to V$ and $\pi : FC(W) \to W$ are the morphisms defining the two cofree coalgebras. From the universal property, it follows that for any coalgebra D and any k-vector space V there exists a natural bijection between $Hom(D, V)$ and $Hom_{k-Cog}(D, FC(V))$, hence the functor $FC : {}_k\mathcal{M} \to k - Cog$ defined above is a right adjoint for U. ∎

It is easy to see that for $V = 0$, the cofree coalgebra over V is k with the trivial coalgebra structure (in which the comultiplication is the canonical isomorphism, and the counit is the identical map of k).

Proposition 1.6.8 *Let $p : k \to 0$ be the zero morphism. Then (k, p) is a cofree coalgebra over the null space.*

Proof: Let D be a coalgebra, and $f : D \to 0$ the zero morphism (the unique morphism from D to the null space). Then there exists a unique morphism of coalgebras $g : D \to k$ for which $pg = f$, namely $g = \varepsilon_D$, which is actually the only morphism of coalgebras between D and k. ∎

The cofree coalgebra over a vector space is a universal object in the category of coalgebras. We show now that such a universal object also exists in the category of cocommutative coalgebras.

Definition 1.6.9 *Let V be a vector space. A* cocommutative cofree coalgebra *over V is a pair (E, p), where E is a cocommutative k-coalgebra, and $p : E \to V$ is a k-linear map such that for any cocommutative k-coalgebra D and any k-linear map $f : D \to V$ there exists a unique morphism of coalgebras $\overline{f} : D \to E$ with $f = p\overline{f}$.* ∎

Exercise 1.6.10 *Show that if (C, p) is a cocommutative cofree coalgebra over the k-vector space V, then p is surjective.*

Theorem 1.6.11 *Let V be a k-vector space. Then there exists a cocommutative cofree coalgebra over V.*

Proof: Let (C, p) be a cofree coalgebra over V, whose existence is granted by Theorem 1.6.6. Denoting by E the sum of all cocommutative subcoalgebras of C (such subcoalgebras exist, e.g. the null subcoalgebra) and let $i : E \to C$ be the canonical injection. It is clear that E is a cocommutative coalgebra, as sum of cocommutative subcoalgebras. Then (E, pi) is a cocommutative cofree coalgebra over V. Indeed, if D is a cocommmutative coalgebra, and $f : D \to V$ is a morphism of vector spaces, then since (C, p) is a cofree coalgebra over V, it follows that there exists a unique morphism of coalgebras $g : D \to C$ such that $pg = f$. Since D is cocommutative, it follows that $Im(g)$ is a cocommutative subcoalgebra of C, and hence $Im(g) \subseteq E$. We denote by $h : D \to E$ the corestriction of g to E, which clearly satisfies $ih = g$. Then h is a morphism of coalgebras, and $pih = pg = f$.
Moreover, the morphism of coalgebras h is unique such that $pih = f$, for if $h' : D \to E$ would be another morphism of coalgebras with $pih' = f$, we would have $p(ih') = f$, and $ih' : D \to C$ is a morphism of coalgebras. From the uniqueness of g it follows that $ih' = g = ih$, and since i is injective it follows that $h' = h$, finishing the proof. ∎

For a k-vector space V, we will denote by $CFC(V)$ the cocommutative cofree coalgebra over V, constructed in the preceding theorem. In fact, we can construct a functor $CFC : {}_k\mathcal{M} \to k - CCog$, where $k - CCog$ is the full subcategory of $k - Cog$ having as objects all cocommutative coalgebras. To a vector space V we associate through this functor the cocommutative cofree coalgebra $CFC(V)$. If $f : V \to W$ is a linear map, and $(CFC(V), p)$

and $(CFC(W), \pi)$ are the cocommutative cofree coalgebras over V and W, then we denote by $CFC(f) : CFC(V) \to CFC(W)$ the unique morphism of coalgebras for which $\pi CFC(f) = fp$ (the existence and uniqueness of $CFC(f)$ follow from the universal property of $CFC(W)$). These associations on objects and morphisms define the functor CFC, which is also a right adjoint functor.

Corollary 1.6.12 *The functor CFC is a right adjoint for the forgetful functor $U : k - CCog \to {}_k\mathcal{M}$.*

Proof: This follows directly from the universal property of the cocommutative cofree coalgebra. ∎

Proposition 1.6.13 *The cocommutative cofree coalgebra over the null space is k, with the trivial coalgebra structure, together with the zero morphism.*

Proof: The cofree coalgebra over the null space is k by Proposition 1.6.8. Since this coalgebra is cocommutative, the construction of the cocommutative cofree coalgebra (described in the proof of Theorem 1.6.11) shows that this is also the cocommutative cofree coalgebra over 0. ∎

We describe now the cocommutative cofree coalgebra over the direct sum of two vector spaces.

Proposition 1.6.14 *Let V_1, V_2 be vector spaces, (C_1, π_1), and (C_2, π_2) the cocommutative cofree coalgebras over them. Let*

$$\pi : C_1 \otimes C_2 \to V_1 \oplus V_2, \ \pi(c \otimes e) = (\pi_1(c)\varepsilon_2(e), \pi_2(e)\varepsilon_1(c))$$

where $\varepsilon_1, \varepsilon_2$ are the counits of C_1 and C_2. Then $(C_1 \otimes C_2, \pi)$ is a cocommutative cofree coalgebra over $V_1 \oplus V_2$.

Proof: Denote by $p_1 : C_1 \otimes C_2 \to C_1, p_2 : C_1 \otimes C_2 \to C_2$ the morphisms of coalgebras defined by $p_1(c \otimes e) = c\varepsilon_2(e)$ and $p_2(c \otimes e) = e\varepsilon_1(c)$. Also denote by $q_1 : V_1 \oplus V_2 \to V_1$ and $q_2 : V_1 \oplus V_2 \to V_2$ the canonical projections. Note that $\pi_1 p_1 = q_1 \pi$ and $\pi_2 p_2 = q_2 \pi$.
Let now D be a cocommutative coalgebra, and $f : D \to V_1 \oplus V_2$ a linear map. Since (C_1, π_1) is a cocommutative cofree coalgebra over V_1, it follows that there exists a unique morphism of coalgebras $g_1 : D \to C_1$ for which $q_1 f = \pi_1 g_1$. Similarly, there exists a unique morphism of coalgebras $g_2 : D \to C_2$ for which $q_2 f = \pi_2 g_2$.
We know that $C_1 \otimes C_2$, together with the maps p_1, p_2 is a product of the coalgebras C_1 and C_2 in the category of cocommutative coalgebras

(by Proposition 1.4.21). It follows that there exists a unique morphism of coalgebras $g : D \to C_1 \otimes C_2$ for which $p_1 g = g_1$ and $p_2 g = g_2$. Then we have

$$q_1 \pi g = \pi_1 p_1 g = \pi_1 g_1 = q_1 f,$$

and similarly $q_2 \pi g = q_2 f$. It follows that $\pi g = f$, and hence we constructed a morphism of coalgebras $g : D \to C_1 \otimes C_2$ such that $\pi g = f$.
Let us show that g is the unique morphism of coalgebras with this property, and then it will follow that $(C_1 \otimes C_2, \pi)$ is a cocommutative cofree coalgebra over $V_1 \oplus V_2$.
Let $g' : D \to C_1 \otimes C_2$ be another morphism of coalgebras with $\pi g' = f$. Then $q_1 f = q_1 \pi g' = \pi_1 p_1 g'$, and from the uniqueness of g_1 with the property that $q_1 f = \pi_1 g_1$, it follows that $p_1 g' = g_1$. Similarly, we obtain that $p_2 g' = g_2$. Finally, from the uniqueness of g with $p_1 g = g_1$ and $p_2 g = g_2$, we obtain that $g' = g$, which ends the proof. ∎

1.7 Solutions to exercises

Exercise 1.1.5 *Let C be a k-space with basis $\{s, c\}$. We define $\Delta : C \to C \otimes C$ and $\varepsilon : C \to k$ by*

$$\begin{aligned} \Delta(s) &= s \otimes c + c \otimes s \\ \Delta(c) &= c \otimes c - s \otimes s \\ \varepsilon(s) &= 0 \\ \varepsilon(c) &= 1. \end{aligned}$$

Show that (C, Δ, ε) is a coalgebra.
Solution: We have

$$(I \otimes \Delta)\Delta(s) = (\Delta \otimes I)\Delta(s) = s \otimes c \otimes c + c \otimes s \otimes c + c \otimes c \otimes s - s \otimes s \otimes s,$$

and

$$(I \otimes \Delta)\Delta(c) = (\Delta \otimes I)\Delta(c) = c \otimes c \otimes c - s \otimes s \otimes c - s \otimes c \otimes s - c \otimes s \otimes s.$$

The counit property is obvious.

Exercise 1.1.6 *Show that on any vector space V one can introduce an algebra structure.*
Solution: It is clear if $V = 0$. Assume $V \neq 0$, choose $e \in V$, $e \neq 0$, and complete $\{e\}$ to a basis of V with the set $S = \{x_i\}_{i \in I}$. Define now an algebra structure on V by

$$e x_i = x_i e = x_i, \quad x_i x_j = 0, \quad \forall i, j \in I.$$

We remark that this is actually isomorphic to

$$\frac{k[X_i \mid \in I]}{(X_iX_j \mid i,j \in I)},$$

and it is also the algebra obtained by adjoining a unit to the ring kS with zero multiplication.

Exercise 1.1.15 *Show that in the category $k-Cog$, isomorphisms (i.e. morphisms of coalgebras having an inverse which is also a coalgebra morphism) are precisely the bijective morphisms.*
Solution: Let $g : C \longrightarrow D$ be a bijective coalgebra map. We have to show that g^{-1} is also a coalgebra morphism. For $c \in C$ we have

$$\begin{aligned}
\Delta(g^{-1}(c)) &= \sum g^{-1}(c)_1 \otimes g^{-1}(c)_2 \\
&= \sum g^{-1}(g(g^{-1}(c)_1)) \otimes g^{-1}(g(g^{-1}(c)_2)) \\
&= \sum g^{-1}(g(g^{-1}(c))_1) \otimes g^{-1}(g(g^{-1}(c))_2) \\
&= \sum g^{-1}(c_1) \otimes g^{-1}(c_2),
\end{aligned}$$

so g preserves the comultiplication. The preservation of the counit is obvious.

Exercise 1.2.2 *An open subspace in a topological vector space is also closed.*
Solution: If U is the open subspace and $x \notin U$, then $x+U$ is a neighbourhood of x which does not meet U, hence the complement of U is open.

Exercise 1.2.3 *When S is a subset of V^* (or V), $S^\perp$ is a subspace of V (or V^*). In fact $S^\perp = \langle S\rangle^\perp$, where $\langle S\rangle$ is the subspace spanned by S. Moreover, we have $S^\perp = ((S^\perp)^\perp)^\perp$, for any subset S of V^* (or V).*
Solution: Let S be a subset of V^*, and $x, y \in S^\perp$, $\lambda, \mu \in k$. Then if $u \in S$, $u(\lambda x + \mu y) = \lambda u(x) + \mu u(y) = 0$, and so $\lambda x + \mu y \in S^\perp$.
Now, since $S \subseteq \langle S\rangle$, it is clear that $S^\perp \supseteq \langle S\rangle^\perp$. On the other hand, if $x \in S^\perp$, any linear combination of elements in S will vanish in x, so equality holds.
Finally, since $S \subseteq (S^\perp)^\perp$, we have $S^\perp \supseteq ((S^\perp)^\perp)^\perp$. Conversely, if $x \in S^\perp$, we have that $u(x) = 0$ for all $u \in (S^\perp)^\perp$ by definition, so $S^\perp = ((S^\perp)^\perp)^\perp$. The other assertions are proved in a similar way.

Exercise 1.2.4 *The set of all $f + W^\perp$, where W ranges over the finite dimensional subspaces of V, form a basis for the filter of neighbourhoods of $f \in V^*$ in the finite topology.*
Solution: We know that a basis for the filter of neighbourhoods of $f \in V^*$

in the finite topology is $f + \mathcal{O}(0, x_1, \ldots, x_n)$. Note that $\mathcal{O}(0, x_1, \ldots, x_n) = W^{\perp}$, where W is the subspace of V spanned by $x_1, \ldots, x_n$.

Exercise 1.2.7 *If S is a subspace of V^*, then prove that $(S^{\perp})^{\perp}$ is closed in the finite topology by showing that its complement is open.*
Solution: If $f \notin (S^{\perp})^{\perp}$, then there is an $x \in S^{\perp}$ such that $f(x) \neq 0$. Then $(f + x^{\perp}) \cap (S^{\perp})^{\perp} = \emptyset$.

Exercise 1.2.10 *If V is a k-vector space, we have the canonical k-linear map*

$$\phi_V : V \longrightarrow (V^*)^*, \quad \phi_V(x)(f) = f(x), \ \forall x \in V, \ f \in V^*.$$

Then the following assertions hold:
a) The map ϕ_V is injective.
b) $Im(\phi_V)$ is dense in $(V^*)^*$.
Solution: a) Let $x \in Ker(\phi_V)$. If $x \neq 0$, there exists $f \in V^*$ such that $f(x) \neq 0$. Since $\phi_V(x) = 0$, we obtain that $f(x) = 0$, $\forall f \in V^*$, a contradiction.
b) We prove that $(Im(\phi_V))^{\perp} = \{0\}$. Let $f \in (Im(\phi_V))^{\perp} \subseteq V^*$. Hence $\phi_V(x)(f) = 0$ for every $x \in V$. Thus $f(x) = 0 \ \forall x \in V$, and therefore $f = 0$.

Exercise 1.2.11 *Let $V = V_1 \oplus V_2$ be a vector space, and $X = X_1 \oplus X_2$ a subspace of V^* ($X_i \subseteq V_i^*$, $i = 1, 2$). If X is dense in V^*, then X_i is dense in V_i^*, $i = 1, 2$.*
Solution: Let $x \in (X_1)^{\perp}$. If $f \in X$, then $f = f_1 + f_2$, with $f_1 \in X_1$ and $f_2 \in X_2$. Since $V^* = V_1^* \oplus V_2^*$, we have that $f_2(V_1) = 0$, so $f(x) = f_1(x) + f_2(x) = 0$. Hence $x \in X^{\perp} = \{0\}$.

Exercise 1.2.14 *Let $X \subseteq V^*$ be a subspace of finite dimension n. Prove that X is closed in the finite topology of V^* by showing that $dim_k((X^{\perp})^{\perp} \leq n$.*
Solution: Let $\{f_1, \ldots, f_n\}$ be a basis of X. Then $X^{\perp} = \bigcap_{i=1}^{n} Ker(f_i)$, and therefore $0 \longrightarrow V/X^{\perp} \longrightarrow k^n$, so $dim_k(V/X^{\perp}) \leq n$, and hence $dim_k(V/X^{\perp})^* \leq n$.
On the other hand, from the exact sequence

$$0 \longrightarrow X^{\perp} \longrightarrow V \longrightarrow V/X^{\perp} \longrightarrow 0,$$

we have

$$0 \longrightarrow (V/X^{\perp})^* \longrightarrow V^* \longrightarrow (X^{\perp})^* \longrightarrow 0,$$

so $(V/X^{\perp})^* \simeq (X^{\perp})^{\perp}$. Hence $dim_k(X^{\perp})^{\perp} \leq n$. Since $X \subseteq (X^{\perp})^{\perp}$, we obtain that $X = (X^{\perp})^{\perp}$.

Exercise 1.2.15 *If X is a finite codimensional k-linear subspace of V^*, then X is closed in the finite topology if and only if $X^\perp = X^{\tilde{\perp}}$, where $X^{\tilde{\perp}}$ is the orthogonal of X in V^{**}.*
Solution: Assume that X is closed and that $dim_k(V^*/X) = n < \infty$. Let

$$\phi_V : V \longrightarrow V^{**}, \quad \phi_V(x)(f) = f(x),$$

denote the canonical map. The equality $X^\perp = X^{\tilde{\perp}}$ actually means $\phi(X^\perp) = X^{\tilde{\perp}}$ We have $\phi_V(X^\perp) = \phi_V(V) \cap X^{\tilde{\perp}}$, so $\phi_V(X^\perp) \subseteq X^{\tilde{\perp}}$.
Let $f \in V^{**}$, $f \in X^{\tilde{\perp}}$. Thus $f : V^* \longrightarrow k$, with $f(X) = 0$. Since X has finite codimension in V^*, it follows from Corollary 1.2.13 ii) that $X^\perp$ has finite dimension as a subspace of V. If we put $W = X^\perp$, then we have $f \in (V^*/X)^* = (V^*/(X^\perp)^\perp)^* \simeq ((X^\perp)^*)^* = W^{**} \simeq W$. So there exists a $x \in W$ such that $f = \phi_V(x)$, and thus $f \in \phi_V(V) \cap X^{\tilde{\perp}} = \phi_V(X^\perp)$. Hence $\phi_V(X^\perp) = X^{\tilde{\perp}}$.
Conversely, assume that $\phi_V(X^\perp) = X^{\tilde{\perp}}$. We prove that $X = (X^\perp)^\perp$. We have $X = \bigcap_{f \in X^{\tilde{\perp}}} Ker(f)$. If $f \in X^{\tilde{\perp}}$, there exists $x \in X^\perp$ such that $f = \phi_V(x)$. Hence $X = \bigcap_{x \in X^\perp} Ker(\phi_V(x)) = (X^\perp)^\perp$. Thus X is closed.

Exercise 1.2.17 *If V is a k-vector space such that $V = \bigoplus_{i \in I} V_i$, where $\{V_i \mid i \in I\}$ is a family of subspaces of V, then $\bigoplus_{i \in I} V_i^*$ is dense in V^* in the finite topology.*
Solution: $\bigoplus_{i \in I} V_i^*$ is the subspace X of V^*, where

$$X = \{f \in V^* \mid f(V_j) = 0 \text{ for almost all } j \in I\}.$$

If $x \in V$, $x \in X^\perp$, such that $x \neq 0$, then $x = \sum_{i \in I} x_i$, where $x_i \in V_i$ are almost all zero. Since $x \neq 0$, there exists $i_0 \in I$ such that $x_{i_0} \neq 0$. Thus there exists $f \in V^*$ such that $f(V_i) = 0$ for $i \neq i_0$, and $f(x_{i_0}) \neq 0$. Clearly $f \in X$, and therefore $0 = f(x) = f(x_{i_0})$, a contradiction.

Exercise 1.2.18 *Let $u : V \longrightarrow V'$ be a k-linear map, and $u^* : V'^* \longrightarrow V^*$ the dual morphism of u. The following assertions hold:*
i) If T is a subspace of V', then $u^*(T^\perp) = u^{-1}(T)^\perp$.
ii) If X is a subspace of V'^*, then $u^*(X)^\perp = u^{-1}(X^\perp)$.
iii) The image of a closed subspace through u^* is a closed subspace.
iv) If u is injective, and $Y \subseteq V'^*$ is a dense subspace, it follows that $u^*(Y)$ is dense in V^*.
Solution: i) Let $f \in u^*(T^\perp)$. Then $f = u^*(g) = g \circ u$ for some $g \in$

$T^\perp$. If $x \in u^{-1}(T)$, then $f(x) = g(u(x)) = 0$, hence $u^*(T^\perp) \subseteq u^{-1}(T)^\perp$. Conversely, let $g \in u^{-1}(T)^\perp$. Define $f \in V^*$ by $f(u(x)) = g(x)$, and $f = 0$ on the complement of $Im(u)$. The definition is correct, because if $u(x) = u(y)$, then $x - y \in Ker(u) \subseteq u^{-1}(T)$. Moreover, $f \circ u = g$, since for $w \in T \cap Im(u)$ we have $w = u(x)$, $x \in u^{-1}(T)$, and so $f(w) = g(x) = 0$. It is clear that $f \in T^\perp$, so we have proved that $u^*(X)^\perp = u^{-1}(X^\perp)$.
ii) We have $x \in u^*(X)^\perp \Leftrightarrow f(u(x)) = 0 \ \forall f \in X \Leftrightarrow u(x) \in X^\perp \Leftrightarrow x \in u^{-1}(X^\perp)$.
iii) Let X be a closed subspace of V'^*. Then

$$\begin{aligned} u^*(X) &= u^*(\overline{X}) \\ &= u^*(X^{\perp\perp}) \\ &= u^{-1}(X^\perp)^\perp \text{ (by i))} \\ &= u^*(X)^{\perp\perp} \text{ (by ii))} \\ &= \overline{u^*(X)}. \end{aligned}$$

iv) We use ii): $u^*(Y)^\perp = u^{-1}(Y^\perp) = u^{-1}(0) = 0$.

Exercise 1.3.1 *Let t be a non-zero element of $X \otimes Y$. Show that there exist a positive integer n, some linearly independent $(x_i)_{i=1,n} \subset X$, and some linearly independent $(y_i)_{i=1,n} \subset Y$ such that $t = \sum_{i=1}^{n} x_i \otimes y_i$*

Solution: Let n be the least positive integer for which there exists a representation $t = \sum_{i=1}^{n} x_i \otimes y_i$ with $(x_i)_{i=1,n}$ linearly independent. We show that $(y_i)_{i=1,n}$ are also linearly independent.
If not, one of the y_i's, say y_n, is a linear combination of the others. Thus $y_n = \sum_{i=1}^{n-1} \alpha_i y_i$, and then

$$\begin{aligned} t &= \sum_{i=1}^{n-1} x_i \otimes y_i + x_n \otimes (\sum_{i=1}^{n-1} \alpha_i y_i) \\ &= \sum_{i=1}^{n-1} (x_i + \alpha_i x_n) \otimes y_i. \end{aligned}$$

But $\{x_1 + \alpha_1 x_n, \ldots, x_{n-1} + \alpha_{n-1} x_n\}$ are obviously linearly independent, and we obtain a representation of t with $n-1$ terms, and linearly independent elements on the first tensor positions, a contradiction.

Exercise 1.3.3 *Show that if M is a finite dimensional k-vector space, then the linear map*

$$\phi : M^* \otimes V \to Hom(M, V),$$

defined by $\phi(f \otimes v)(m) = f(m)v$ for $f \in M^*$, $v \in V$, $m \in M$, is an isomorphism.
Solution: We know from Lemma 1.3.2 that ϕ is injective. Let $v_i \in M$, $v_i^* \in M^*$, $i = 1, \dots, n$ be dual bases, i.e. $\sum_{i=1}^{n} v_i^*(v)v_i = v$, $\forall v \in M$. Then for any $f \in Hom(M, V)$ we have that $f = \phi(\sum_{i=1}^{n} v_i^* \otimes f(v_i))$, so ϕ is also surjective.

Exercise 1.3.4 *Let M and N be k-vector spaces. Let the k-linear map:*

$$\rho : V^* \otimes W^* \longrightarrow (V \otimes W)^*, \quad \rho(f \otimes g)(x \otimes y) = f(x)g(y),$$

$\forall f \in M^*, g \in N^*, x \in M, y \in N$. Then the following assertions hold:
a) $Im(\rho)$ is dense in $(M \otimes N)^*$.
b) If M or N is finite dimensional, then ρ is bijective.
Solution: a) We prove that $(Im(\rho))^{\perp} = \{0\}$. Let $z = \sum_{i=1}^{n} x_i \otimes y_i \in M \otimes N$ be such that $z \in (Im(\rho))^{\perp}$. Hence for any $f \in M^*$, $g \in N^*$ we have

$$\rho(f \otimes g)(\sum_{i=1}^{n} x_i \otimes y_i) = \sum_{i=1}^{n} f(x_i)g(y_i) = 0. \tag{1.3}$$

We can assume that $\{y_i \mid 1 \leq i \leq n\}$ are linearly independent. There exists a $g \in N^*$ such that $g(y_i) \neq 0$ and $g(y_j) = 0$ for $j \neq i$. From (1.3) it follows that $f(x_i) = 0$ for every $f \in M^*$, thus $x_i = 0$. Since $i \in \{1, \dots, n\}$ is arbitrary, we have that $z = 0$.
b) Assume that N is finite dimensional. By induction we can assume that $N \simeq k$ (i.e. $dim_k(N) = 1$). In this case $N^* \simeq k$, and so $M^* \otimes N^* \simeq M^* \otimes k \simeq M^*$. Also $(M \otimes N)^* \simeq (M \otimes k)^* \simeq M^*$.

Exercise 1.3.11 *Let $A = M_n(k)$ be the algebra of $n \times n$ matrices. Then the dual coalgebra of A is isomorphic to the matrix coalgebra $M^c(n, k)$.*
Solution: If $(e_{ij})_{1 \leq i,j \leq n}$ is the usual basis of $M_n(k)$ (e_{ij} is the matrix having 1 on position (i, j) and 0 elsewhere), let $(e_{ij}^*)_{1 \leq i,j \leq n}$ be the dual basis of A^*. We recall that $e_{ij}e_{pq} = \delta_{jp}e_{iq}$ for any i, j, p, q. Then Remark 1.3.10 shows that

$$\begin{aligned}
\Delta(e_{ij}^*) &= \sum_{1 \leq p,q,r,s \leq n} e_{ij}^*(e_{pq}e_{rs})e_{pq}^* \otimes e_{rs}^* \\
&= \sum_{1 \leq p,q,s \leq n} e_{ij}^*(e_{ps})e_{pq}^* \otimes e_{qs}^* \\
&= \sum_{1 \leq q \leq n} e_{iq}^* \otimes e_{qj}^*
\end{aligned}$$

and clearly

$$\varepsilon(e^*_{ij}) = e^*_{ij}(1_A) = e^*_{ij}(\sum_{1\leq q\leq n} e_{qq}) = \delta_{ij}$$

We have obtained that A^* is isomorphic to $M^c(n,k)$.

Exercise 1.4.4 *Show that if I is a coideal it does not follow that I is a left or right coideal.*
Solution: Let $k[X]$ be the polynomial ring, which is a coalgebra by

$$\Delta(X^n) = (X\otimes 1 + 1\otimes X)^n, \quad \varepsilon(X^n) = 0 \quad \text{for } n \geq 1$$

$$\Delta(1) = 1\otimes 1, \quad \varepsilon(1) = 1$$

Take $I = kX$, the subspace spanned by X.

Exercise 1.4.12 *Show that the category $k - Cog$ has coequalizers, i.e. if $f, g : C \to D$ are two morphisms of coalgebras, there exists a coalgebra E and a morphism of coalgebras $h : D \to E$ such that $h\circ f = h\circ g$.*
Solution: We show that $I = Im(f-g)$ is a coideal of D, then take $E = D/I$ and h the canonical projection. If $d\in I$, then we have $d = (f-g)(c)$ for some $c\in C$, and

$$\begin{aligned}
\Delta(d) &= \Delta(f(c)) - \Delta(g(c)) \\
&= \sum f(c)_1\otimes f(c)_2 - \sum g(c)_1\otimes g(c)_2 \\
&= \sum (f(c_1)\otimes f(c_2) - g(c_1)\otimes g(c_2)) \\
&= \sum (f(c_1)\otimes f(c_2) - f(c_1)\otimes g(c_2) + \\
&\quad + f(c_1)\otimes g(c_2) - g(c_1)\otimes g(c_2)) \\
&= \sum f(c_1)\otimes (f-g)(c_2) + \sum (f-g)(c_1)\otimes g(c_2) \in \\
&\quad \in D\otimes I + I\otimes D.
\end{aligned}$$

Exercise 1.4.16 *Let S be a set, and kS the grouplike coalgebra (see Example 1.1.4, 1). Show that $G(kS) = S$.*
Solution: Let $g = \sum a_i s_i \in G(kS)$. Then $\Delta(g) = g\otimes g$ becomes

$$\sum_i a_i s_i\otimes s_i = \sum_{i,j} a_i a_j s_i\otimes s_j. \tag{1.4}$$

If k and l are such that $k\neq l$ and $a_k\neq 0$, $a_l\neq 0$, let g_k and g_l be the functions from k^S defined by $g_r(s) = \delta_{s,s_r}$ for $r\in\{k,l\}$. Applying $g_k\otimes g_l$

to both sides of (1.4) we obtain $0 = a_k a_l$, a contradiction. Thus $g = as$ for some $a \in k$ and $s \in S$. From $\varepsilon(g) = 1$ we obtain $g \in S$. The converse inclusion is clear.

Exercise 1.4.18 *Check directly that there are no grouplike elements in $M^c(n,k)$ if $n > 1$.*
Solution: Let $x \in M^c(n,k)$ be a grouplike, $x = \sum\limits_{i,j} a_{ij} e_{ij}$. Then we have $\Delta(x) = x \otimes x$, i.e.

$$\sum_{i,j,k} a_{ij} e_{ik} \otimes e_{kj} = \sum_{i,j,k,l} a_{ij} a_{kl} e_{ij} \otimes e_{kl}.$$

Let $i_0 \neq j_0$, and $f \in M^c(n,k)^*$ such that $f(e_{ij}) = \delta_{ii_0}\delta_{jj_0}$. Applying $f \otimes f$ to the equality above, we get $0 = a_{i_0 j_0}^2$, hence $a_{i_0 j_0} = 0$. If $g \in M^c(n,k)^*$ is such that $g(e_{ij}) = \delta_{ij_0}\delta_{ji_0}$, and we apply $f \otimes g$ to the same equality, we get $a_{i_0 i_0} = a_{i_0 j_0} a_{j_0 i_0} = 0$. Since i_0 and j_0 were arbitrarily chosen, it follows that $x = 0$, a contradiction.

Exercise 1.5.11 *Let G be a group, and $\rho : G \to GL_n(k)$ a representation of G. If we denote $\rho(x) = (f_{ij}(x))_{i,j}$, let $V(\rho)$ be the k-subspace of k^G spanned by the $\{f_{ij}\}_{i,j}$. Then the following assertions hold:*
i) $V(\rho)$ is a finite dimensional subbimodule of k^G.
ii) $R_k(G) = \sum\limits_{\rho} V(\rho)$, where ρ ranges over all finite dimensional representations of G.
Solution: i) Let $f \in V(\rho)$, and $y \in G$. If $f = \sum a_{ij} f_{ij}$, then

$$(yf)(x) = \sum a_{ij} f_{ij}(xy) = \sum a_{ij} f_{ik}(x) g_{kj}(y),$$

because

$$\rho(xy) = (f_{ij}(xy))_{i,j} = \rho(x)\rho(y) = (\sum f_{ik}(x) g_{kj}(y))_{i,j}.$$

Thus $yf = \sum a_{ij} g_{kj} f_{ik} \in V(\rho)$. The proof of $fy \in V(\rho)$ is similar.
ii) ($\supseteq$) follows from i). In order to prove the reverse inclusion, let $f \in R_k(G)$. Then the left kG-submodule generated by f is finite dimensional, say with basis $\{f_1, \ldots, f_n\}$. Write

$$xf_i = \sum g_{ij}(x) f_j.$$

Then

$$\rho : G \to GL_n(k), \quad \rho(x) = (g_{ij}(x))_{i,j}$$

is a representation of G, $V(\rho)$ is spanned by the g_{ij}'s, and we obtain that $f_i = \sum f_j(1_G) g_{ij} \in V(\rho)$, thus $f \in V(\rho)$ too.

Exercise 1.5.14 *The coalgebra C is coreflexive if and only if every ideal of finite codimension in C^* is closed in the finite topology.*
Solution: By Exercise 1.2.15, we have to prove that ϕ_C is surjective if and only if for all finite codimensional ideals I of C^* we have $I^{\perp} = I^{\tilde{\perp}}$.
($\Rightarrow$) Let I be a finite codimensional ideal of C^*. If $\mu \in I^{\tilde{\perp}}$, then the restriction of μ to I is zero, and hence $\mu \in C^{*0}$. Since ϕ_C is surjective, it follows that $\mu \in I^{\perp}$. Thus $I^{\perp} = I^{\tilde{\perp}}$.
($\Leftarrow$) Let $\mu \in C^{*0}$. By definition, there exists an ideal I of C^*, of finite codimension, such that $\mu \mid_I = 0$. It follows that $\mu \in I^{\tilde{\perp}} = \phi_C(I^{\perp})$, hence ϕ_C is surjective.

Exercise 1.5.15 *Give another proof for Proposition 1.5.3 using the representative coalgebra. Deduce that any coalgebra is a subcoalgebra of a representative coalgebra.*
Solution: If we take $c \in C$, $\Delta(c) = \sum c_1 \otimes c_2$, and regard the elements of C as functions on C^* via ϕ_C, then for $f, g \in C^*$ we have

$$c(f * g) = (f * g)(c) = \sum f(c_1)g(c_2) = \sum c_1(f)c_2(g).$$

This shows that the elements of C are representative functions on C^*, and ϕ_C is a coalgebra map.

Exercise 1.5.17 *If C is a coalgebra, show that C is cocommutative if and only if C^* is commutative.*
Solution: If C is cocommutative, then for any $f, g \in C^*$ and $c \in C$ we have $(f*g)(c) = \sum f(c_1)g(c_2) = \sum f(c_2)g(c_1) = (g*f)(c)$, so C^* is commutative. Conversely, if C^* is commutative, then C^{*0} is cocommutative, and the assertion follows from the fact that C is isomorphic to a subcoalgebra of C^{*0}.

Exercise 1.5.19 *If A is an algebra, then the algebra map $i_A : A \to A^{0*}$ defined by $i_A(a)(a^*) = a^*(a)$ for any $a \in A, a^* \in A^0$, is not injective in general.*
Solution: If A is the algebra from Remark 1.5.7.2), then $A^{0*} = 0$.

Exercise 1.5.21 *If A is a k-algebra, the following assertions are equivalent:*
a) A is proper.
b) A^0 is dense in A^* in the finite topology.
c) The intersection of all ideals of finite codimension in A is zero.
Solution: By Corollary 1.2.9, we know that A^0 is dense in A^* if and only if $(A^0)^{\perp} = \{0\}$. But

$$(A^0)^{\perp} = \{a \in A \mid f(a) = 0, \forall f \in A^0\} = Ker(i_A).$$

Thus a)$\Leftrightarrow$b).
Denote by $\mathcal{F}$ the set of finite codimensional ideals of A. Then, by the definition we have that $A^\circ = \bigcup_{I\in\mathcal{F}} I^\perp$. But then

$$(A^\circ)^\perp = (\bigcup_{I\in\mathcal{F}} I^\perp)^\perp = \bigcap_{I\in\mathcal{F}} I^{\perp\perp} = \bigcap_{I\in\mathcal{F}} I,$$

hence we also have b)$\Leftrightarrow$c).

Exercise 1.6.2 *Show that if (C,p) is a cofree coalgebra over the k-vector space V, then p is surjective.*
Solution: We know that V can be endowed with a coalgebra structure (see Example 1.1.4, 1). Apply then the definition to the identity map from V to V in order to obtain a right inverse for p.

Exercise 1.6.10 *Show that if (C,p) is a cocommutative cofree coalgebra over the k-vector space V, then p is surjective.*
Solution: The coalgebra in Example 1.1.4, 1 is cocommutative, so the proof is the same as for Exercise 1.6.2.

Bibliographical notes

Our main sources of inspiration for this chapter were the books of M. Sweedler [218], E. Abe [1], and S. Montgomery [149], P. Gabriel's paper [85], B. Pareigis' notes [178], and F.W. Anderson and K. Fuller [3] for module theoretical aspects. Further references are R. Wisbauer [244], I. Kaplansky [104], Heyneman and Radford [95]. It should be remarked that we are dealing only with coalgebras over fields, but in some cases coalgebras over rings may also be considered. This is the case in [244], [145] or [88].

Chapter 2

Comodules

2.1 The category of comodules over a coalgebra

In the same way as in the first chapter, where we gave an alternative definition for an algebra, using only morphisms and diagrams, we begin this chapter by defining in a similar way modules over an algebra. Let then (A, M, u) be a k-algebra.

Definition 2.1.1 *A left* A-module *is a pair* (X, μ)*, where* X *is a* k*-vector space, and* $\mu : A \otimes X \longrightarrow X$ *is a morphism of* k*-vector spaces such that the following diagrams are commutative:*

$$\begin{tikzcd} A \otimes A \otimes X \arrow[r, "I \otimes \mu"] \arrow[d, "M \otimes I"'] & A \otimes X \arrow[d, "\mu"] \\ A \otimes X \arrow[r, "\mu"] & X \end{tikzcd} \qquad \begin{tikzcd} & A \otimes X \arrow[d, "\mu"] \\ k \otimes X \arrow[ur, "\varepsilon \otimes I"] \arrow[r, "\sim"'] & X \end{tikzcd}$$

(We denote everywhere by I *the identity maps, and the not named arrow from the second diagram is the canonical isomorphism.)* ∎

Remark 2.1.2 *Similarly, one can define right modules over the algebra* A*, the only difference being that the structure map of the right module* X *is of the form* $\mu : X \otimes A \to X$. ∎

By dualization we obtain the notion of a comodule over a coalgebra. Let then (C, Δ, ε) be a k-coalgebra.

Definition 2.1.3 *We call a right C-*comodule *a pair (M, ρ), where M is a k-vector space, $\rho : M \longrightarrow M \otimes C$ is a morphism of k-vector spaces such that the following diagrams are commutative:*

$$\begin{tikzcd} M \arrow[r, "\rho"] \arrow[d, "\rho"'] & M \otimes C \arrow[d, "I \otimes \Delta"] \\ M \otimes C \arrow[r, "\rho \otimes I"] & M \otimes C \otimes C \end{tikzcd} \qquad \begin{tikzcd} M \arrow[rd, "\sim"] \arrow[d, "\rho"] & \\ M \otimes C \arrow[r, "I \otimes \varepsilon"'] & M \otimes k \end{tikzcd}$$ ∎

Remark 2.1.4 *Similarly, one can define left comodules over a coalgebra C, the difference being that the structure map of a left C-comodule M is of the form $\rho : M \to C \otimes M$. The conditions that ρ must satisfy are $(\Delta \otimes I)\rho = (I \otimes \rho)\rho$ and $(\varepsilon \otimes I)\rho$ is the canonical isomorphism.* ∎

2.1.5 The sigma notation for comodules. *Let M be a right C-comodule, with structure map $\rho : M \to M \otimes C$. Then for any element $m \in M$ we denote*

$$\rho(m) = \sum m_{(0)} \otimes m_{(1)}$$

the elements on the first tensor position (the $m_{(0)}$'s) being in M, and the elements on the second tensor position (the $m_{(1)}$'s) being in C.
If M is a left C-comodule with structure map $\rho : M \to C \otimes M$, we denote

$$\rho(m) = \sum m_{(-1)} \otimes m_{(0)}.$$

The definition of a right comodule may be written now using the sigma notation as the following equalities:

$$\sum (m_{(0)})_{(0)} \otimes (m_{(0)})_{(1)} \otimes m_{(1)} = \sum m_{(0)} \otimes (m_{(1)})_1 \otimes (m_{(1)})_2$$

$$\sum \varepsilon(m_{(1)}) m_{(0)} = m.$$

The first formula allows us to extend the sigma notation, as in the case of coalgebras, by writing

$$\sum m_{(0)} \otimes m_{(1)} \otimes m_{(2)} = \sum (m_{(0)})_{(0)} \otimes (m_{(0)})_{(1)} \otimes m_{(1)} =$$

$$= \sum m_{(0)} \otimes (m_{(1)})_1 \otimes (m_{(1)})_2.$$

The rules for computing with the sigma notation, which were presented in detail in the first chapter, may be easily transferred to comodules. Thus, we can write for any $n \geq 2$

$$\sum m_{(0)} \otimes m_{(1)} \otimes \ldots \otimes m_{(n)} = \sum \rho(m_{(0)}) \otimes m_{(1)} \otimes \ldots \otimes m_{(n-1)},$$

and for any $1 \leq i \leq n-1$ we have

$$\sum m_{(0)} \otimes m_{(1)} \otimes \ldots \otimes m_{(n)} =$$

$$= \sum m_{(0)} \otimes m_{(1)} \otimes \ldots \otimes m_{(i-1)} \otimes \Delta(m_{(i)}) \otimes m_{(i+1)} \otimes \ldots \otimes m_{(n-1)}.$$

For left C-comodules, the sigma notation is the following: if $\rho : M \to C \otimes M$ is the map defining the comodule structure, then we denote $\rho(m) = \sum m_{(-1)} \otimes m_{(0)}$ for any $m \in M$, where this time $m_{(-1)}$ are representing elements of C, and $m_{(0)}$ elements in M.
Later we will omit the brackets, because even if the sigma notation for comodules will be used in the same time as the one for coalgebras, confusion can always be avoided.
The definition of the left comodule may be written using the sigma notation as the following equalities:

$$\sum m_{(-1)} \otimes (m_{(0)})_{(-1)} \otimes (m_{(0)})_{(0)} = \sum (m_{(-1)})_1 \otimes (m_{(-1)})_2 \otimes m_{(0)}$$

$$\sum \varepsilon(m_{(-1)}) m_{(0)} = m$$

Also

$$\sum m_{(-n)} \otimes m_{(-n+1)} \otimes \ldots \otimes m_{(0)} = \sum m_{(-n)} \otimes m_{(-n+1)} \otimes \ldots \otimes \rho(m_{(0)}) =$$

$$= \sum m_{(-n)} \otimes m_{(-n+1)} \otimes \ldots \otimes m_{(-i-1)} \otimes \Delta(m_{(-i)}) \otimes m_{(-i+1)} \otimes \ldots \otimes m_{(0)}$$

for any $1 \leq i \leq n$.

Example 2.1.6 *1) A coalgebra C is a left and right comodule over itself, the map giving the comodule structure being in both cases the comultiplication $\Delta : C \to C \otimes C$.*
2) If C is a coalgebra and X is a k-vector space, then $X \otimes C$ becomes a right C-comodule with structure map $\rho : X \otimes C \to X \otimes C \otimes C$ induced by Δ, hence $\rho = I \otimes \Delta$. Thus $\rho(x \otimes c) = \sum x \otimes c_1 \otimes c_2$.

3) Let S be a non-empty set, and $C = kS$, the k-vector space with basis S, endowed with a coalgebra structure as in Example 1.1.4,1). Let $(M_s)_{s\in S}$ be a family of k-vector spaces, and $M = \oplus_{s\in S} M_s$. Then M is a right C-comodule, where the structure map $\rho : M \to M \otimes C$ is defined by $\rho(m_s) = m_s \otimes s$ for any $s \in S$ and $m_s \in M_s$ (extended by linearity). ∎

The following result is the analog for comodules of Theorem 1.4.7.

Theorem 2.1.7 *(The Fundamental Theorem of Comodules) Let V be a right C-comodule. Any element $v \in V$ belongs to a finite dimensional subcomodule.*

Proof: Let $\{c_i\}_{i\in I}$ be a basis for C, denote by $\rho : V \to V\otimes C$ the comodule structure map, choose $v \in V$, and write

$$\rho(v) = \sum v_i \otimes c_i,$$

where almost all of the v_i's are zero. Then the subspace W generated by the v_i's is finite dimensional. We have

$$\Delta(c_i) = \sum a_{ijk} c_j \otimes c_k,$$

and

$$\sum \rho(v_i) \otimes c_i = \sum v_i \otimes a_{ijk} c_j \otimes c_k.$$

Cosequently, $\rho(v_k) = \sum v_i \otimes a_{ijk} c_j$, so W is a finite dimensional subcomodule, and $v = (I \otimes \varepsilon)\rho(v) \in W$. ∎

Exercise 2.1.8 *Use Theorem 2.1.7 to prove Theorem 1.4.7.*

We define now the morphisms of comodules. In order to keep to dualizing the corresponding definitions from the case of modules, we also give the definition of a module morphism using commutative diagrams.

Definition 2.1.9 *i) Let A be a k-algebra, and $(X, \nu), (Y, \mu)$ two left A-modules. The k-linear map $f : X \longrightarrow Y$ is called a morphism of A-modules if the following diagram is commutative:*

$$\begin{tikzcd} A \otimes X \arrow[r, "I \otimes f"] \arrow[d, "\nu"'] & A \otimes Y \arrow[d, "\mu"] \\ X \arrow[r, "f"] & Y \end{tikzcd}$$

ii) Let C be a k-coalgebra, and $(M,\rho),(N,\phi)$ two right C-comodules. The k-linear map $g : M \longrightarrow N$ is called a morphism of C-comodules if the following diagram is commutative

$$\begin{tikzcd} M \arrow[r, "g"] \arrow[d, "\rho"'] & N \arrow[d, "\phi"] \\ M \otimes C \arrow[r, "g \otimes I"] & N \otimes C \end{tikzcd}$$

The commutativity of the second diagram may be written in the sigma notation as:

$$\phi(g(c)) = \sum g(c_{(0)}) \otimes c_{(1)}.$$

■

We can now define *the category of right comodules* over the coalgebra C. The objects are all right C-comodules, and the morphisms between two objects are the morphisms of comodules. We denote this category by $\mathcal{M}^C$. We will also denote the morphisms in $\mathcal{M}^C$ from M to N by $Com_C(M,N)$. Similarly, the category of left C-comodules will be denoted by ${}^C\mathcal{M}$. For an algebra A, the category of left (resp. right) A-modules will be denoted by ${}_A\mathcal{M}$ (resp. $\mathcal{M}_A$).

Proposition 2.1.10 *Let C be a coalgebra. Then the categories ${}^C\mathcal{M}$ and $\mathcal{M}^{C^{cop}}$ are isomorphic.*

Proof: Let $M \in {}^C\mathcal{M}$ with the comodule structure given by the map $\rho : M \to C \otimes M$, $\rho(m) = \sum m_{(-1)} \otimes m_{(0)}$. Then M becomes a right comodule over the co-opposite coalgebra C^{cop} via the map $\rho' : M \to M \otimes C^{cop}$, $\rho'(m) = \sum m_{(0)} \otimes m_{(-1)}$. Moreover, it is immediate that if M and N are two left C-comodules, and $f : M \to N$ is a morphism of left C-comodules, then f is also a morphism of right C^{cop}-comodules when M and N are regarded with these structures. This defines a functor $F : {}^C\mathcal{M} \to \mathcal{M}^{C^{cop}}$. Similarly, we can define a functor $G : \mathcal{M}^{C^{cop}} \to {}^C\mathcal{M}$, by associating to a right C^{cop}-comodule M, with structure map $\mu : M \to M \otimes C^{cop}$, $\mu(m) = \sum m_{(0)} \otimes m_{(1)}$, a left C-comodule structure on M defined by $\mu' : M \to C \otimes M$, $\mu'(m) = \sum m_{(1)} \otimes m_{(0)}$. It is clear that the functors F and G define an isomorphism of categories. ■

Remark 2.1.11 *The preceding proposition shows that any result that we obtain for right comodules has an analogue for left comodules. This is why we are going to work generally with right comodules, without explicitely mentioning the similar results for left comodules.* ∎

We define now the notions of subobject and factor object in the category $\mathcal{M}^C$.

Definition 2.1.12 *Let (M,ρ) be a right C-comodule. A k-vector subspace N of M is called a right C-subcomodule if $\rho(N) \subseteq N \otimes C$.* ∎

Remark 2.1.13 *If N is a subcomodule of M, then (N,ρ_N) is a right C-comodule, where $\rho_N : N \to N \otimes C$ is the restriction and corestriction of ρ to N and $N \otimes C$. Moreover, the inclusion map $i : N \to M, i(n) = n$ for any $n \in N$ is a morphism of comodules.* ∎

Let now (M,ρ) be a right C-comodule, and N a C-subcomodule of M. Let M/N be the factor vector space, and $p : M \to M/N$ the canonical projection, $p(m) = \overline{m}$, where by $\overline{m}$ we denote the coset of $m \in M$ in the factor space.

Proposition 2.1.14 *There exists a unique structure of a right C-comodule on M/N for which $p : M \to M/N$ is a morphism of C-comodules.*

Proof: Since $(p\otimes I)\rho(N) \subseteq (p \otimes I)(N \otimes C) \subseteq p(N) \otimes C = 0$, by the universal property of the factor vector space it follows that there exists a unique morphism of vector spaces $\overline{\rho} : M/N \to M/N \otimes C$ for which the diagram

$$\begin{array}{ccc} M & \xrightarrow{p} & M/N \\ \rho \downarrow & & \downarrow \overline{\rho} \\ M \otimes C & \xrightarrow{p \otimes I} & M/N \otimes C \end{array}$$

is commutative. This map is defined by $\overline{\rho}(\overline{m}) = \sum \overline{m_{(0)}} \otimes m_{(1)}$ for any $m \in M$. Then $(M/N, \overline{\rho})$ is a right C-comodule, since

$$(I \otimes \Delta)\overline{\rho}(\overline{m}) = \sum \overline{m_{(0)}} \otimes m_{(1)} \otimes m_{(2)} = (\overline{\rho} \otimes I)\overline{\rho}(\overline{m})$$

The fact that $\overline{\rho}$ is a morphism of comodules follows immediately from the commutativity of the diagram.

If we would have a right C-comodule structure on M/N given by $\omega : M/N \to M/N \otimes C$ such that p is a morphism of comodules, then the diagram obtained by replacing $\overline{\rho}$ by ω in the above diagram should be also commutative. But then it would follow that $\omega = \overline{\rho}$ from the universal property of the factor vector space. ∎

Remark 2.1.15 *The comodule M/N, with the structure given as in the above proposition, is called the factor comodule of M with respect to the subcomodule N.* ∎

Proposition 2.1.16 *Let M and N be two right C-comodules, and $f : M \to N$ a morphism of C-comodules. Then $Im(f)$ is a C-subcomodule of N and $Ker(f)$ is a C-subcomodule of M.*

Proof: We denote by $\rho_M : M \to M \otimes C$ and $\rho_N : N \to N \otimes C$ the maps giving the comodule structures. Since f is a morphism of comodules, we have $(f \otimes I)\rho_M = \rho_N f$. Then

$$(f \otimes I)\rho_M(Ker(f)) = \rho_N f(Ker(f)) = 0,$$

which shows that $\rho_M(Ker(f)) \subseteq Ker(f \otimes I) = Ker(f) \otimes C$, and hence $Ker(f)$ is a C-subcomodule of M.
Now

$$\rho_N(Im(f)) = (f \otimes I)\rho_M(m) \subseteq Im(f) \otimes C,$$

which shows that $Im(f)$ is a C-subcomodule of N. ∎

Theorem 2.1.17 *(The fundamental isomorphism theorem for comodules) Let $f : M \to N$ be a morphism of right C-comodules, $p : M \to M/Ker(f)$ the canonical projection, and $i : Im(f) \to N$ the inclusion. Then there exists a unique isomorphism $\overline{f} : M/Ker(f) \to Im(f)$ of C-comodules for which the diagram*

$$\begin{tikzcd}
M \arrow[r, "f"] \arrow[d, "p"'] & N \\
M/Ker(f) \arrow[r, "\overline{f}"] & Im(f) \arrow[u, "i"']
\end{tikzcd}$$

is commutative.

Proof: The existence of a unique morphism $\overline{f} : M/Ker(f) \to Im(f)$ of vector spaces making the diagram commutative follows from the fundamental isomorphism theorem for k-vector spaces. We know that $\overline{f}$ is defined by $\overline{f}(\overline{m}) = f(m)$ for any $\overline{m} \in M/Ker(f)$. It remains to show that $\overline{f}$ is a morphism of comodules. Denoting by $\omega : M/Ker(f) \to M/Ker(f) \otimes C$ and $\theta : Im(f) \to Im(f) \otimes C$ the maps giving the comodule structures, we have

$$\begin{aligned}
(\overline{f} \otimes I)\omega(\overline{m}) &= \sum \overline{f}(\overline{m_{(0)}}) \otimes m_{(1)} \\
&= \sum f(m_{(0)}) \otimes m_{(1)} \\
&= \sum f(m)_{(0)} \otimes f(m)_{(1)} \\
&= \theta(f(m)) \\
&= \theta\overline{f}(\overline{m})
\end{aligned}$$

which shows that $\overline{f}$ is a morphism of comodules. ∎

Proposition 2.1.18 *Let C be a coalgebra. Then the category $\mathcal{M}^C$ has coproducts.*

Proof: Let $(M_i)_{i\in I}$ be a family of right C-comodules, with structure maps $\rho_i : M_i \to M_i \otimes C$. Let $\oplus_{i\in I}M_i$ be the direct sum of this family in ${}_k\mathcal{M}$, and $q_j : M_j \to \oplus_{i\in I}M_i$ the canonical injections. Then there exists a unique morphism ρ in ${}_k\mathcal{M}$ such that the diagram

$$\begin{tikzcd}
M_j \arrow[r, "q_j"] \arrow[d, "\rho_j"'] & \oplus_{i\in I}M_i \arrow[d, "\rho"] \\
M_j \otimes C \arrow[r, "q_j \otimes I"] & (\oplus_{i\in I}M_i) \otimes C
\end{tikzcd}$$

is commutative. It is easy to check that $(\oplus_{i\in I}M_i, \rho)$ is a right C-comodule, and moreover that this comodule is the coproduct of the family $(M_i)_{i\in I}$ in the category $\mathcal{M}^C$. ∎

Corollary 2.1.19 *The category $\mathcal{M}^C$ is abelian.* ∎

2.2 Rational modules

Let C be a coalgebra, and C^* the dual algebra. If M is a k-vector space, and $\omega : M \to M \otimes C$ is a k-linear map, we define $\psi_\omega : C^* \otimes M \to M$ by

$\psi_\omega = \phi(\gamma \otimes I_M)(I_{C^*} \otimes T)(I_{C^*} \otimes \omega)$, where I_M and I_{C^*} are the identity maps, $T : M \otimes C \to C \otimes M$ is defined by $T(m \otimes c) = c \otimes m$, $\gamma : C^* \otimes C \to k$ is defined by $\gamma(c^* \otimes c) = c^*(c)$, and $\phi : k \otimes M \to M$ is the canonical isomorphism. If $\omega(m) = \sum_i m_i \otimes c_i$, then $\psi_\omega(c^* \otimes m) = \sum_i c^*(c_i)m_i$.

Proposition 2.2.1 *(M, ω) is a right C-comodule if and only if (M, ψ_ω) is a left C^*-module.*

Proof: Assume that (M, ω) is a right C-comodule. Denoting by $c^* \cdot m = \psi_\omega(c^* \otimes m)$, we have $c^* \cdot m = \sum c^*(m_{(1)})m_{(0)}$ for any $c^* \in C^*, m \in M$. First, we have that

$$1_{C^*} \cdot m = \varepsilon \cdot m = \sum \varepsilon(m_{(1)})m_{(0)} = m$$

from the definition of a comodule. Then, for $c^*, d^* \in C^*$ and $m \in M$

$$\begin{aligned} c^* \cdot (d^* \cdot m) &= c^* \cdot (\sum d^*(m_{(1)})m_{(0)}) \\ &= \sum d^*(m_{(1)})(c^* \cdot m_{(0)}) \\ &= \sum d^*(m_{(1)})c^*((m_{(0)})_{(1)})(m_{(0)})_{(0)} \\ &= \sum d^*(m_{(2)})c^*(m_{(1)})m_{(0)} \\ &= \sum (c^*d^*)(m_{(1)})m_{(0)} \\ &= (c^*d^*) \cdot m \end{aligned}$$

which shows that (M, ψ_ω) is a left C^*-module.

Assume now that (M, ψ_ω) is a left C^*-module. We denote $\omega(m) = \sum m_{(0)} \otimes m_{(1)}$. From $\varepsilon \cdot m = m$ it follows that $\sum \varepsilon(m_{(1)})m_{(0)} = m$, hence the second condition from the definition of a comodule is checked. If $c^*, d^* \in C^*, m \in M$, then

$$\begin{aligned} (c^*d^*) \cdot m &= \sum (c^*d^*)(m_{(1)})m_{(0)} \\ &= \sum c^*((m_{(1)})_1)d^*((m_{(1)})_2)m_{(0)} \\ &= \phi'(I \otimes c^* \otimes d^*)(I \otimes \Delta)\omega(m) \end{aligned}$$

where $\phi' : M \otimes k \otimes k \to M$ is the canonical isomorphism, and I stands everywhere for the suitable identity map. Also

$$\begin{aligned} c^* \cdot (d^* \cdot m) &= c^* \cdot (\sum d^*(m_{(1)})m_{(0)}) \\ &= \sum d^*(m_{(1)})(c^* \cdot m_{(0)}) \\ &= \sum d^*(m_{(1)})c^*((m_{(0)})_{(1)})(m_{(0)})_{(0)} \\ &= \phi'(I \otimes c^* \otimes d^*)(\omega \otimes I)\omega(m) \end{aligned}$$

Denoting

$$y = (I \otimes \Delta)\omega(m) - (\omega \otimes I)\omega(m) \in M \otimes C \otimes C$$

we have $(I \otimes c^* \otimes d^*)(y) = 0$ for any $c^*, d^* \in C^*$. This shows that $y = 0$. Indeed, if we denote by $(e_i)_i$ a basis of C, we can write $y = \sum_{i,j} m_{ij} \otimes e_i \otimes e_j$ for some $m_{ij} \in M$. Fix i_0 and j_0 and consider the maps $e_i^* \in C^*$ defined by $e_i^*(e_j) = \delta_{i,j}$ for any j. Then $m_{i_0 j_0} = (I \otimes e_{i_0}^* \otimes e_{j_0}^*)(y) = 0$, and from this we get that $y = 0$. ∎

Let now M be a left C^*-module, and $\psi_M : C^* \otimes M \to M$ the map giving the module structure of M. We define

$$\rho_M : M \to Hom(C^*, M), \rho_M(m)(c^*) = c^* m.$$

Let $j : C \to C^{**}$, $j(c)(c^*) = c^*(c)$ be the canonical embedding, and

$$f_M : M \otimes C^{**} \to Hom(C^*, M), f_M(m \otimes c^{**})(c^*) = c^{**}(c^*)m,$$

which is an injective morphism. It follows that the map

$$\mu_M : M \otimes C \to Hom(C^*, M), \mu_M = f_M(I \otimes j)$$

is injective. It is clear from the definition that $\mu_M(m \otimes c)(c^*) = c^*(c)m$ for $c \in C, c^* \in C^*, m \in M$.

Definition 2.2.2 *The left C^*-module M is called* rational *if*

$$\rho_M(M) \subseteq \mu_M(M \otimes C)$$

∎

Remark 2.2.3 *1) M is a rational C^*-module if and only if for any $m \in M$ there exist two finite families of elements $(m_i)_i \subseteq M$ and $(c_i)_i \subseteq C$ such that $c^* m = \sum_i c^*(c_i) m_i$ for any $c^* \in C^*$.*
2) If M is a rational C^*-module, and for an element $m \in M$ there exist two pairs of families $(m_i)_i, (c_i)_i$ and $(m'_j)_j, (c'_j)_j$ as in 1), then $\sum_i m_i \otimes c_i = \sum_j m'_j \otimes c'_j$, since $\mu_M(\sum_i m_i \otimes c_i) = \mu_M(\sum_j m'_j \otimes c'_j)$ and μ_M is injective.
∎

Example 2.2.4 *If C is a finite dimensional coalgebra, then the left C^*-module C^* is rational. Indeed, in this situation $j : C \to C^{**}$ is an isomorphism of vector spaces from Proposition 1.3.14, and $f_{C^*} : C^* \otimes C^{**} \to Hom(C^*, C^*)$ is an isomorphism of vector spaces by Lemma 1.3.2.i). It follows that $\mu_{C^*}(C^* \otimes C) = Hom(C^*, C^*)$, and hence $\rho_{C^*}(C^*) \subseteq \mu_{C^*}(C^* \otimes C)$, which shows that C^* is rational.* ∎

We will denote by $Rat(_{C^*}\mathcal{M})$ the full subcategory of $_{C^*}\mathcal{M}$ having as objects all rational C^*-modules.

Theorem 2.2.5 *The categories $\mathcal{M}^C$ and $Rat(_{C^*}\mathcal{M})$ are isomorphic.*

Proof: Let (M, ω) be a right C-comodule. We show that (M, ψ_ω) is a rational C^*-module. Let $m \in M$. Then from the definition of ψ_ω it follows that $c^* \cdot m = \sum c^*(m_{(1)})m_{(0)}$, and then M is a rational module by the preceding remark.
Let now M and N be two right C-comodules, and $f : M \to N$ a morphism of comodules. We show that if we regard M and N with the left C^*-module structures, f is a morphism of C^*-modules. Indeed, for $m \in M$ and $c^* \in C^*$ we have

$$\begin{aligned} f(c^* \cdot m) &= f(\sum c^*(m_{(1)})m_{(0)}) \\ &= \sum c^*(m_{(1)})f(m_{(0)}) \\ &= \sum c^*(f(m)_{(1)})f(m)_{(0)} \\ &= c^* \cdot f(m) \end{aligned}$$

In this way we have defined a functor $T : \mathcal{M}^C \to Rat(_{C^*}\mathcal{M})$, such that $T(M, \omega) = (M, \psi_\omega)$ for any C-comodule (M, ω), and $T(f) = f$ for any morphism of C-comodules $f : M \to N$.
Let now (M, ψ) be a rational left C^*-module. Since $\mu_M : M \otimes C \to Hom(C^*, M)$ is an injective map, it follows that $\tilde{\mu}_M : M \otimes C \to \mu_M(M \otimes C)$, the corestriction of μ_M, is an isomorphism of vector spaces. We define

$$\omega_\psi : M \to M \otimes C, \quad \omega_\psi(m) = \tilde{\mu}_M^{-1}(\rho_M(m)).$$

We remark that for $m \in M$ we have $\omega_\psi(m) = \sum_i m_i \otimes c_i$, where $(m_i)_i, (c_i)_i$ are two families of elements in M, respectively C, such that

$$c^* m = \sum_i c^*(c_i) m_i$$

for any $c^* \in C^*$. We show that (M, ω_ψ) is a right C-comodule. For this we consider the map $\omega_\psi : M \to M \otimes C$, and we show that $\psi_{(\omega_\psi)} = \psi$. Then (M, ω_ψ) will be a C-comodule by Proposition 2.2.1 and due to the fact that (M, ψ) is a C^*-module.
Let then $\omega_\psi(m) = \sum_i m_i \otimes c_i$. We have $\tilde{\mu}_M^{-1}(\rho_M(m)) = \sum_i m_i \otimes c_i$, hence

$$\rho_M(m) = \sum_i \tilde{\mu}_M(m_i \otimes c_i) = \sum_i \mu_M(m_i \otimes c_i)$$

By evaluation in c^* we obtain that $c^* \cdot m = \sum_i c^*(c_i)m_i$. On the other hand,

$$\psi_{\omega_\psi}(c^* \otimes m) = \sum_i c^*(c_i)m_i = c^* \cdot m$$

and thus we have showed that (M, ω_ψ) is a C-comodule.

Let now (M, ψ_M) and (N, ψ_N) be two rational left C^*-modules, and $f : M \to N$ a morphism of C^*-modules. We show that f is a morphism of C-comodules from (M, ω_{ψ_M}) to (N, ω_{ψ_N}). Let $m \in M$ and $\omega_{\psi_M}(m) = \sum_i m_i \otimes c_i$. Then

$$\begin{aligned}
\mu_N((f \otimes I)\omega_{\psi_M}(m))(c^*) &= \mu_N(\sum_i f(m_i) \otimes c_i)(c^*) \\
&= \sum_i c^*(c_i)f(m_i) \\
&= f(\sum_i c^*(c_i)m_i) \\
&= f(c^* \cdot m)
\end{aligned}$$

and

$$\begin{aligned}
\mu_N(\omega_{\psi_N} f(m))(c^*) &= (\mu_N \tilde{\mu}_N^{-1} \rho_N f(m))(c^*) \\
&= \rho_N f(m)(c^*) \\
&= c^* \cdot f(m)
\end{aligned}$$

We have obtained that $\mu_N((f \otimes I)\omega_{\psi_M}(m)) = \mu_N(\omega_{\psi_N} f(m))$, and since μ_N is injective, it follows that $(f \otimes I)\omega_{\psi_M} = \omega_{\psi_N} f$, showing that f is a morphism of C-comodules.

We have thus defined a new functor

$$S : Rat({}_{C^*}\mathcal{M}) \to \mathcal{M}^C$$

by $S((M, \psi)) = (M, \omega_\psi)$ for any rational C^*-module M, and $S(f) = f$, for any morphism $f : M \to N$ of rational C^*-modules. We show that $ST = Id$, the identity functor. Let $(M, \omega) \in \mathcal{M}^C$. The comodule structure of $S(T(M))$ is given by

$$\omega_{(\psi_\omega)} : M \to M \otimes C, \quad \omega_{(\psi_\omega)}(m) = \tilde{\mu}_M^{-1}(\rho_M(m))$$

Then

$$(\mu_M \omega_{(\psi_\omega)}(m))(c^*) = \rho_M(m)(c^*) = c^* \cdot m$$

and

$$\begin{aligned}(\mu_M\omega(m))(c^*) &= (\mu_M(\sum m_{(0)}\otimes m_{(1)}))(c^*)\\ &= \sum c^*(m_{(1)})m_{(0)}\\ &= \psi_\omega(c^*\otimes m)\\ &= c^*\cdot m,\end{aligned}$$

and since μ_M is injective, it follows that $\omega_{(\psi_\omega)} = \omega$. We show now that $TS = Id$. Indeed, if $(M,\psi) \in Rat({}_{C^*}\mathcal{M})$, then $(TS)(M) = (M, \psi_{(\omega_\psi)}) = (M,\psi)$, which ends the proof. ∎

The following result presents some of the basic properties of rational modules.

Theorem 2.2.6 *Let C be a coalgebra. Then:*
i) A cyclic submodule of a rational C^*-module is finite dimensional.
ii) If M is a rational C^*-module, and N is a C^*-submodule of M, then N and M/N are rational C^*-modules.
iii) If $(M_i)_{i\in I}$ is a family of rational C^*-modules, then $\oplus_{i\in I}M_i$, the direct sum as a C^*-module, is a rational C^*-module.
iv) Any C^*-module L has a biggest rational C^*-submodule L^{rat}. More precisely, L^{rat} is the sum of all rational submodules of L.
Morevoer, the correspondence $L \mapsto L^{rat}$ defines a left exact functor Rat : ${}_{C^*}\mathcal{M} \to {}_{C^*}\mathcal{M}$.

Proof: i) Let M be a rational C^*-module, and $C^*\cdot m$ the cyclic submodule generated by $m \in M$. Since M is rational, there exist two finite families of elements $(c_i)_{i\in F} \subseteq C$ and $(m_i)_{i\in F} \subseteq M$ for which $c^*\cdot m = \sum_{i\in F} c^*(c_i)m_i$ for any $c^* \in C^*$. It follows that $C^*\cdot m$ is contained in the vector subspace spanned by the family $(m_i)_{i\in F}$, and so it is finite dimensional.
ii) If N is a submodule of M, then Remark 2.2.3.1) shows immediately that N is rational. If we denote by $\overline{m}$ the coset of an element $m \in M$ modulo N, then with the notation from i) we have that for any $c^* \in C^*$

$$c^*\cdot\overline{m} = \sum_{i\in F} c^*(c_i)\overline{m_i},$$

and using again the same remark it follows that M/N is rational too.
iii) Let $q_j : M_j \to \oplus_{i\in I}M_i$ be the canonical inclusion of M_j in the direct sum, and let $m = \sum_{i\in F} q_i(m_i)$ be an element of $\oplus_{i\in I}M_i$, where F is a finite subset of I. For any $i \in F$, the module M_i is rational, hence there exist two families of elements $(c_{ij})_{j\in F_i} \subseteq C$ and $(m_{ij})_{j\in F_i} \subseteq M_i$, F_i finite

sets, such that $c^* \cdot m_i = \sum_{j \in F_i} c^*(c_{ij}) m_{ij}$ for any $c^* \in C^*$. Then

$$\begin{aligned} c^* \cdot m &= \sum_{i \in F} q_i(c^* \cdot m_i) \\ &= \sum_{i \in F} \sum_{j \in F_i} q_i(c^*(c_{ij}) m_{ij}) \\ &= \sum_{i \in F} \sum_{j \in F_i} c^*(c_{ij}) q_i(m_{ij}) \end{aligned}$$

and now $\oplus_{i \in I} M_i$ is rational by Remark 2.2.3 1).
iv) If L is a left C^*-module, let

$$L^{rat} = \sum \{ N \mid N \text{ is a rational } C^* - \text{submodule of } L \}$$

Assertions ii) and iii) show that L^{rat} is a rational C^*-submodule of L. From the definition, it is clear that any rational submodule of L is contained in L^{rat}.
Now let us check that the correspondence $L \mapsto L^{rat}$ defines a functor. If $f : L \to L'$ is a morphism of C^*-modules, define $f^{rat} : L^{rat} \to L'^{rat}$ to be the restriction and corestriction of f. The definition is correct due to ii). Let now

$$0 \longrightarrow L_1 \longrightarrow L_2 \longrightarrow L_3 \longrightarrow 0$$

be an exact sequence in ${}_{C^*}\mathcal{M}$. Since we can assume that the two maps are the inclusion and the canonical projection, respectively, the fact that the sequence

$$0 \longrightarrow L_1^{rat} \longrightarrow L_2^{rat} \longrightarrow L_3^{rat}$$

is exact amounts to the fact that $L_1^{rat} = L_1 \cap L_2^{rat}$, which is clear by ii) and the definition of the rational part. ∎

Corollary 2.2.7 *The category $Rat({}_{C^*}\mathcal{M})$ is a Grothendieck category.*

Proof: In view of Corollary 2.1.19 and Theorem 2.2.6, the only thing that remains to show is that $Rat({}_{C^*}\mathcal{M})$ has a family of generators. Any rational C^*-module M is a sum of finite dimensional C^*-submodules (since any cyclic submodule is finite dimensional), so M is a homomorphic image of a direct sum of finite dimensional rational left C^*-modules. This shows that the family of all finite dimensional rational left C^*-modules is a family of generators of $Rat({}_{C^*}\mathcal{M})$, and the proof is finished. ∎

Corollary 2.2.8 *The category $\mathcal{M}^C$ is a Grothendieck category.*

Proof: It follows from Theorem 2.2.5 and the preceding corollary. ∎

Another consequence is a new proof for the fundamental theorem of comodules (Theorem 2.1.7).

Corollary 2.2.9 *Let M be a right C-comodule. Then:*
i) The subcomodule generated by an element of M is finite dimensional.
ii) M is the sum of its finite dimensional subcomodules.

Proof: i) The subcomodule generated by an element $m \in M$ is the cyclic left C^*-submodule generated by m of the rational C^*-module M, and this is finite dimensional from Theorem 2.2.6.
ii) We regard M as a rational left C^*-module. It is clear that M is the sum of its cyclic submodules, and all of these are finite dimensional subcomodules of M. ∎

Remark 2.2.10 *If C is a coalgebra, then C^* is a left C^*-module, and hence it makes sense to talk about the biggest rational left submodule of C^*. We will denote this submodule by C_l^{*rat}. Similarly, regarding C^* as a right C^*-module, we denote by C_r^{*rat} the biggest rational right submodule of C^*. In case C is finite dimensional, Remark 2.2.4 shows that $C_l^{*rat} = C_r^{*rat} = C^*$.* ∎

Remark 2.2.11 *If C is a coalgebra, since C is a right C-comodule via Δ, we may regard C as a (rational) left C^*-module. We denote this left action of C^* on C by $\rightharpoonup$. Thus $c^* \rightharpoonup c = \sum c^*(c_2)c_1$ for any $c^* \in C^*$ and $c \in C$. Similarly, C is a rational right C^*-module with the action $c \leftharpoonup c^* = \sum c^*(c_1)c_2$.* ∎

Lemma 2.2.12 *Let M be a rational right C^*-module which is finite dimensional. Then M^*, with the induced left C^*-module structure, is rational.*

Proof: Since M is a rational right C^*-module, we can regard M as a left C-comodule too. Let $\rho : M \to C \otimes M$, $\rho(m) = \sum m_{(-1)} \otimes m_{(0)}$ be the map giving this comodule structure. Since M is finite dimensional, Exercise 1.3.3 shows that there exists a linear isomorphism

$$\theta : M^* \otimes C \otimes M \to Hom(M, C \otimes M),\ \theta(m^* \otimes c \otimes m)(m') = m^*(m')c \otimes m$$

Let $z = \sum_i m_i^* \otimes c_i \otimes m_i \in M^* \otimes C \otimes M$ for which $\theta(z) = \rho$. This means that for any $m \in M$ we have

$$\rho(m) = \theta(z)(m) = \sum_i m_i^*(m)c_i \otimes m_i$$

The left C^*-module structure of $M^* = Hom(M,k)$ is given by

$$(c^* \cdot m^*)(m) = m^*(m \cdot c^*) = m^*(\sum_i c^*(c_i)m_i^*(m)m_i) =$$

$$= \sum_i c^*(c_i)m^*(m_i)m_i^*(m)$$

This shows that

$$c^* \cdot m^* = \sum_i c^*(c_i)m^*(m_i)m_i^*$$

for all $c^* \in C^*$, hence M^* is rational as a left C^*-module. ∎

Let C be a coalgebra and $M \in \mathcal{M}^C$, i.e. $M \in Rat(_{C^*}\mathcal{M})$. We consider the dual space $M^* = Hom_k(M,k)$, which is a right C^*-module with the action given by $(uc^*)(m) = u(c^*m)$ for any $u \in M^*, c^* \in C^*$ and $m \in M$. In general M^* is not a rational right C^*-module. By an opposite version of Lemma 2.2.12, if $dim(M)$ is finite, then M^* is a rational right C^*-module. Following P. Gabriel [85] a right C^*-module M is called pseudocompact if it is a topological C^*-module which is Hausdorff separated, complete and it satisfies the following axiom

(MPC) *M has a basis of neighbourhoods of 0 consisting of submodules N such that M/N is finite dimensional.*

Similar to Theorem 1.5.33, we have the following.

Corollary 2.2.13 *If $M \in \mathcal{M}^C$, then M^* is a right topological pseudocompact module.*

Proof: We first show that the multiplication $\mu : M^* \times C^* \to M^*$, $\mu(u,c^*) = uc^*$, is continuous. Let $u \in M^*$, $c^* \in C^*$ and $uc^* + W^\perp$ an open neighbourhood of uc^* in the finite topology of M^*, where W is a finite dimensional subspace of M. If $\rho : M \to M \otimes C$ is the comodule structure map of M, then there exist two finite dimensional subspaces $W_1 \leq M$ and $W_2 \leq C$ such that $\rho(W) \subseteq W_1 \otimes W_2$. In this case $u + W_1^\perp$ is an open neighbourhood of $u \in M^*$ and $c^* + W_2^\perp$ is an open neighbourhood of $c^* \in C^*$. If $f \in W_1^\perp$ and $g \in W_2^\perp$ we have

$$(u+f)(c^*+g) = uc^* + fc^* + ug + fg$$

For any $m \in W$ we have that

$$\begin{aligned}(fc^*)(m) &= f(c^*m)\\ &= \sum f(m_0c^*(m_1))\\ &= 0 \ \ (\text{since } f(W_1) = 0)\end{aligned}$$

Thus $fc^* \in W^\perp$, and similarly we have $ug \in W^\perp$ and $fg \in W^\perp$, showing that

$$\mu(u + W_1^\perp, c^* + W_2^\perp) \subseteq uc^* + W^\perp$$

which means that μ is continuous.
Clearly M^* is Hausdorff separated in the finite topology. On the other hand, M is the union of all its finite dimensional subcomodules N, so

$$\begin{aligned} M^* &= Hom_k(\varinjlim N, k) \\ &= \varprojlim Hom_k(N, k) \\ &= \varprojlim N^* \end{aligned}$$

where in all limits N ranges over the set of all finite dimensional subcomodules of M. Since $N^* \simeq M^*/N^\perp$ we obtain that $M^* \simeq \lim_{\leftarrow} M^*/N^\perp$. Thus M^* is complete and the set

$$\{N^\perp | N \text{ is a finite dimensional subcomodule of } M\}$$

is a basis of open neighbourhoods of 0 in M^*. Since for any finite dimensional N the space $M^*/N^\perp$ has finite dimension, we obtain that M^* is pseudocompact. ∎

Theorem 2.2.14 *Let C be a coalgebra and M a left C^*-module. The following assertions are equivalent.*
(i) $M \in Rat({}_{C^*}\mathcal{M})$.
(ii) $ann_{C^*}(x) = \{c^* \in C^* | c^*x = 0\}$ is a closed (and open) left ideal of finite codimension for any $x \in M$.
(iii) For any $x \in M$ there exists a closed (open) two-sided ideal $I \subseteq C^*$ of finite codimension such that $Ix = 0$.

Proof: $(i) \Rightarrow (ii)$ Any element of M belongs to a finite dimensional submodule of M, so we can reduce to the case where M is finite dimensional. Denote $N = M^*$, which is a rational right C^*-module with $dim(N) = dim(M)$ and $N^* \simeq M$. By Corollary 2.2.13, N^* is a topological left C^*-module. Since N has finite dimension, the finite topology on N^* is discrete. On the other hand, the map $\phi : C^* \longrightarrow M \simeq N^*$, $\phi(c^*) = c^*x$, is continuous, and since $\{x\}$ is open and closed in M, we have that $ann_{C^*}(x) = Ker(\phi)$ is open and closed in C^*. Clearly $C^*/ann_{C^*}(x)$ is finite dimensional, so (ii) holds.
$(ii) \Rightarrow (iii)$ As in $(i) \Rightarrow (ii)$ we may assume that M is finite dimensional, say $M = kx_1 + \ldots + kx_n$. In this case

$$ann_{C^*}(M) = \cap_{1 \le i \le n} ann_{C^*}(x_i)$$

so $I = ann_{C^*}(M)$ is open and closed in C^*. Clearly I is a two-sided ideal of finite codimension.
$(iii) \Rightarrow (i)$ If $Ix = 0$, then C^*x is a quotient of the left C^*-module C^*/I. Since I is closed, then $I = (I^\perp)^\perp$, so

$$C^*/I = C^*/(I^\perp)^\perp \simeq (I^\perp)^*$$

Then $I^\perp$ is a finite dimensional subcoalgebra of C. Since $I^\perp$ is a left and right C-comodule, then so is $(I^\perp)^*$. In particular C^*/I is a rational left C^*-module, so C^*x is a rational left C^*-module. We conclude that M is a rational left C^*-module. ∎

Lemma 2.2.15 *Let A be a k-algebra and M a right A-module. Then*
(i) If M is projective, then $M^* = Hom_k(M, k)$ is an injective left A-module.
(ii) If A has finite dimension and M is finitely generated and injective as a right A-module, then M^* is a projective left A-module.

Proof: We recall that the left A-module structure of M^* is given by $(af)(m) = f(ma)$ for any $a \in A, f \in M^*$ and $m \in M$.
(i) Let $u : N' \to N$ be an injective morphism of left A-modules, and $f : N' \to M^*$ a morphism of left A-modules. The dual morphism $u^* : N^* \to N'^*$ is a surjective morphism of right A-modules. Let $\alpha_M : M \to M^{**}$ be the natural injection, $\alpha_M(m)(v) = v(m)$ for any $m \in M, v \in M^*$. Since M is projective as a right A-module, there exists a morphism of right A-modules $g : M \to N^*$ such that $f^*\alpha_M = u^*g$. Denoting by $\alpha_N : N \to N^{**}$ and $\alpha_{N'} : N' \to (N')^{**}$ the natural injections, we have that

$$\begin{aligned} g^*\alpha_N u &= g^*u^{**}\alpha_{N'} \\ &= (u^*g)^*\alpha_{N'} \\ &= (f^*\alpha_M)^*\alpha_{N'} \\ &= \alpha_M^* f^{**}\alpha_{N'} \\ &= \alpha_M^*\alpha_{M^*} f \end{aligned}$$

But if $m^* \in M^*$ we have

$$\begin{aligned} (\alpha_M^*\alpha_{M^*})(m^*) &= \alpha_M^*(\alpha_{M^*}(m^*)) \\ &= \alpha_M^*(m^*)\alpha_M \end{aligned}$$

For any $m \in M$ we have

$$\begin{aligned} (\alpha_M^*(m^*)\alpha_M)(m) &= \alpha_M^*(m^*)(\alpha_M(m)) \\ &= \alpha_M(m)(m^*) \\ &= m^*(m) \end{aligned}$$

Thus $\alpha_M^*(m^*)\alpha_M = m^*$, showing that $\alpha_M^*\alpha_M = Id_{M^*}$. Hence $(g^*\alpha_N)u = f$, so M^* is injective.
(ii) Clearly M is finite dimensional. Since M is finitely generated, there exists an epimorphism $A^n \longrightarrow M^* \longrightarrow 0$ in the category of left A-modules. Apply the functor $Hom(-, k)$ and obtain an exact sequence $0 \longrightarrow M^{**} \longrightarrow A^{*\,n}$. Since $M^{**} \simeq M$ and M is injective, we have $A^{*\,n} \simeq M \oplus N$ for some right A-module N. Then $A^n \simeq (A^{*\,n})^* \simeq M^* \oplus N^*$, so M^* is a projective left A-module. ∎

The following gives in particular a description of the rational part of C^*.

Corollary 2.2.16 *Let C be a coalgebra and $M \in {}^C\mathcal{M}$. Then the following three sets are equal.*
(i) $Rat({}_{C^*}M^*)$.
(ii) The sum of all finite dimensional C^*-submodules of M^*.
(iii) The set of all elements $m^* \in M^*$ such that $Ker(m^*)$ contains a left C-subcomodule of M of finite codimension.

Proof: $(i) \subseteq (ii)$ is obvious.
$(ii) \subseteq (i)$ Let $m \in (ii)$. Then there exists a finite dimensional C^*-submodule X of M^* such that $m^* \in X$, so $ann_{C^*}(m^*)$ is a left ideal of C^* of finite codimension. On the other hand, since the map from C^* to M^* obtained by right multiplication with m^* is continuous, the kernel of this map is open and closed in C^* (see Corollary 2.2.13), so $m^* \in Rat({}_{C^*}M^*)$ (Theorem 2.2.14).
$(i) \subseteq (iii)$ Let $m^* \in Rat({}_{C^*}M^*)$ and X a finite dimensional C^*-submodule of M^* such that $m^* \in X$. Then $X^\perp$ is a subcomodule of M and $m^*X^\perp = 0$, so $X^\perp \subseteq Ker(m^*)$. Since $X^\perp$ has finite dimension we obtain that $m^* \in (iii)$.
$(iii) \subseteq (i)$ Let $m^* \in M^*$ such that $Y \subseteq Ker(m^*)$ for some subcomodule Y of M of finite codimension. Then we can regard m^* as a linear map from M/Y to k, so $m^* \in (M/Y)^* \leq M^*$. Since $(M/Y)^*$ is a right C-comodule of finite dimension, $(M/Y)^*$ is a rational left C^*-submodule of M^*, so $m^* \in Rat({}_{C^*}M^*)$. ∎

Exercise 2.2.17 *Let C be a coalgebra and $\phi_C : C \to C^{**}$ the natural injection. Then $\phi_C(Rat({}_{C^*}C)) = Rat({}_{C^*}C^{**})$.*

Exercise 2.2.18 *Let $(C_i)_{i\in I}$ be a family of coalgebras and $C = \oplus_{i\in I}C_i$ the coproduct of this family in the category of coalgebras. Then the following assertions hold.*
(i) $C^* \simeq \prod_{i\in I} C_i^*$. Moreover, this is an isomorphism of topological rings if we consider the finite topology on C^* and the product topology on $\prod_{i\in I} C_i^*$.

(ii) If $M \in \mathcal{M}^C$ then for any $m \in M$ there exists a two-sided ideal I of C^* such that $Im = 0$, $I = \prod_{i \in I} I_i$, where I_i is a two-sided ideal of C_i^* which is closed and has finite codimension, and $I_i = C_i^*$ for all but a finite number of i's.
(iii) The category $\mathcal{M}^C$ is equivalent to the direct product of categories $\prod_{i \in I} \mathcal{M}^{C_i}$.
(iv) If A is a subcoalgebra of $C = \oplus_{i \in I} C_i$, then there exists a family $(A_i)_{i \in I}$ such that A_i is a subcoalgebra of C_i for any $i \in I$, and $A = \oplus_{i \in I} A_i$.

Exercise 2.2.19 *Let $(C_i)_{i \in I}$ be a family of subcoalgebras of the coalgebra C and A a simple subcoalgebra of $\sum_{i \in I} C_i$ (i.e. A is a subcoalgebra which has precisely two subcoalgebras, 0 and A; more details will be given in Chapter 3). Then there exists $i \in I$ such that $A \subseteq C_i$.*

2.3 Bicomodules and the cotensor product

Definition 2.3.1 *Let C and D be two coalgebras. A k-vector space M is called a left-D, right-C bicomodule if M has a left D-comodule structure given by $\mu : M \to D \otimes M$, $\mu(m) = \sum m_{[-1]} \otimes m_{[0]}$, a right C-comodule structure given by $\rho : M \to M \otimes C$, $\rho(m) = \sum m_{(0)} \otimes m_{(1)}$, such that $(\mu \otimes I)\rho = (I \otimes \rho)\mu$. This compatibility may be written as*

$$\sum (m_{(0)})_{[-1]} \otimes (m_{(0)})_{[0]} \otimes m_{(1)} = \sum m_{[-1]} \otimes (m_{[0]})_{(0)} \otimes (m_{[0]})_{(1)}$$

for any $m \in M$.
If M and N are two such bicomodules, then a morphism of bicomodules from M to N is a linear map $f : M \to N$ which is a morphism of left D-comodules, and in the same time a morphism of right C-comodules.
In this way we can define a category of left-D, right-C bicomodules, which we will denote by ${}^D\mathcal{M}^C$. ∎

Example 2.3.2 *Any coalgebra C is a left-C, right-C bicomodule, with the left and right comodule structures defined by the comultiplication of C.* ∎

If C and D are two coalgebras, then we consider the dual algebras C^* and D^*, and we denote by ${}_{C^*}\mathcal{M}_{D^*}$ the category of left-C^*, right-D^* bimodules. We recall that such an object is a vector space having a structure of a left C^*-module and a right D^*-module structure, which are compatible in the sense that $c^* \cdot (m \cdot d^*) = (c^* \cdot m) \cdot d^*$ for any $c^* \in C^*, m \in M, d^* \in D^*$. The morphisms between two objects in this category are linear maps which are also morphisms of left C^*-modules, and in the same time morphisms of right D^*-modules. We will denote by $Rat({}_{C^*}\mathcal{M}_{D^*})$ the full subcategory of

${}_{C^*}\mathcal{M}_{D^*}$ consisting of all objects which are rational left C^*-modules, and in the same time rational right D^*-modules.

Theorem 2.3.3 *Let C and D be two coalgebras. Then the categories ${}^D\mathcal{M}^C$ and $Rat({}_{C^*}\mathcal{M}_{D^*})$ are isomorphic.*

Proof: The proof relies essentially on the proof of Theorem 2.2.5. Let $M \in {}^D\mathcal{M}^C$. Then we know already from the cited theorem that M is a rational left C^*-module with the action given by $c^* \cdot m = \sum c^*(m_{(1)})m_{(0)}$, and that M is a rational right D^*-module with the action given by $m \cdot d^* = \sum d^*(m_{[-1]})m_{[0]}$. It remains to check that these two structures induce a bimodule. We have

$$\begin{aligned}(c^* \cdot m) \cdot d^* &= \sum c^*(m_{(1)})m_{(0)} \cdot d^* \\ &= \sum c^*(m_{(1)})d^*((m_{(0)})_{[-1]})(m_{(0)})_{[0]}\end{aligned}$$

and

$$\begin{aligned}c^* \cdot (m \cdot d^*) &= \sum d^*(m_{[-1]})c^* \cdot m_{[0]} \\ &= \sum d^*(m_{[-1]})c^*((m_{[0]})_{(1)})(m_{[0]})_{(0)},\end{aligned}$$

and the equality follows from the definition of the bicomodule.

Conversely, if M is a left-C^*, right-D^* bimodule, which is rational on both sides, we know that M has a structure of a left D-comodule, which we will denote by $m \mapsto \sum m_{[-1]} \otimes m_{[0]}$, and a structure of a right C-comodule, which we will denote by $m \mapsto \sum m_{(0)} \otimes m_{(1)}$. From the fact that M is a bimodule, and from the above computations, we obtain that

$$c^*(m_{(1)})d^*((m_{(0)})_{[-1]})(m_{(0)})_{[0]} = \sum d^*(m_{[-1]})c^*((m_{[0]})_{(1)})(m_{[0]})_{(0)}$$

for any $c^* \in C^*$ and $d^* \in D^*$. This means that

$$(d^* \otimes I \otimes c^*)(\sum (m_{(0)})_{[-1]} \otimes (m_{(0)})_{[0]} \otimes m_{(1)} -$$

$$- \sum m_{[-1]} \otimes (m_{[0]})_{(0)} \otimes (m_{[0]})_{(1)}) = 0$$

for any $c^* \in C^*, d^* \in D^*$. But if for an element $z \in D \otimes M \otimes C$ we have $(d^* \otimes I \otimes c^*)(z) = 0$ for any $c^* \in C^*, d^* \in D^*$, then $z = 0$. Indeed, we choose a basis $(d_i)_i$ of D and a basis $(c_j)_j$ of C. Then we can write $z = \sum_{i,j} d_i \otimes m_{ij} \otimes c_j$ for some $m_{ij} \in M$. Fix r and s, and consider the maps $d_r^* \in D^*$, $c_s^* \in C^*$ for which $d_r^*(d_i) = \delta_{ri}$ şi $c_s^*(c_j) = \delta_{sj}$. Then

$0 = (d_r^* \otimes I \otimes c_s^*)(z) = m_{rs}$. From this we deduce that $z = 0$, and the proof is now complete due to Theorem 2.2.5. ∎

We recall that for any subset X of a coalgebra C there exists a smallest subcoalgebra of C containing X, and this is called the subcoalgebra generated by X (Remark 1.5.30). If the set X has only one element c, then the subcoalgebra generated by $\{c\}$ is called simply the subcoalgebra generated by c. The following exercise illustrates the use of bicomodules for proving the fundamental theorem of coalgebras (Theorem 1.4.7).

Exercise 2.3.4 *Let C be a coalgebra, and $c \in C$. Show that the subcoalgebra of C generated by c is finite dimensional, using the bicomodule structure of C.*

Corollary 2.3.5 *Let C be a coalgebra. Then the subcoalgebra generated by a finite family of elements of C is finite dimensional.*

Proof: It is clear that the subcoalgebra generated by $\{ c_1, \dots, c_n \}$ is the sum of the subcoalgebras generated by each of the c_i, and since all of these are finite dimensional, it follows that their sum is finite dimensional too. ∎

We present now a construction dual to the tensor product of modules over an algebra. Let C be a coalgebra, M a right C-comodule with comodule structure map $\rho_M : M \to M \otimes C$ and N a left C-comodule with comodule structure map $\rho_N : N \to C \otimes N$. We denote by $M \Box_C N$ the kernel of the morphism

$$\rho_M \otimes I - I \otimes \rho_N : M \otimes N \to M \otimes C \otimes N$$

$M \Box_C N$ is a k-subspace of $M \otimes N$ which is called the cotensor product of the comodules M and N. If $f \in Com_C(M, M')$ and $g \in Com_C(N, N')$ are two morphisms in the categories $\mathcal{M}^C$ and ${}^C\mathcal{M}$, then the map $f \otimes g : M \otimes N \to M' \otimes N'$ induces a linear morphism $f \Box_C g : M \Box_C N \to M' \Box_C N'$. It is easy to see that the correspondence $(M, N) \mapsto M \Box_C N$ defines an additive functor from $\mathcal{M}^C \times {}^C\mathcal{M} \to_k \mathcal{M}$, called the cotensor functor.
Since the tensor functor of vector spaces is exact and the cotensor is a kernel, we have that the cotensor functor is left exact. Also, since the tensor functor commutes with direct sums and with filtered inductive limits, we obtain that the cotensor functor also commutes with direct sums and with filtered inductive limits.
If $C = k$, then $M \Box_k N$ is just the tensor product $M \otimes N$, since in this case $\rho_M \otimes I - I \otimes \rho_N = 0$.
Let C and D be two coalgebras and assume that $M \in {}^D\mathcal{M}^C$. Denote by $\rho^- : M \to D \otimes M$ and $\rho^+ : M \to M \otimes C$ the comodule structure maps of M. We have that $(\rho^- \otimes I)\rho^+ = (I \otimes \rho^+)\rho^-$. Let $N \in {}^C\mathcal{M}$ with comodule

structure map $\mu : N \to C \otimes N$. Then $\rho^{-} \otimes I : M \otimes N \to D \otimes M \otimes N$ endows $M \otimes N$ with a structure of a left D-comodule. The induced structure of a right rational D^*-module of $M \otimes N$ is given by $(m \otimes n)d^* = md^* \otimes n$ for any $m \in M$, $n \in N$ and $d^* \in D^*$. On the other hand, if $d^* \in D^*$, the map $u : M \to M, u(m) = md^*$ for any $m \in M$, is a morphism of right C-comodules, since $M \in {}^D\mathcal{M}^C$. Hence by the above argument it follows that $(u \otimes I)(M \square_C N) \subseteq M \square_C N$, thus $M \square_C N$ is a D^*-submodule of $M \otimes N$. Moreover, it is a rational D^*-module, so $M \square_C N$ is a D-subcomodule of $M \otimes N$, i.e. $(\rho^- \otimes I)(M \square_C N) \subseteq D \otimes (M \square_C N)$. In this way, for any $M \in {}^D\mathcal{M}^C$ we obtain a left exact functor

$$M \square_C - : {}^C\mathcal{M} \to {}^D\mathcal{M}$$

The following gives the main properties of the cotensor functor.

Proposition 2.3.6 *(i) If $M \in \mathcal{M}^C$ and $N \in {}^C\mathcal{M}$, then $M \square_C C \simeq M$ as right C-comodules and $C \square_C N \simeq N$ as left C-comodules.*
(ii) If $M \in \mathcal{M}^C$ and $N \in {}^C\mathcal{M}$, then $M \square_C N \simeq N \square_{C^{cop}} M$ as linear spaces. In particular if C is cocommutative, then $M \square_C N \simeq N \square_C M$.
(iii) If C and D are two coalgebras and $M \in {}^C\mathcal{M}^D$, $L \in {}^C\mathcal{M}$ and $N \in {}^D\mathcal{M}$, then we have a natural isomorphism $(L \square_C M) \square_D N \simeq L \square_C (M \square_D N)$.

Proof: (i) We define a linear map $\alpha : M \square_C C \to M$ as follows. For $z \in M \square_C C \subseteq M \otimes C$, say $z = \sum_i x_i \otimes c_i$ with $(x_i)_i \subseteq M$ and $(c_i)_i \subseteq C$, we set $\alpha(z) = \sum \varepsilon(c_i)x_i$. On the other hand, since $(\rho_M \otimes I)\rho_M = (I \otimes \Delta)\rho_M$, where ρ_M is the comodule structure map of M and Δ is the comultiplication of C, then we have $(\rho_M \otimes I)\rho_M = (I \otimes \Delta)\rho_M$, showing that $\rho_M(M) \subseteq M \square_C C$. Thus it makes sense to define $\beta : M \to M \square_C C$ by $\beta(m) = \rho_M(m) = \sum m_0 \otimes m_1$ for any $m \in M$. If $z = \sum_i x_i \otimes c_i \in M \square_C C$, then we have $\sum_i \rho_M(x_i) \otimes c_i = \sum_i x_i \otimes \Delta(c_i)$, and applying $I \otimes I \otimes \varepsilon$ we obtain $\sum_i \varepsilon(c_i)\rho_M(x_i) = \sum_i x_i \otimes c_i = z$. This shows that $(\beta\alpha)(z) = z$, i.e. $\beta\alpha = Id_{M \square_C C}$. It is clear that for any $m \in M$ we have $(\alpha\beta)(m) = m$, thus $\alpha\beta = Id_M$. We have obtained that α and β are inverse each other. It is clear that β is a morphism of right C-comodules, and this ends the proof of (i).
(ii) Let $\rho_M : M \to M \otimes C$ be the comodule structure map of M as a right C-comodule and $\rho'_M : M \to C^{cop} \otimes M$, the comodule structure map of M as a left C^{cop}-comodule. If $\rho_M(m) = \sum m_0 \otimes m_1$, then $\rho'_M(m) = \sum m_1 \otimes m_0$. Similarly we denote by $\rho_N : N \to C \otimes N$ and $\rho'_N : N \to N \otimes C^{cop}$ the comodule structures map of N as a left C-comodule,respectively as a right C^{cop}-comodule. Let $\tau : M \otimes N \to N \otimes M$ and $\overline{\tau} : M \otimes C \otimes N \to N \otimes C^{cop} \otimes M$ be the linear isomorphisms defined by $\tau(m \otimes n) = n \otimes m$ and $\overline{\tau}(m \otimes c \otimes n) = n \otimes c \otimes m$. We have that

$$\overline{\tau}(\rho_M \otimes I - I \otimes \rho_N) = (I \otimes \rho'_M - \rho'_N \otimes I)\tau$$

implying that $M\Box_C N \simeq N\Box_{C^{cop}} M$. The second part is clear since for a cocommutative C we have $C = C^{cop}$.
(iii) Since the tensor product functor over a field is exact, we have a natural isomorphism

$$(L \otimes M)\Box_D N \simeq L \otimes (M\Box_D N)$$

Now the exact sequence of right D-comodules

$$0 \longrightarrow L\Box_C M \longrightarrow L \otimes M \overset{\rho_L \otimes I - I \otimes \rho_M^+}{\longrightarrow} L \otimes C \otimes M$$

and the fact that the cotensor functor is left exact produces a commutative diagram

$$\begin{tikzcd} M \otimes N \arrow[r, "\rho_M \otimes I - I \otimes \rho_N"] \arrow[d, "\tau"'] & M \otimes C \otimes N \arrow[d, "\overline{\tau}"] \\ N \otimes M \arrow[r, "I \otimes \rho'_M - \rho'_N \otimes I"] & N \otimes C^{cop} \otimes M \end{tikzcd}$$

and then we have a natural isomorphism $(L\Box_C M)\Box_D N \simeq L\Box_C(M\Box_D N)$. ∎

Assume now that N is a finite dimensional left C-comodule with comodule structure map $\rho_N : N \to C \otimes N$, $\rho_N(n) = \sum n_{(-1)} \otimes n_{(0)}$. Let $N^* = Hom_k(N, k)$. Since N is finite dimensional, the natural morphism

$$\theta : N^* \otimes C \to Hom(N, C),\ \theta(f \otimes c)(n) = f(n)c$$

is a linear isomorphism. N^* has a natural structure of a right C-comodule given by

$$\rho_{N^*} : N^* \to N^* \otimes C,\ \rho_{N^*}(n^*) = \theta^{-1}((I \otimes n^*)\rho_N)$$

If $n^* \in N^*$ and $\rho_{N^*}(n^*) = \sum_i f_i \otimes c_i$ with $f_i \in N^*$ and $c_i \in C$, then $c^*n^* = \sum_i c^*(c_i)f_i$ for any $c^* \in C^*$. Therefore $(c^*n^*)(n) = \sum_i c^*(c_i)f_i(n)$ for any $n \in N$. On the other hand we have $\theta(\sum_i f_i \otimes c_i) = (I \otimes n^*)\rho_N$, so if $\rho_N(n) = \sum n_{(-1)} \otimes n_{(0)}$ we have $\sum_i f_i(n)c_i = \sum n^*(n_{(0)})n_{(-1)}$, and then $\sum_i f_i(n)c^*(c_i) = \sum n^*(n_{(0)})c^*(n_{(-1)})$ for any $c^* \in C^*$. We obtain that $(c^*n^*)(n) = \sum c^*(n_{(-1)})n^*(n_{(0)})$, and this gives a structure of a rational left C^*-module to N^*, which is associated to the right C-comodule structure of N^* defined by ρ_{N^*}. This left C^*-module structure of N^* is the same with the left C^*-module structure of $N^* = Hom_k(N, k)$ obtained by regarding

N as a right C^*-module induced by the comodule map ρ_N (see also Lemma 2.2.12).

Proposition 2.3.7 *Let N be a finite dimensional left C-comodule and M a right C-comodule. Then we have a natural linear isomorphism $M\square_C N \simeq Com_C(N^*, M)$.*

Proof: Since N has finite dimension, we have the natural linear isomorphism

$$\alpha : M \otimes N \to Hom(N^*, M),\ \alpha(x \otimes y)(f) = f(y)x$$

Let $z = \sum_i x_i \otimes y_i \in M\square_C N \subseteq M \otimes N$, i.e. we have

$$\sum_i (x_i)_{(0)} \otimes (x_i)_{(1)} \otimes y_i = \sum_i x_i \otimes (y_i)_{(-1)} \otimes (y_i)_{(0)} \tag{2.1}$$

For any $c^* \in C^*$ and $n^* \in N^*$ we have that

$$\begin{aligned}
\alpha(z)(c^*n^*) &= \sum_i (c^*n^*)(y_i)x_i \\
&= \sum_i c^*((y_i)_{(-1)})n^*((y_i)_{(0)})x_i \\
&= \sum_i n^*(y_i)c^*((x_i)_{(1)})(x_i)_{(0)} \quad \text{(by (2.1))} \\
&= c^* \sum_i n^*(y_i)x_i \\
&= c^*\alpha(z)(n^*)
\end{aligned}$$

so $\alpha(z)$ is a morphism of left C^*-modules, which is the same to a morphism of right C-comodules from N^* to M.
With the same computation we obtain that if $\alpha(z) \in Com_C(N^*, M)$, then $z \in M\square_C N$. ∎

Let C and D be two coalgebras and $\phi : C \to D$ a coalgebra morphism. If $M \in \mathcal{M}^C$, then the map $(I \otimes \phi)\rho_M : M \to M \otimes D$ gives M a structure of a right D-comodule. We denote by M_ϕ the space M regarded with this structure of a right D-comodule. In this way we construct an exact functor

$$(-)_\phi : \mathcal{M}^C \to \mathcal{M}^D,\ \ M \mapsto M_\phi$$

In particular, since C is a left-C, right-C bicomodule, we can regard C as a left-D, right-C bicomodule via ϕ. Then $\phi : C \to D$ is a morphism of left D-comodules.

If $N \in \mathcal{M}^D$, we can define the right C-comodule $N^\phi = N\square_D C$, and in this way we have a new functor

$$(-)^\phi : \mathcal{M}^D \to \mathcal{M}^C, \quad N \mapsto N^\phi$$

which is left exact. In particular if $D = k$ and $\phi = \varepsilon$, the counit of C, then the functor $(-)_\varepsilon$ is just the forgetful functor $U : \mathcal{M}^C \to_k \mathcal{M}$, and the functor $(-)^\phi$ is exactly the functor $- \otimes C :_k \mathcal{M} \to \mathcal{M}^C$.

Proposition 2.3.8 *Let $\phi : C \to D$ be a morphism of coalgebras. Then the functor $(-)_\phi : \mathcal{M}^C \to \mathcal{M}^D$ is a left adjoint of the functor $(-)^\phi : \mathcal{M}^D \to \mathcal{M}^C$. In particular the forgetful functor $U : \mathcal{M}^C \to_k \mathcal{M}$ is a left adjoint of the functor $- \otimes C :_k \mathcal{M} \to \mathcal{M}^C$.*

Proof: Let $M \in \mathcal{M}^C$ and $N \in \mathcal{M}^D$, and define the natural maps

$$\Phi : Com_C(M, N^\phi) \to Com_D(M_\phi, N)$$

$$\Psi : Com_D(M_\phi, N) \to Com_C(M, N^\phi)$$

as follows. For $u \in Com_C(M, N^\phi)$ we put $\Phi(u) = (I \otimes \varepsilon)u$, where ε is the counit of C and $I \otimes \varepsilon$ is regarded here as the restriction of $I \otimes \varepsilon : N \otimes C \to N$ to $N\square_D C$. In fact $\Phi(u)$ is the composition of the morphisms

$$M \xrightarrow{u} N\square_D C \xrightarrow{I\otimes\phi} N\square_D D \overset{I\otimes\varepsilon}{\simeq} N$$

If $v \in Com_D(M_\phi, N)$, then we put $\Psi(v) = (v \otimes I)\rho_M$. We prove that $\Psi(v) \in Com_C(M, N^\phi)$. Indeed, since $v \in Com_D(M_\phi, N)$ we have

$$(v \otimes I)(I \otimes \phi)\rho_M = \rho_N v$$

On the other hand we have that

$$\begin{aligned}
(\rho_N \otimes I)(v \otimes I)\rho M &= ((\rho_N v) \otimes I)\rho_M \\
&= (((v \otimes I)(I \otimes \phi)\rho_M) \otimes I)\rho_M \\
&= (v \otimes I \otimes I)(I \otimes \phi \otimes I)(\rho_M \otimes I)\rho_M \\
&= (v \otimes I \otimes I)(I \otimes \phi \otimes I)(I \otimes \Delta)\rho_M \\
&= (I \otimes \phi \otimes I)(v \otimes I \otimes I)(I \otimes \Delta)\rho_M \\
&= (I \otimes \phi \otimes I)(I \otimes \Delta)(v \otimes I)\rho_M
\end{aligned}$$

This shows that for any $m \in M$ we have $\Psi(v)(m) \in N\square_D C$, so $\Psi(v)$ can be regarded as a morphism from M to N^ϕ.

If $u \in Com_C(M, N^\phi)$ then we have

$$\begin{aligned}
\Psi(\Phi(u)) &= (I \otimes \varepsilon \otimes I)(u \otimes I)\rho_M \\
&= (I \otimes \varepsilon \otimes I)(I \otimes \Delta)u \quad (u \text{ is a comodule map}) \\
&= (I \otimes I)u \\
&= u
\end{aligned}$$

so $\Psi\Phi = Id$. Conversely, for $v \in Com_D(M_\phi, N)$ we have

$$\begin{aligned}
\Phi(\Psi(v)) &= (I \otimes \varepsilon)\Psi(v) \\
&= (I \otimes \varepsilon)(v \otimes I)\rho_M \\
&= (I \otimes \varepsilon_D)(I \otimes \phi)(v \otimes I)\rho_M \\
&= (I \otimes \varepsilon_D)(v \otimes I)(I \otimes \phi)\rho_M \\
&= (I \otimes \varepsilon_D)\rho_N v \quad (v \text{ is a comodule map}) \\
&= v
\end{aligned}$$

showing that $\Phi\Psi = Id$, which ends the proof. ∎

Remark 2.3.9 *Let A be a k-algebra, M a right A-module with module structure map $\mu : M \otimes A \to M$ and N a left A-module with module structure map $\rho : A \otimes N \to N$. By restricting scalars, M and N are k-vector spaces, and we can form the tensor product $M \otimes N$ over k. Then the tensor product $M \otimes_A N$ of A-modules is precisely $Coker(\mu \otimes I - I \otimes \rho)$. Thus the cotensor product is a construction dual to the tensor product.*

Exercise 2.3.10 *Let C and D be two coalgebras. Show that the categories ${}^D\mathcal{M}^C$, $\mathcal{M}^{C \otimes D^{cop}}$, $\mathcal{M}^{D^{cop} \otimes C}$, ${}^{D \otimes C^{cop}}\mathcal{M}$ and ${}^{C^{cop} \otimes D}\mathcal{M}$ are isomorphic.*

Exercise 2.3.11 *Let C, D and L be cocommutative coalgebras and $\phi : C \to L$, $\psi : D \to L$ coalgebra morphisms. Regard C and D as L-comodules via the morphisms ϕ and ψ. Show that $C \square_L D$ is a (cocommutative) subcoalgebra of $C \otimes D$, and moreover, $C \square_L D$ is the fiber product in the category of all cocommutative coalgebras.*

2.4 Simple comodules and injective comodules

Definition 2.4.1 *A right C-comodule is said to be* free *if it is isomorphic to a comodule of the form $X \otimes C$, with X a vector space, with the right comodule structure map $I \otimes \Delta : X \otimes C \to X \otimes C \otimes C$.* ∎

Remark 2.4.2 *It is clear that if X is a vector space having the basis $(e_i)_{i\in I}$, then the comodule $X \otimes C$ is isomorphic to $C^{(I)}$, the direct sum in the category $\mathcal{M}^C$ of a family of copies of C indexed by the set I.* ∎

Proposition 2.4.3 *Any right C-comodule is isomorphic to a subcomodule of a free C-comodule.*

Proof: Let $M \in \mathcal{M}^C$. Then $M \otimes C$ is a right C-comodule via $I \otimes \Delta : M \otimes C \to M \otimes C \otimes C$. Let $\rho : M \to M \otimes C$ be the morphism giving the comodule structure of M. Then the definition of the comodule shows that ρ is a morphism of right C-comodules from M to $M \otimes C$, where the second one is regarded with the above mentioned structure. Moreover, ρ is injective, since if for an $m \in M$ we have $\rho(m) = \sum m_{(0)} \otimes m_{(1)} = 0$, then $m = \sum \varepsilon(m_{(1)})m_{(0)} = 0$. It follows that M is isomorphic to the subcomodule $Im(\rho)$ of the free comodule $M \otimes C$. ∎

Definition 2.4.4 *A right C-comodule M is called* injective *if it is an injective object in the category $\mathcal{M}^C$, i.e. for any injective morphism $i : X \to Y$ of right C-comodules, and for any morphism $f : X \to M$ of right C-comodules, there exists a morphism of right C-comodules $\overline{f} : Y \to M$ for which $\overline{f}i = f$.* ∎

Corollary 2.4.5 *A free right C-comodule is injective. In particular, C is an injective right C-comodule.*

Proof: Consider the adjunction from Proposition 2.3.8. Since U is an exact functor, and $\mathcal{M}^C$ and ${}_k\mathcal{M}$ are Grothendieck categories, it follows that $X \otimes C$ is an injective object in $\mathcal{M}^C$ for any injective object X from ${}_k\mathcal{M}$. But in ${}_k\mathcal{M}$ every obiect is injective, which ends the proof. ∎

Remark 2.4.6 *Since the category $\mathcal{M}^C$ is Grothendieck, it follows that every object has an injective envelope. This means that for any $M \in \mathcal{M}^C$ there exists $E(M) \in \mathcal{M}^C$ such that M is an essential subcomodule in $E(M)$ (i.e. for any nonzero subcomodule X of $E(M)$ we have $X \cap M \neq 0$).* ∎

The following result provides a characterization of injective comodules.

Proposition 2.4.7 *Let M be a right C-comodule. Then M is injective if and only if M is a direct summand in a free C-comodule.*

Proof: Assume that $F = M \oplus X$ for some free right C-comodule F and some right C-comodule X. Since F is injective by Corollary 2.4.5, we obtain that both M and X are injective.

Conversely, assume that M is injective. Proposition 2.4.3 yields the existence of an injective morphism of comodules $i : M \to C^{(I)}$ for some set I. The injectivity of M shows that the morphism i splits (i.e. there exists a morphism of comodules $j : C^{(I)} \to M$ with $ji = Id_M$) and then $C^{(I)} \simeq i(M) \oplus Ker(j) \simeq M \oplus Ker(j)$, hence M is a direct summand in a free comodule. ∎

In a Grothendieck category a finite direct sum of injective objects is an injective object. In a category of comodules we have even more, as the following shows.

Proposition 2.4.8 *Let $(M_i)_{i\in I}$ be a family of injective right C-comodules. Then their direct sum $\oplus_{i\in I}M_i$ is an injective object in the category $\mathcal{M}^C$.*

Proof: Proposition 2.4.7 shows that for each $i \in I$ there exists a set J_i such that M_i is a direct summand in $C^{(J_i)}$. Then, denoting by $J = \bigsqcup_{i\in I} J_i$ the coproduct of the family $(J_i)_{i\in I}$ in the category of sets (which is exactly the disjoint union of the family), we obtain that $\oplus_{i\in I}M_i$ is a direct summand in $C^{(J)}$, and so it is injective. ∎

Definition 2.4.9 *A right C-comodule is called* simple *if $M \neq 0$ and if the only subcomodules of M are 0 and M.* ∎

Remark 2.4.10 *1) From the isomorphism between the category $\mathcal{M}^C$ and the category of the rational left C^*-modules it follows that a right C-comodule M is simple if and only if it is a simple object when it is regarded as a rational left C^*-module. Since any submodule of a rational module is rational, this is equivalent to the fact that M is simple as a left C^*-module. We will therefore regard throughout a (simple) right C-comodule also as a (simple) left C^*-module.*
2) If M is a right C-comodule, then we regard M as a left C^*-module, and thus it makes sense to consider the socle $s(M)$ of M, which is the sum of the simple C^*-submodules. This is a semisimple left C^*-module, in particular it is a direct sum of simple submodules. From the above considerations it follows that $s(M)$ is also the sum of the simple right C-subcomodules of M. A classical result from module theory says that if $M = \oplus_{i\in I}M_i$, then $s(M) = \oplus_{i\in I}s(M_i)$. ∎

Proposition 2.4.11 *Any nonzero comodule contains a simple subcomodule.*

Proof: Let M be a non-zero simple right C-comodule, and let $m \in M$, $m \neq 0$. Then the subcomodule $C^* \cdot m$ generated by m is finite dimensional (by Theorem 2.2.6.i)) and then there exists a subcomodule S of $C^* \cdot m$ having the least possible dimension among all non-zero subcomodules of $C^* \cdot m$. It is clear that S is simple. ∎

Corollary 2.4.12 *Let M be a non-zero right C-comodule. Then its socle $s(M)$ is an essential subcomodule in M.*

Proof: If $s(M)$ would not be essential in M, then there would exist a non-zero subcomodule X of M with $s(M) \cap X = 0$. The preceding proposition shows that X contains a simple subcomodule S. But then S is also a simple subcomodule of M, thus $S \subseteq s(M)$, a contradiction. ∎

Proposition 2.4.13 *A simple C-comodule is finite dimensional.*

Proof: Let S be a simple right C-comodule, and let $x \in S$, $x \neq 0$. Then S is generated by x as a comodule, and from Theorem 2.1.7 it follows that S is finite dimensional. ∎

Proposition 2.4.14 *A simple right C-comodule S is isomorphic to a right coideal of C (hence S may be embedded in C).*

Proof: Remark 2.4.2 and Proposition 2.4.3 show that there exists an injective morphism of comodules $S \to C^n$, where $n = dim(S)$. Regarding this embedding as being an embedding of left C^*-modules, we obtain that $S \subseteq s(C^n)$. Hence S is isomorphic to a submodule of $s(C^n)$. Taking into account the formula for the socle of a direct sum of modules (which was recalled above), it follows that S is isomorphic to a simple submodule of C, hence to a right C-subcomodule of C, and the proof is finished. ∎

Corollary 2.4.15 *Let S be a simple C-comodule. Then there exists an injective envelope $E(S)$ of S with the property that $E(S) \subseteq C$.*

Proof: Let $E(S)$ be an injective envelope of S, and $f : S \to E(S)$ the canonical injection. We know that $f(S)$ is essential in $E(S)$. The preceding proposition shows that there exists an embedding $i : S \to C$ of S in C, and since C is an injective object in the category $\mathcal{M}^C$, we obtain that there exists a morphism of C-comodules $g : E(S) \to C$ for which $gf = i$. Since i is injective, we obtain that $Ker(g) \cap f(S) = 0$. But $f(S)$ is essential in $E(S)$, hence $Ker(g) = 0$. Thus g is injective, and this shows that $E(S)$ may be embedded in C. ∎

Theorem 2.4.16 *Let C be a coalgebra, and $s(C) = \oplus_{i \in I} M_i$ the socle of C regarded as a right C-comodule (M_i are all simple right C-subcomodules of C). Then $C = \oplus_{i \in I} E(M_i)$, where $E(M_i)$ is an injective envelope of M_i contained in C.*

Proof: Corollary 2.4.15 shows that for any i there exists an injective envelope $E(M_i) \subseteq C$ of M_i. Since the (M_i)'s are simple C^*-submodules of

C, whose sum is direct, and every M_i is essential in $E(M_i)$, it follows that the sum of the subcomodules $E(M_i)$ is also direct. Thus

$$s(C) = \oplus_{i \in I} M_i \subseteq \oplus_{i \in I} E(M_i) \subseteq C$$

Since $\oplus_{i \in I} E(M_i)$ is an injective subobject of C by Proposition 2.4.8, it follows that it is a direct summand in C, hence $C = (\oplus_{i \in I} E(M_i)) \oplus X$ for a subcomodule X of C. But $s(C)$ is essential in C by Corollary 2.4.12, so $\oplus_{i \in I} E(M_i)$ is also essential in C. This shows that $X = 0$ and the proof is finished. ∎

Let C be a coalgebra and $Q \in \mathcal{M}^C$. The definition of injective comodules shows that Q is injective if and only if the functor $Com_C(-, Q) : \mathcal{M}^C \to Ab$ is exact. A right C-comodule M is called coflat if the cotensor functor $M \square_C - : {}^C\mathcal{M} \to_k \mathcal{M}$ is exact.
If $M \in \mathcal{M}^C$, then an object $Q \in \mathcal{M}^C$ is called M-injective if for any subcomodule M' of M, and for any $f \in Com_C(M', Q)$ there exists $g \in Com_C(M, Q)$ such that $g_{|M'} = f$, where by $g_{|M'}$ we denote the restriction of g to M'. Clearly, an object $Q \in \mathcal{M}^C$ is injective if and only if Q is M-injective for any $M \in \mathcal{M}^C$.

Theorem 2.4.17 *Let Q be a right C-comodule. The following assertions are equivalent.*
(i) Q is an injective comodule.
(ii) Q is M-injective for any right C-comodule M of finite dimension.
(iii) For any two-sided ideal I of C^* which is closed and has finite codimension and for any morphism of left C^*-modules $f : I \to Q$ there exists $q \in Q$ such that $f(\lambda) = \lambda q$ for any $\lambda \in I$.
(iv) Q is a right coflat comodule.

Proof: $(i) \Rightarrow (ii)$ is obvious.
$(ii) \Rightarrow (i)$ Let X be an arbitrary object of $\mathcal{M}^C$. Then there exist a family $(M_i)_{i \in I}$ of finite dimensional C-comodules and an epimorphism $\phi : \oplus_{i \in I} M_i \to X$. Denote $Y = \oplus_{i \in I} M_i$ and $Z = Ker(\phi)$. If X' is a subcomodule of X, then there exists $Y' \leq Y$ such that $Y'/Z \simeq X'$. The commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Z & \longrightarrow & Y & \longrightarrow & X & \longrightarrow & 0 \\ & & \| & & \cup & & \cup & & \\ 0 & \longrightarrow & Z & \longrightarrow & Y' & \longrightarrow & X' & \longrightarrow & 0 \end{array}$$

produces a commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & Com(X',Q) & \longrightarrow & Com(Y',Q) & \longrightarrow & Com(Z,Q) \\
 & & \downarrow & & \downarrow & & \| \\
0 & \longrightarrow & Com(X,Q) & \longrightarrow & Com(Y,Q) & \longrightarrow & Com(Z,Q)
\end{array}$$

If we assume that the natural morphism $Com_C(Y',Q) \to Com_C(Y,Q)$ is surjective, we obtain that the morphism $Com_C(X',Q) \to Com_C(X,Q)$ is surjective. Therefore for proving $(ii) \Rightarrow (i)$ it is enough to show that Q is Y-injective. For this, we will show that if Q is M_i-injective for any $i \in I$, then Q is $\oplus_{i\in I} M_i$-injective. Denote $M = \oplus_{i\in I} M_i$ and take $K \leq M$ and $f \in Com_C(K,Q)$. We consider the set

$$\mathcal{P} = \{(L,g) | K \leq L \leq M, g \in Com_C(L,Q) \text{ and } g_{|K} = f\}$$

which can be ordered as follows. If (L,g) and (L',g') are two elements of $\mathcal{P}$, the $(L,g) \leq (L',g')$ if and only if $L \subseteq L'$ and $g = g'_L$. A standard argument shows that $\mathcal{P}$ is inductive, and by applying Zorn's Lemma we can find a maximal element (L_0, f_0).
We show that $M_i \subseteq L_0$ for any $i \in I$. If there were some $i_0 \in I$ such that M_{i_0} is not contained in L_0, let us denote by h the restriction of f_0 to $L_0 \cap M_{i_0}$, $h : L_0 \cap M_{i_0} \to Q$. Since Q is M_{i_0}-injective, there exists a morphism $\overline{h} : M_{i_0} \to Q$ such that the restriction of $\overline{h}$ to $L_0 \cap M_{i_0}$ is h. Clearly L_0 is strictly contained in $L_0 + M_{i_0}$. We define $\overline{f_0} : L_0 + M_{i_0} \to Q$ by $\overline{f_0}(x+y) = f_0(x) + \overline{h}(y)$ for any $x \in L_0$ and $y \in M_{i_0}$. The morphism $\overline{f_0}$ is correctly defined, since for $x, x' \in L_0$ and $y, y' \in M_{i_0}$ such that $x + y = x' + y'$, we have $y - y' = x' - x \in L_0 \cap M_{i_0}$, so

$$\overline{h}(y-y') = h(y-y') = f_0(x'-x)$$

thus $f_0(x) + \overline{h}(y) = f_0(x') + \overline{h}(y')$. Since the restriction of $\overline{f_0}$ to L_0 is f_0 and $L_0 \neq L_0 + M_{i_0}$, we obtain a contradiction.
$(i) \Rightarrow (iii)$ is clear.
$(iii) \Rightarrow (i)$ We know that the set

$$\mathcal{G} = \{C^*/I | I \text{ a closed two} - \text{sided ideal of finite codimension of } C^*\}$$

is a family of generators of the category $Rat(_{C^*}\mathcal{M}) \simeq \mathcal{M}^C$ (see Theorem 2.2.14). Let U be the direct sum of all the elements of $\mathcal{G}$, which is a generator of $\mathcal{M}^C$. Since Q is M-injective for any $M \in \mathcal{G}$, we see as in the

proof of $(ii) \Rightarrow (i)$ that Q is U-injective, and hence that Q is $U^{(I)}$-injective for any non-empty set I.
If $M \in \mathcal{M}^C$, there exist a non-empty set I and an epimorphism $U^{(I)} \longrightarrow M$. With the same argument as in the proof of $(ii) \Rightarrow (i)$ we see that Q is M-injective. Thus Q is injective.
$(i) \Rightarrow (iv)$ If Q is injective in $\mathcal{M}^C$, then $C^{(J)} \simeq Q \oplus Q'$ as C-comodules for some set J and for some C-comodule Q'. Let us consider an exact sequence of left C-comodules

$$0 \longrightarrow N' \xrightarrow{u} N \xrightarrow{v} N'' \longrightarrow 0$$

By cotensoring with Q we obtain an exact sequence of abelian groups

$$0 \longrightarrow Q\square_C N' \xrightarrow{I\square u} Q\square_C N \xrightarrow{I\square v} Q\square_C N''$$

We show that $I\square v$ is surjective. This is clear in the case where $Q = C^{(J)}$, since

$$Q\square_C N \simeq (C\square_C N)^{(J)} \simeq N^{(J)}$$

In general, if $C^{(J)} \simeq Q \oplus Q'$, we have an exact sequence

$$(Q \oplus Q')\square_C N \xrightarrow{I\square v} (Q \oplus Q')\square_C N'' \longrightarrow 0$$

We have the commutative diagram

$$\begin{tikzcd}
(Q \oplus Q')\square_C N \arrow[r, "I\square v"] \arrow[d] & (Q \oplus Q')\square_C N'' \arrow[r] \arrow[d] & 0 \\
Q\square_C N \arrow[r, "I\square v"] \arrow[d] & Q\square_C N'' \arrow[d] & \\
0 & 0 &
\end{tikzcd}$$

which shows that $I_Q\square v$ is surjective, i.e. Q is a right coflat comodule.
$(iv) \Rightarrow (ii)$ If M is a finite dimensional right C-comodule, then $M^* = Hom_k(M, k)$ is a finite dimensional left C-comodule. On the other hand

$$Q\square_C M^* \simeq Com_C(M^{**}, Q) \simeq Com_C(M, Q)$$

(where the first isomorphism comes from Proposition 2.3.7). Since Q is coflat we obtain that Q is M-injective. ∎

Corollary 2.4.18 *Let P be a projective left C-comodule. Then $Rat(_{C^*}P^*)$ is an injective right C-comodule.*

Proof: By Theorem 2.4.17 it is enough to show that $Rat(_{C^*}P^*)$ is N-injective for any finite dimensional right C-comodule N. Let N be such an object, $u : N' \to N$ an injective morphism of comodules and $f : N' \to Rat(P^*_{C^*})$ a morphism of right C-comodules. Regard f as a morphism from N' to P^*, and take the dual morphism $f^* : P^{**} \to N'^*$. If $\alpha : P \to P^{**}$ is the natural injection, $\alpha(p)(p^*) = p^*(p)$ for any $p \in P, p^* \in P^*$, then $f^*\alpha : P \to N'^*$ and $u^* : N^* \to N'^*$ is a surjective morphism. Since N and N' are finite dimensional right C-comodules, we have that N^* and N'^* are left C-comodules, and then since P is a projective left C-comodule, there exists a comodule morphism $g : P \to N^*$ such that $u^*g = f^*\alpha$. Taking the dual, this implies that $(f^*\alpha)^* = g^*u^{**}$. If $\alpha_N : N \to N^{**}$ and $\alpha_{N'} : N' \to N'^{**}$ are the natural injections, we have that

$$g^*\alpha_N u = g^*u^{**}\alpha_{N'} = (f^*\alpha)^*\alpha_{N'} = f$$

where the last equality follows from the following easy computation.

$$\begin{aligned}
(((f^*\alpha)^*\alpha_{N'})(n))(p) &= ((f^*\alpha)^*(\alpha_{N'}(n)))(p)\\
&= (\alpha_{N'}(n)f^*\alpha)(p)\\
&= (\alpha_{N'}(n)f^*)(\alpha(p))\\
&= \alpha_{N'}(n)(\alpha(p)f)\\
&= (\alpha(p)f)(n)\\
&= \alpha(p)(f(n))\\
&= f(n)(p)
\end{aligned}$$

for any $n \in N, p \in P$. Since $\alpha_N g^*$ is a morphism of left C^*-modules and N is rational, we can regard $\alpha_N g^*$ as a morphism from N to $Rat(_{C^*}P^*)$, showing that $Rat(_{C^*}P^*)$ is N-injective. ∎

Corollary 2.4.19 *Let Q be a finite dimensional right C-comodule. Then Q is injective (projective) as a left C^*-module if and only if it is injective (projective) as a right C-comodule.*

Proof: We only have to show the if part. Assume that Q is injective in $\mathcal{M}^C$. Since Q is finite dimensional, there exist a positive integer n and a right C-comodule Q' such that $C^n \simeq Q \oplus Q'$. Applying the functor $Hom_k(-, k)$ we obtain that $C^{*\,n} \simeq Q^* \oplus Q'^*$ as right C^*-modules, so Q^* is a projective right C^*-module. Lemma 2.2.15 implies that $Q \simeq (Q^*)^*$ is an injective left C^*-module.

Assume now that Q is a projective object in $\mathcal{M}^C$. Since the functor $Hom_k(-,k)$ defines a duality between the category of finite dimensional right C-comodules and the category of finite dimensional left C-comodules, we see that Q^* is an injective object in the category of finite dimensional left C-comodules. Theorem 2.4.17 shows that Q^* is an injective object in ${}^C\mathcal{M}$, so there exist a positive integer n and a left C-comodule X such that $C^n \simeq Q^* \oplus X$. Then

$$C^{*\,n} \simeq Q^{**} \oplus X^* \simeq Q \oplus X^*$$

showing that Q is a projective left C^*-module. ∎

Corollary 2.4.20 *Let M be a finite dimensional right C-comodule. Then M is an injective right C-comodule if and only if M^* is a projective left C-comodule.*

Proof: If M^* is projective as a left C-comodule, then $M \simeq (M^*)^*$ is an injective right C-comodule by Theorem 2.4.17.
Conversely, assume that M is an injective right C-comodule. The proof of Corollary 2.4.18 shows that M^* is a projective right C^*-module, i.e. M^* is a projective object in the category $Rat(\mathcal{M}_{C^*})$. Then M^* is a projective object in ${}^C\mathcal{M}$. ∎

We say that a Grothendieck category $\mathcal{A}$ has enough projectives if for any object $M \in \mathcal{A}$ there exist a projective object $P \in \mathcal{A}$ and an epimorphism $P \longrightarrow M$ in $\mathcal{A}$.

Corollary 2.4.21 *Let C be a coalgebra. The following assertions are equivalent.*
(i) The injective envelope of any finite dimensional right C-comodule in the category $\mathcal{M}^C$ is finite dimensional.
(ii) The injective envelope of any simple right C-comodule in the category $\mathcal{M}^C$ is finite dimensional.
(iii) If N is a finite dimensional left C-comodule, then there exist a finite dimensional projective left C-comodule P and an epimorphism $P \longrightarrow N$ in the category ${}^C\mathcal{M}$.
(iv) The category ${}^C\mathcal{M}$ has enough projective objects.

Proof: $(i) \Leftrightarrow (ii)$ is immediate.
$(i) \Leftrightarrow (iii)$ follows from Corollary 2.4.19.
$(iii) \Rightarrow (iv)$ follows from the fact that the family of all finite dimensional left C-comodules is a family of generators in the category ${}^C\mathcal{M}$.
$(iv) \Rightarrow (iii)$ Let $N \in {}^C\mathcal{M}$. By the hypothesis there exist a projective object P of ${}^C\mathcal{M}$ and an epimorphism $P \longrightarrow N$. Since the family of all finite

dimensional left C-comodules is a family of generators for the category ${}^C\mathcal{M}$, we can find a family $(X_i)_{i\in I}$ of finite dimensional left C-comodules and an epimorphism $\oplus_{i\in I}X_i \longrightarrow P$ in the category ${}^C\mathcal{M}$. Since P is projective, it is a direct summand of $\oplus_{i\in I}X_i$. We can clearly assume that all the X_i's are indecomposable. Then a result of Crawley, Jonsson and Warfield (see [3, Corollary 26.6, page 300]) shows that $P \simeq \oplus_{i\in J}X_i$ for some subset $J \subseteq I$. Since N has finite dimension we can find a finite subset K of J and an epimorphism $\oplus_{i\in K}X_i \longrightarrow N$. Any X_i, $i \in K$, is projective, as a direct summand of P, and then so is $\oplus_{i\in K}X_i$. Moreover $\oplus_{i\in K}X_i$ is finite dimensional, which ends the proof. ∎

Corollary 2.4.22 *Let P be a projective object in the category $\mathcal{M}^C$. Then P is projective in the category ${}_{C^*}\mathcal{M}$. Moreover, $Rat(P^*_{C^*})$ is dense in P^*.*

Proof: There exist a family $(M_i)_{i\in I}$ of finite dimensional right C-comodules and an epimorphism $\oplus_{i\in I}M_i \longrightarrow P$ of right C-comodules. Then P is a direct summand of $\oplus_{i\in I}M_i$, so there exists a right C-comodule N such that $\oplus_{i\in I}M_i \simeq P \oplus N$. By the Theorem of Crawley-Jonsson-Warfield we obtain that $P = \oplus_{j\in J}P_j$, where P_j are finite dimensional projective left C-comodules (in fact we can assume more, that the P_j's are indecomposable). By Corollary 2.4.19 we have that P_j is a projective left C^*-module for any j, so P is also a projective left C^*-module. On the other hand P^* is a direct summand in $(\oplus_{i\in I}M_i)^* \simeq \prod_{i\in I} M_i^*$. Since $\oplus_{i\in I}M_i^*$ is dense in $\prod_{i\in I} M_i^*$ and $\oplus_{i\in I}M_i^* \subseteq Rat(\prod_{i\in I} M_i^*)$, we obtain that $Rat(P^*_{C^*})$ is dense in P^*. ∎

Exercise 2.4.23 *Let C and D be two coalgebras and $\phi : C \to D$ a coalgebra morphism. Show that the following are equivalent.*
(i) C is an injective (coflat) left D-comodule.
(ii) Any injective (coflat) left C-comodule is also injective (coflat) as a left D-comodule.
(iii) The functor $(-)^\phi = -\square_D C : \mathcal{M}^D \to \mathcal{M}^C$ is exact.

2.5 Some topics on torsion theories on $\mathcal{M}^C$

Let $\mathcal{A}$ be a Grothendieck category and $\mathcal{C}$ a full subcategory of $\mathcal{A}$. Then $\mathcal{C}$ is called a closed subcategory if $\mathcal{C}$ is closed under subobjects, quotient objects and direct sums. If $\mathcal{C}$ is furthermore closed under extensions, then $\mathcal{C}$ is called a localizing subcategory of $\mathcal{A}$. A closed subcategory of a Grothendieck category is also a Grothendieck category. Indeed, if $U \in \mathcal{A}$ is a generator of $\mathcal{A}$, then

$$\{U/K | K \in \mathcal{A} \text{ and } U/K \in \mathcal{C}\}$$

is a family of generators of $\mathcal{C}$, and then the direct sum of this family is a generator of $\mathcal{C}$.
If $\mathcal{C}$ is closed, then for any $M \in \mathcal{A}$ we denote by $t_{\mathcal{C}}(M)$ the sum of all subobjects of M which belong to $\mathcal{C}$. In this way we define a left exact functor $t_{\mathcal{C}} : \mathcal{A} \longrightarrow \mathcal{A}$, called the preradical functor associated to $\mathcal{C}$. An object $M \in \mathcal{A}$ is called a $\mathcal{C}$-torsion object if $t_{\mathcal{C}}(M) = M$, and this is clearly equivalent to $M \in \mathcal{C}$. If $t_{\mathcal{C}}(M) = 0$, then M is called a $\mathcal{C}$-torsionfree object.
If $\mathcal{C}$ is a localizing subcategory, we have that $t_{\mathcal{C}}(M/t_{\mathcal{C}}(M)) = 0$ for any $M \in \mathcal{A}$, since $\mathcal{C}$ is closed under extensions. In this case $t_{\mathcal{C}}$ is called a radical functor.
Following [216, Chapter VI], a closed subcategory $\mathcal{C}$ of $\mathcal{A}$ is called a hereditary pretorsion theory, and a localizing subcategory of $\mathcal{A}$ is called a hereditary torsion theory in $\mathcal{A}$.
If $\mathcal{A}$ is a Grothendieck category and $M \in \mathcal{A}$ is an object, we denote by $\sigma_{\mathcal{A}}[M]$ (or shortly $\sigma[M]$) the class of all objects of $\mathcal{A}$ which are subgenerated by M, i.e. which are isomorphic to subobjects of quotient objects of direct sums of copies of M. Dually, we denote by $\sigma'_{\mathcal{A}}[M]$ (or shortly $\sigma'[M]$) the class of all objects of $\mathcal{A}$ which are isomorphic to quotient objects of subobjects of direct sums of copies of M.

Proposition 2.5.1 *With the above notation, the following assertions are true.*
(i) $\sigma[M]$ is the smallest closed subcategory of $\mathcal{A}$ containing M.
(ii) $\sigma[M] = \sigma'[M]$.
(iii) If $\mathcal{C}$ is a closed subcategory of $\mathcal{A}$, there exists an object $M \in \mathcal{A}$ such that $\mathcal{C} = \sigma[M]$.

Proof: (i) Since the direct sum functor is exact, we obtain that $\sigma[M]$ is closed to direct sums. Let now

$$0 \longrightarrow Y' \longrightarrow Y \longrightarrow Y'' \longrightarrow 0$$

be an exact sequence in $\mathcal{A}$ such that $Y \in \sigma[M]$. The definition of $\sigma[M]$ shows immediately that $Y' \in \sigma[M]$. Since $Y \in \sigma[M]$, there exist an epimorphism $f : M^{(I)} \longrightarrow X$ and a monomorphism $u : Y \longrightarrow X$. We have that $Y'' \simeq Y/Y'$ and $Y/Y' \leq X/Y' = X''$, so X'' is a quotient object of X, and then it is also a quotient object of $M^{(I)}$, and then $Y'' \in \sigma[M]$. Thus $\sigma[M]$ is a closed subcategory of $\mathcal{A}$.
Assume that $\mathcal{C}$ is a closed subcategory of $\mathcal{A}$ such that $M \in \mathcal{C}$. Then for Y, f and u as above, we have that $M^{(I)} \in \mathcal{C}$, so $X \in \mathcal{C}$, showing that $Y \in \mathcal{C}$. Therefore $\sigma[M] \subseteq \mathcal{C}$.
(ii) The definition tells us that an object $Y \in A$ is in $\sigma'_{\mathcal{A}}[M]$ if and only if there exist a set I, a subobject X of $M^{(I)}$, and a morphism $f : X \longrightarrow Y$

with $Im(f) = Y$. Since $\sigma_{\mathcal{A}}[M]$ is closed under direct sums, subobjects and quotient objects, we obviously have that $\sigma'_{\mathcal{A}}[M] \subseteq \sigma_{\mathcal{A}}[M]$.
Since $M \in \sigma'_{\mathcal{A}}[M]$ and $\sigma_{\mathcal{A}}[M]$ is the smallest closed subcategory containing M, in order to prove that $\sigma_{\mathcal{A}}[M] \subseteq \sigma'_{\mathcal{A}}[M]$, it is enough to show that $\sigma'_{\mathcal{A}}[M]$ is closed. Clearly $\sigma'_{\mathcal{A}}[M]$ is closed under direct sums and homomorphic images. Assume that $Y \in \sigma'_{\mathcal{A}}[M]$ (with I, f and X as above) and let Y' be a subobject of Y. Then $X' = f^{-1}(Y')$ is a subobject of $M^{(I)}$, and Y' is a homomorphic image of X' (via the restriction and the corestriction of f). Thus $Y' \in \sigma'_{\mathcal{A}}[M]$, so $\sigma'_{\mathcal{A}}[M]$ is also closed under subobjects.
(iii) Since $\mathcal{C}$ is a closed subcategory of $\mathcal{A}$, then $\mathcal{C}$ is a Grothendieck category. If U is a generator of $\mathcal{A}$, the family

$$\{U/U' | U' \leq U \text{ and } U/U' \in \mathcal{C}\}$$

is a family of generators of $\mathcal{C}$. Then the direct sum of this family

$$M = \oplus_{U' \leq U, U/U' \in \mathcal{C}} U/U'$$

is a generator of the category $\mathcal{C}$ and clearly $\mathcal{C} = \sigma[M]$. ∎

If C is a coalgebra, then the category $\mathcal{M}^C$ is a Grothendieck category which is isomorphic to the category $Rat({}_{C^*}\mathcal{M})$ of rational left C^*-modules.

Corollary 2.5.2 *We have that $Rat({}_{C^*}\mathcal{M}) = \sigma[{}_{C^*}C]$.*

Proof: Clearly any object of $\sigma[{}_{C^*}C]$ is rational, so we have that $\sigma[{}_{C^*}C] \subseteq Rat({}_{C^*}\mathcal{M})$. Conversely, if $M \in Rat({}_{C^*}\mathcal{M})$, then M is a right C-comodule, and then there exists a nonempty set I such that M is isomorphic as a C-comodule to a subobject of a direct sum $C^{(I)}$ of copies of C. Regarding this in the category ${}_{C^*}\mathcal{M}$, it means that $M \in \sigma[{}_{C^*}C]$. ∎

Proposition 2.5.3 *Let C be a coalgebra. Then the following assertions hold.*
(i) If I is a left ideal of C^*, then $I^\perp = ann_C(I) = \{c \in C | I \rightharpoonup c = 0\}$.
(ii) If X is a left coideal of C, then $X^\perp = ann_{C^*}(X)$, where

$$ann_{C^*}(X) = \{f \in C^* | f \rightharpoonup x = 0 \text{ for any } x \in X\}.$$

(iii) If $\rho : M \to M \otimes C$ is the comodule structure map of the right C-comodule M, and J is a two-sided ideal of C^* such that $JM = 0$, then $\rho(M) \subseteq M \otimes J^\perp$, i.e. M is a right comodule over the subcoalgebra $J^\perp$ of C.
(iv) If M is a right C-comodule and $A = (ann_{C^*}(M))^\perp$, then A is the smallest subcoalgebra of C such that $\rho(M) \subseteq M \otimes A$. The subcoalgebra A is called the coalgebra associated to the comodule M.

Proof: (i) Let $c \in ann_C(I)$. Then $f \rightharpoonup c = 0$ for any $f \in I$. Then

$$\begin{aligned} f(c) &= f(\sum \varepsilon(c_1)c_2) \\ &= \sum \varepsilon(f(c_2)c_1) \\ &= \varepsilon(f \rightharpoonup c) \\ &= 0 \end{aligned}$$

so $c \in I^\perp$.
Conversely, if $c \in I^\perp$, then $f(c) = 0$ for any $f \in I$. Let $\Delta(c) = \sum_{1 \le i \le n} x_i \otimes y_i$ with $(x_i)_{1 \le i \le n}$ linearly independent. If $1 \le t \le n$, there exists $g \in C^*$ such that $g(x_t) = 1$ and $g(x_i) = 0$ for any $i \ne t$. Then $gf \in I$ and

$$\begin{aligned} 0 &= (gf)(c) \\ &= \sum_{1 \le i \le n} g(x_i) f(y_i) \\ &= f(y_t) \end{aligned}$$

so $f(y_t) = 0$. Then $f \rightharpoonup c = \sum_{1 \le i \le n} f(y_i)x_i = 0$, which shows that $c \in ann_C(I)$. Thus $I^\perp \subseteq ann_C(I)$.
(ii) If $f \in X^\perp$ then $f(X) = 0$. Let $x \in X$. Then $f \rightharpoonup x = \sum f(x_2)x_1 = 0$, thus $x \in ann_{C^*}(X)$.
Conversely, assume that $f \in ann_{C^*}(X)$. Then for any $x \in X$ we have that

$$\begin{aligned} f(x) &= f(\sum \varepsilon(x_1)x_2) \\ &= \varepsilon(\sum f(x_2)x_1) \\ &= \varepsilon(f \rightharpoonup x) \\ &= 0 \end{aligned}$$

so $f \in X^\perp$.
(iii) For $m \in M$ let $\rho(m) = \sum m_0 \otimes m_1$, and assume that the m_0's are linearly independent. If $f \in J$ we have that $0 = fm = \sum f(m_1)m_0$, so $f(m_1) = 0$ for any m_1, thus $m_1 \in J^\perp$. We obtain that $\rho(M) \subseteq M \otimes J^\perp$.
(iv) Denote $J = ann_{C^*}(M)$. Then J is a two-sided ideal of C^* and by (iii) we have $\rho(M) \subseteq M \otimes A$, and $A = J^\perp$ is a subcoalgebra of C.
Assume that B is a subcoalgebra of C such that $\rho(M) \subseteq M \otimes B$. If $f \in B^\perp$ and $m \in M$, then $fm = 0$, so $B^\perp \subseteq ann_{C^*}(M) = J$. Thus $J^\perp \subseteq (B^\perp)^\perp = B$, and we find that $A \subseteq B$. ∎

Exercise 2.5.4 *Let M be a finite dimensional right C-comodule with comodule structure map $\rho : M \to M \otimes C$, $(m_i)_{i=1,n}$ a basis of M and*

$(c_{ij})_{1\le i,j\le n}$ be elements of C such that $\rho(m_i)=\sum_{1\le j\le n} m_j\otimes c_{ji}$ for any i. Show that the coalgebra A associated to M is the subspace of C spanned by the set $(c_{ij})_{1\le i,j\le n}$, and that $\Delta(c_{ji})=\sum_{1\le t\le n} c_{jt}\otimes c_{ti}$ and $\varepsilon(c_{ij})=\delta_{ij}$ for any i,j.

Theorem 2.5.5 *Let C be a coalgebra and A a subcoalgebra of C. We denote by*

$$\mathcal{C}_A=\{M\in\mathcal{M}^C \mid \rho_M(M)\subseteq M\otimes A\}$$

where ρ_M stands for the comodule structure map of M. Then the following assertions hold.
(i) $M\in\mathcal{C}_A$ if and only if $A^\perp M=0$.
(ii) $\mathcal{C}_A$ is a closed subcategory of $\mathcal{M}^C$.
(iii) The map $A\mapsto\mathcal{C}_A$ is a bijective correspondence between the set of all subcoalgebras of C and the set of all closed subcategories of $\mathcal{M}^C$.

Proof: (i) Assume that $M\in\mathcal{C}_A$ and $f\in A^\perp$. Then $f(A)=0$. Since $\rho_M(M)\subseteq M\otimes A$ we have $fm=\sum f(m_1)m_0$ with $m_0\in M$ and $m_1\in A$, so then $fm=0$, and $A^\perp M=0$. Conversely, if $A^\perp M=0$, by Proposition 2.5.3 we have $\rho_M(M)\subseteq M\otimes A^{\perp\perp}=M\otimes A$.
(ii) It is easy to see that (i) implies that $\mathcal{C}_A$ is closed under subobjects, quotient objects and direct sums.
(iii) Let $\mathcal{C}$ be a closed subcategory of $\mathcal{M}^C$. Since $\mathcal{M}^C\simeq Rat({}_{C^*}\mathcal{M})$, which is a closed subcategory of ${}_{C^*}\mathcal{M}$, we have that $\mathcal{C}$ is a closed subcategory of ${}_{C^*}\mathcal{M}$. Since C is a left-C, right-C bicomodule, we also have that C is a left-C^*, right-C^* bimodule. Let $A=t_{\mathcal{C}}({}_{C^*}C)$, where $t_{\mathcal{C}}$ is the preradical associated to the closed subcategory $\mathcal{C}$ of ${}_{C^*}\mathcal{M}$. Then A is a left C^*-submodule of ${}_{C^*}C$. For any $g\in C^*$ the map $u_g: C\to C, u_g(c)=c\leftharpoonup g$ is a morphism of left C^*-modules. $\mathcal{C}$ is closed under quotient objects, so $u(A)\subseteq A$, i.e. $A\leftharpoonup g\subseteq A$. We obtain that A is a left-C^*, right-C^* subbimodule of ${}_{C^*}C_{C^*}$.
If we consider A as a comodule, then we have $\Delta(A)\subseteq A\otimes C$ and $\Delta(A)\subseteq C\otimes A$, so $\Delta(A)\subseteq(A\otimes C)\cap(C\otimes A)=A\otimes A$, showing that A is a subcoalgebra of C. It is clear that A, regarded as a right C-comodule, belongs to $\mathcal{C}$. Let $M\in\mathcal{C}$. Then there exists a monomorphism

$$0\longrightarrow M\longrightarrow C^{(I)}$$

for some non-empty set I. Since $t_{\mathcal{C}}$ is an exact functor which commutes with direct sums, we obtain an exact sequence

$$0\longrightarrow M\longrightarrow t_{\mathcal{C}}(C)^{(I)}$$

i.e. an exact sequence of right C-comodules

$$0\longrightarrow M\longrightarrow A^{(I)}$$

Since $A^{\perp}(A^{(I)}) = 0$, then $A^{\perp}M = 0$ and $M \in \mathcal{C}_A$ by assertion (i). Thus $\mathcal{C} \subseteq \mathcal{C}_A$. Conversely, if $M \in \mathcal{C}_A$, then $\rho_M(M) \subseteq M \otimes A$, so M is a right A-comodule. Thus there exists a right C-comodule morphism

$$0 \longrightarrow M \longrightarrow A^{(I)}$$

for some non-empty set I. Since $A \in \mathcal{C}$ we have $M \in \mathcal{C}$, therefore $\mathcal{C} = \mathcal{C}_A$. We have obtained that the correspondence $A \mapsto \mathcal{C}_A$ is surjective. Now if B is another subcoalgebra of C and $\mathcal{C}_A = \mathcal{C}_B$, then clearly $A \in \mathcal{C}_B$ and $B \in \mathcal{C}_A$, so $A^{\perp} \rightharpoonup B = 0$ and $B^{\perp} \rightharpoonup A = 0$. Proposition 2.5.3 shows that $B \subseteq A^{\perp\perp} = A$, and $A \subseteq B^{\perp\perp} = B$. Thus $A = B$, which ends the proof. ∎

Corollary 2.5.6 *If $\mathcal{C}$ is a closed subcategory of $\mathcal{M}^C$, then $\mathcal{C}$ is closed to direct products.*

Proof: Let $(M_i)_{i\in I}$ be a family of objects of $\mathcal{C}$. Since $\mathcal{C} = \mathcal{C}_A$ for some subcoalgebra A of C, we have that $A^{\perp}(\prod_{i\in I} M_i) = 0$, where M_i is considered as a left C^*-module. Since $Rat({}_{C^*}\mathcal{M})$ is a closed subcategory of ${}_{C^*}\mathcal{M}$, it is easy to see that $(\prod_{i\in I} M_i)^{rat}$ is the direct product of the family $(M_i)_{i\in I}$ in the category $Rat({}_{C^*}\mathcal{M}) \simeq \mathcal{M}^C$. On the other hand $(\prod_{i\in I} M_i)^{rat} \subseteq \prod_{i\in I} M_i$, so $A^{\perp}(\prod_{i\in I} M_i)^{rat} = 0$, i.e. $(\prod_{i\in I} M_i)^{rat} \in \mathcal{C}$. Thus $\mathcal{C}$ is closed to direct products. ∎

We introduce now some notation. For any subspaces X and Y of the coalgebra C we denote by $X \wedge Y$ the subspace

$$X \wedge Y = \Delta^{-1}(X \otimes C + C \otimes Y)$$

The subspace $X \wedge Y$ is called the wedge of the subspaces X and Y. We define recurrently $\wedge^0 X = 0$, $\wedge^1 X = X$, and $\wedge^n X = (\wedge^{n-1} X) \wedge X$ for any $n \geq 2$. With this notation we have the following.

Lemma 2.5.7 *For any subspaces X and Y of the coalgebra C we have that $X \wedge Y = (X^{\perp}Y^{\perp})^{\perp}$.*
In particular, if A is a subcoalgebra of C, then for any positive integer n we have that $\wedge^n A = (J^n)^{\perp}$, where $J = A^{\perp}$.

Proof: Let $f \in X^{\perp}$ and $g \in Y^{\perp}$, then since $\Delta(X \wedge Y) \subseteq X \otimes C + C \otimes Y$ we see that $(fg)(X \wedge Y) = 0$, so $X \wedge Y \subseteq (X^{\perp}Y^{\perp})^{\perp}$. Conversely, let $c \in (X^{\perp}Y^{\perp})^{\perp}$. We can write

$$\Delta(c) = \sum_{1\leq i\leq m} x_i \otimes y_i + \sum_{1\leq j\leq n} z_j \otimes u_j$$

where the set $\{x_i | 1 \leq i \leq m\} \cup \{z_j | 1 \leq j \leq n\}$ is linearly independent, $x_i \in X$ for any i and z_j belongs to a complement of X for any j. Fix

some j_1. Then there exists $f \in C^*$ such that $f(X) = 0$, $f(z_{j_1}) = 1$, and $f(z_j) = 0$ for any $j \neq j_1$. For any $g \in Y^\perp$ we have that $fg \in X^\perp Y^\perp$, so $(fg)(c) = 0$. But $(fg)(c) = g(u_j)$, and we obtain that $u_j \in (Y^\perp)^\perp = Y$. Thus $\Delta(c) \in X \otimes C + C \otimes Y$, i.e. $c \in X \wedge Y$.
We prove the second statement by induction on n. It is obvious for $n = 1$. Assume the assertion holds for some n. Then

$$\begin{aligned} \wedge^{n+1} A &= (\wedge^n A) \wedge A \\ &= (J^n)^\perp \wedge A \quad \text{(induction hypothesis)} \\ &= ((J^n)^{\perp\perp} J)^\perp \quad \text{(by the first part)} \\ &= (\overline{J^n} J)^\perp \end{aligned}$$

where $\overline{J^n}$ is the closure of J^n. We clearly have the inclusion $(\overline{J^n} J)^\perp \subseteq (J^{n+1})^\perp$. Let now take some $c \in (J^{n+1})^\perp$. By Proposition 2.5.3(i) we have that $J^{n+1} \rightharpoonup c = 0$, so $J^n \rightharpoonup (J \rightharpoonup c) = 0$. Thus $J^n \rightharpoonup x = 0$ for any $x \in J \rightharpoonup c$, i.e. $J^n \subseteq ann_{C^*}(x)$. By Theorem 2.2.14, $ann_{C^*}(x)$ is closed, and then $\overline{J^n} \subseteq ann_{C^*}(x)$, so $\overline{J^n} \rightharpoonup x = 0$ for any $x \in J \rightharpoonup c$. Then $\overline{J^n} \rightharpoonup (J \rightharpoonup c) = 0$ and $c \in (\overline{J^n} J)^\perp$. We obtain that $\wedge^{n+1} A = (J^{n+1})^\perp$. ∎

Exercise 2.5.8 *Let C be a coalgebra and X, Y, Z three subspaces of C. Show that $(X \wedge Y) \wedge Z = X \wedge (Y \wedge Z)$.*

Exercise 2.5.9 *Let $f : C \to D$ be a coalgebra morphism and X, Y subspaces of C. Show that $f(X \wedge Y) \subseteq f(X) \wedge f(Y)$.*

A subcoalgebra A of C is called co-idempotent if $A \wedge A = A$. Clearly, if $J = A^\perp$ is an idempotent two-sided ideal of C^*, then A is a co-idempotent subcoalgebra. Keeping the same notation as in Theorem 2.5.5 we have the following.

Theorem 2.5.10 *Let C be a coalgebra and let A be a subcoalgebra of C. Then the following assertions hold.*
(i) If A is co-idempotent, then $\mathcal{C}_A$ is a localizing subcategory of $\mathcal{M}^C$.
(ii) The map $A \mapsto \mathcal{C}_A$ defines a bijective correspondence between the set of all co-idempotent subcoalgebras of C and the set of all localizing subcategories of $\mathcal{M}^C$.

Proof: (i) Taking into account Theorem 2.5.5, it remains to prove that $\mathcal{C}_A$ is closed under extensions. Let

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

be an exact sequence in $\mathcal{M}^C$ with $M', M'' \in \mathcal{C}_A$. If we put $J = A^\perp$, then $JM' = JM'' = 0$, and then $J^2 M = 0$. So $\rho_M(M) \subseteq M \otimes (J^2)^\perp$. Since A

is co-idempotent we have $A = A \wedge A = (J^2)^\perp$, so $\rho_M(M) \subseteq M \otimes A$ and $M \in \mathcal{C}_A$.

(ii) Let $\mathcal{C}$ be a localizing subcategory of $\mathcal{M}^C$. By Theorem 2.5.5 there exists a subcoalgebra A of C such that $\mathcal{C} = \mathcal{C}_A$. It remains to prove that $A = A \wedge A$. Clearly $A \subseteq A \wedge A$. Denote $M = (\wedge^2 A)/A$, and we have an exact sequence of right C-comodules

$$0 \longrightarrow A \longrightarrow \wedge^2 A \longrightarrow (\wedge^2 A)/A \longrightarrow 0$$

Clearly $A^\perp \rightharpoonup A = 0$ and $A \in \mathcal{C}_A$. On the other hand

$$A^\perp \rightharpoonup (\wedge^2 A) = J \rightharpoonup (J^2)^\perp = 0$$

But $\wedge^2 A = \{c \in C | J^2 \rightharpoonup c = 0\}$ by Proposition 2.5.3, so for any $c \in \wedge^2 A$ we have $J \rightharpoonup (J \rightharpoonup c) = 0$, which means that $J \rightharpoonup c \subseteq J^\perp = A$. Then $A^\perp \rightharpoonup (\wedge^2 A) = 0$, so $A^\perp M = 0$. Since $\mathcal{C}_A$ is closed under extensions, we have that $\wedge^2 A \in \mathcal{C}_A$. Finally, since $A \subseteq \wedge^2 A$ and $\wedge^2 A$ is a subcoalgebra, we obtain by Theorem 2.5.5 that $A = \wedge^2 A$. ∎

We present now some generalizations of the finite dual of an algebra. Let A be a k-algebra. We denote by $Id_{f.c}(A)$ the set of all two-sided ideals of A of finite codimension. $Id_{f.c}(A)$ is a filter, i.e. it is closed to finite intersections and if $I \subseteq J$ are two-sided ideals such that $I \in Id_{f.c}(A)$, then $J \in Id_{f.c}(A)$. Let γ be a subfilter of $Id_{f.c}(A)$, i.e. $\gamma \subseteq Id_{f.c}(A)$, if $I, J \in \gamma$ then $I \cap J \in \gamma$, and for any two-sided ideals $I \subseteq J$ with $I \in \gamma$, we also have that $J \in \gamma$. We denote by

$$A^{\circ,\gamma} = \varinjlim_{I \in \gamma} (A/I)^*$$

Since $(A/I)^*$ can be embedded in A^* for any I, we have that

$$A^{\circ,\gamma} = \{f \in A^* |\text{ there exists } I \in \gamma \text{ such that } I \subseteq Ker(f)\}$$

If $\gamma = Id_{f.c}(A)$, then $A^{\circ,\gamma} = A^\circ$, the finite dual of the algebra A defined in Section 1.5.

Proposition 2.5.11 *$A^{\circ,\gamma}$ has a natural structure of a coalgebra.*

Proof: If $I \in \gamma$, since I has finite codimension in A we have a natural monomorphism

$$0 \longrightarrow (A/I)^* \longrightarrow (A/I)^* \otimes (A/I)^*$$

If we apply the inductive limit functor we obtain a monomorphism

$$0 \longrightarrow \varinjlim_{I \in \gamma} (A/I)^* \longrightarrow \varinjlim_{I \in \gamma} ((A/I)^* \otimes (A/I)^*)$$

On the other hand we have a natural morphism

$$(A/I)^* \otimes (A/I)^* \longrightarrow \varinjlim_{I\in\gamma}(A/I)^* \otimes \varinjlim_{I\in\gamma}(A/I)^*$$

and by the universal property of the inductive limit we obtain a natural morphism

$$\Delta^\gamma : A^{\circ,\gamma} \longrightarrow A^{\circ,\gamma} \otimes A^{\circ,\gamma}$$

As in the case of A°, a standard argument shows that Δ^γ is coassociative. The counit $\varepsilon : A^{\circ,\gamma} \to k$ is defined by $\varepsilon(a^*) = a^*(1)$ for $a^* \in A^{\circ,\gamma}$, i.e. $a^* \in (A/I)^*$ for some $I \in \gamma$. ∎

Remark 2.5.12 *If γ and γ' are two subfilters of $Id_{f.c}(A)$ such that $\gamma \subseteq \gamma'$, then we have $A^{\circ,\gamma} \subseteq A^{\circ,\gamma'} \subseteq A^\circ$.* ∎

Let $\phi : A \to B$ be a morphism of k-algebras, and let us consider two subfilters $\gamma \subseteq Id_{f.c}(A)$ and $\gamma' \subseteq Id_{f.c}(B)$ such that for any $J \in \gamma'$ we have $\phi^{-1}(J) \in \gamma$. The morphism ϕ induces a monomorphism

$$0 \longrightarrow A/\phi^{-1}(J) \longrightarrow B/J$$

for any $J \in \gamma'$. Then we have a natural epimorphism

$$(B/J)^* \longrightarrow (A/\phi^{-1}(J))^* \longrightarrow 0$$

and taking the inductive limit we obtain a natural morphism

$$B^{\circ,\gamma'} = \varinjlim_{J\in\gamma'} (B/J)^* \longrightarrow \varinjlim_{J\in\gamma'} (A/\phi^{-1}(J))^*$$

By the universal property of inductive limits we have a natural morphism

$$\varinjlim_{J\in\gamma'} (A/\phi^{-1}(J))^* \longrightarrow \varinjlim_{I\in\gamma}(A/I)^*$$

Therefore the algebra morphism $\phi : A \to B$ induces a natural morphism $\phi^{\circ,\gamma,\gamma'} : B^{\circ,\gamma'} \to A^{\circ,\gamma}$. By standard arguments one can show that $\phi^{\circ,\gamma,\gamma'}$ is a coalgebra morphism.

We recall that a k-algebra A is called pseudocompact if A is a separated and complete topological space which has a basis of neighbourhoods of 0 which are two-sided ideals of finite codimension. We denote by APC_k the category of all pseudocompact k-algebras. In this category morphisms are continuous algebra morphisms. If C is a k-coalgebra, then C^* is a pseudocompact k-algebra, and in this way we can define a contravariant functor $F : k - Cog \to APC_k$, $F(C) = C^*$.

Theorem 2.5.13 *The functor F defined above is an equivalence between the dual category $(k-Cog)^\circ$ and the category APC_k.*

Proof: For $A \in APC_k$ we take the subfilter γ of $Id_{f.c}(A)$ consisting of all open two-sided ideals of A. We can consider the coalgebra $A^{\circ,\gamma}$, and so we can define now a contravariant functor $G : APC_k \to k-Cog$ by $G(A) = A^{\circ,\gamma}$. Moreover, for $A \in APC_k$ we have that

$$\begin{aligned} F(G(A)) &= F(A^{\circ,\gamma}) \\ &= F(\varinjlim_{I\in\gamma}(A/I)^*) \\ &= (\varinjlim_{I\in\gamma}(A/I)^*)^* \\ &= \varprojlim_{I\in\gamma}(A/I)^{**} \\ &\simeq \varprojlim_{I\in\gamma} A/I \\ &\simeq A \end{aligned}$$

thus $FG \simeq Id_{APC_k}$. For the other composition, let C be a k-coalgebra. Then the set

$$\mathcal{B} = \{D^\perp | D \text{ is a finite dimensional subcoalgebra of } C\}$$

is a basis of neighbourhoods of 0 in the topological algebra C^*, and then

$$\begin{aligned} G(C^*) &= \varinjlim_{D\in\mathcal{B}}(C^*/D^\perp)^* \\ &\simeq \varinjlim_{D\in\mathcal{B}}(D^*)^* \\ &\simeq \varinjlim_{D\in\mathcal{B}} D \\ &= C \end{aligned}$$

so $GF \simeq Id_{k-Cog}$. ∎

Let A be a pseudocompact k-algebra. We denote by $MPC(A)$ the category of pseudocompact right A-modules, whose objects are all right A-modules that are pseudocompact (see Section 2.2) and with morphisms A-linear continuous maps. If C is a coalgebra and $M \in \mathcal{M}^C$, then M^* is a pseudocompact right C^*-module. The correspondence $M \mapsto M^*$ defines a contravariant functor $F : \mathcal{M}^C \to MPC(C^*)$.

Theorem 2.5.14 *With the above notation, the functor F defines an equivalence between the dual category $(\mathcal{M}^C)^\circ$ and the category $MPC(C^*)$.*

Proof: Let $M \in MPC(C^*)$ and N a right C^*-submodule of M such that N is open and N has finite codimension in M. Then $I = ann_{C^*}(M/N)$ is a two-sided ideal of C^* of finite codimension, and since the topology of M/N is discrete we see that I is open in C^*. The multiplication morphism

$$M/N \otimes C^*/I \longrightarrow M/N$$

defines a morphism

$$(M/N)^* \longrightarrow (C^*/I)^* \otimes (M/N)^*$$

If we take

$$M^\circ = \varinjlim_N (M/N)^*$$

where the inductive limit is taken over the open submodules N of M of finite codimension, then we have a natural morphism $\delta_{M^\circ} : M^\circ \to C \otimes M^\circ$ and standard arguments show that M° is a right C-comodule. Then the correspondence $M \mapsto M^\circ$ defines a contravariant functor $G : MPC(C^*) \to \mathcal{M}^C$, and as in Theorem 2.5.13 one can show that $GF \simeq Id_{\mathcal{M}^C}$ and $FG \simeq Id_{MPC(C^*)}$. ∎

2.6 Solutions to exercises

Exercise 2.1.8 *Use Theorem 2.1.7 to prove Theorem 1.4.7.*
Solution: Let C be a coalgebra, $c \in C$ and V a finite dimensional right subcomodule of C (i.e. $\Delta(V) \subseteq V \otimes C$) such that $c \in V$. If $\{v_i\}$ is a basis of V, we have

$$\Delta(v_i) = \sum v_j \otimes c_{ji},$$

and so

$$\sum v_k \otimes c_{kj} \otimes c_{ji} = \sum v_j \otimes \Delta(c_{ji}).$$

It follows that $\Delta(c_{ki}) = \sum c_{kj} \otimes c_{ji}$, and so the subspace spanned by V and the c_{ji}'s is a finite dimensional subcoalgebra containing c.

Exercise 2.2.17 *Let C be a coalgebra and $\phi_C : C \to C^{**}$ the natural injection. Then $\phi_C(Rat(_{C^*}C)) = Rat(_{C^*}C^{**})$.*
Solution: Since ϕ_C is injective we clearly have that $\phi_C(Rat(_{C^*}C)) \subseteq Rat(_{C^*}C^{**})$. Conversely, let $f \in Rat(_{C^*}C^{**})$. Theorem 2.2.14 tells that there exists a two-sided ideal I of C^*, which is closed, of finite codimension, and satisfies $If = 0$. Since for any $c^* \in I$ we have $(c^*f)(C^*) = 0$, we see that $f(I) = f(C^*I) = 0$, so $f \in (C^*/I)^*$. But $I = (I^\perp)^\perp$ since I is closed, so

$$C^*/I \simeq C^*/(I^\perp)^\perp \simeq (I^\perp)^*$$

Thus $f \in (I^{\perp})^{**}$. Since $I^{\perp}$ has finite dimension, then $I^{\perp} \simeq (I^{\perp})^{**}$ via the restriction of the morphism ϕ_C. In particular we can find some $x \in I^{\perp}$ such that $f = \phi_C(x)$, so we have that $Rat({}_{C^*}C^{**}) \subseteq \phi_C(Rat({}_{C^*}C))$.

Exercise 2.2.18 *Let $(C_i)_{i\in I}$ be a family of coalgebras and $C = \oplus_{i\in I}C_i$ the coproduct of this family in the category of coalgebras. Then the following assertions hold.*
(i) $C^* \simeq \prod_{i\in I} C_i^*$. Moreover, this is an isomorphism of topological rings if we consider the finite topology on C^* and the product topology on $\prod_{i\in I} C_i^*$.
(ii) If $M \in \mathcal{M}^C$ then for any $m \in M$ there exists a two-sided ideal I of C^* such that $Im = 0$, $I = \prod_{i\in I} I_i$, where I_i is a two-sided ideal of C_i^* which is closed and has finite codimension, and $I_i = C_i^*$ for all but a finite number of i's.
(iii) The category $\mathcal{M}^C$ is equivalent to the direct product of categories $\prod_{i\in I} \mathcal{M}^{C_i}$.
(iv) If A is a subcoalgebra of $C = \oplus_{i\in I}C_i$, then there exists a family $(A_i)_{i\in I}$ such that A_i is a subcoalgebra of C_i for any $i \in I$, and $A = \oplus_{i\in I}A_i$.
Solution: (i) Define the map $\phi : C^* \to \prod_{i\in I} C_i^*$ by $\phi(f) = (f_i)_{i\in I}$, where for $f \in C^* = Hom(C, k)$, f_i is the restriction of f to C_i for any $i \in I$. It is easy to see that if $f, g \in C^*$, then $(fg)_i = f_i g_i$ (the convolution product), so $\phi(fg) = \phi(f)\phi(g)$. Also, it is clear that ϕ is bijective. We prove now that ϕ is a morphism of topological rings. Let $f \in C^*$ and $c = \sum_{t=1,n} c_{i_t} \in C$ with $c_{i_t} \in C_{i_t}$. If $\phi(f) = (f_i)_{i\in I}$, then $f + c^{\perp} = \prod_{i\neq i_1,\dots,i_n} C_i \times \prod_{t=1,n}(f_{i_t} + C_{i_t}^{\perp})$, showing that ϕ is a morphism of topological rings.
(ii) By Theorem 2.2.14 there exists a closed (open) two-sided ideal I of C^* of finite codimension such that $Im = 0$. Let $A = I^{\perp}$, a finite dimensional subcoalgebra of C. Then there exist $i_1, \dots, i_n \in I$ such that $A \subseteq C_{i_1} \oplus \dots \oplus C_{i_n}$, and then $A^{\perp}$ is a two-sided ideal in $\prod_{1\leq t\leq n} C_{i_t}^*$. Then there exist two-sided ideals I_{i_t} of $C_{i_t}^*$ such that $A^{\perp} = \prod_{1\leq t\leq n} I_t$. It is easy to see that

$$I = I^{\perp\perp} = A^{\perp} = \prod_{t\in I} D_t$$

where $D_t = C_t^*$ for any $t \notin \{i_1, \dots, i_n\}$ and $D_t = I_t$ for $t \in \{i_1, \dots, i_n\}$. Moreover D_t is closed (open) and has finite codimension in C_t^* for any t.
(iii) Let $M \in \mathcal{M}^C$. We have $C^* \simeq \prod_{i\in I} C_i^*$, and we denote by e_i the element of this direct product having 1 (more precisely the identity of C_i^*) on the i-th spot and 0 elsewhere. We obtain a family $(e_i)_{i\in I}$ of orthogonal primitive central idempotents of C^*. Since e_i is central, we have that e_iM is a C^*-submodule of M. On the other hand

$$\begin{aligned} C_i^{\perp} &= \{(f_t)_{t\in I} | f_t \in C_t^* \text{ for any } t \in I \text{ and } f_i = 0\} \\ &= \{f | f \in C^* \text{ and } f_{|C_i} = 0\} \end{aligned}$$

and $C_i^{\perp}(e_iM) = 0$, so e_iM is a rational C_i^*-module. We have $M = \oplus_{i\in I}e_iM$ as C^*-modules. Indeed, the sum is direct since the e_i's are orthogonal. Also, if $m \in M$, then by (ii) we see that $e_tm = 0$ for all but finitely many $t \in I$. We obviously have that $e_t(m - \sum_{i\in I} e_im) = 0$, and since $e_t = \varepsilon_{|C_t}$, we obtain that $\varepsilon \cdot (m - \sum_{i\in I} e_im) = 0$, so $m - \sum_{i\in I} e_im = 0$, showing that $m \in \sum_{i\in I} e_iM$.
We can define now a functor

$$F : \mathcal{M}^C \to \prod_{i\in I} \mathcal{M}^{C_i},\ F(M) = (e_iM)_{i\in I}$$

and it is easy to see that this defines an equivalence of categories.
(iv) follows from *(iii)*.

Exercise 2.2.19 *Let $(C_i)_{i\in I}$ be a family of subcoalgebras of the coalgebra C and A a simple subcoalgebra of $\sum_{i\in I} C_i$ (i.e. A is a subcoalgebra which has precisely two subcoalgebras, 0 and A; more details will be given in Chapter 3). Then there exists $i \in I$ such that $A \subseteq C_i$.*
Solution: Since A has finite dimension, we can assume that the family $(C_i)_{i\in I}$ is finite, say that $A \subseteq C_1 + \ldots + C_n$. Moreover, if we prove for $n = 2$, then we can easily prove by induction for any positive integer n. Let $A \subseteq D + E$, where D and E are subcoalgebras of C. If $A \cap D \neq 0$, the $A \cap D = A$, since A is simple, so then $A \subseteq D$. If $A \cap D = 0$, pick some $a \in A$. Then

$$\Delta(a) \in \Delta(D + E) = \Delta(D) + \Delta(E) \subseteq D \otimes D + E \otimes E$$

Thus $\Delta(a) = \sum a_1 \otimes a_2 + \sum b_1 \otimes b_2$ with $a_1, a_2 \in D$ and $b_1, b_2 \in E$. Since $A \cap D = 0$, there exists $f \in C^*$ such that $f_{|D} = 0$ and $f_{|A} = \varepsilon_{|A}$. Then $f \rightharpoonup a \in A$ (note that A is a left and right C^*-module) we have that $f \rightharpoonup a = \varepsilon \rightharpoonup a = a$. On the other hand $f \rightharpoonup a = \sum f(a_2)a_1 + \sum f(b_2)b_1 = \sum f(b_2)b_1 \in E$, so $a \in E$. We obtain that $A \subseteq E$.

Exercise 2.3.4 *Let C be a coalgebra, and $c \in C$. Show that the subcoalgebra of C generated by c is finite dimensional, using the bicomodule structure of C.*
Solution: We know that C is an object of the category ${}^C\mathcal{M}^C$ with left and right comodule structures induced by Δ. A subspace V of C is a subobject in the category ${}^C\mathcal{M}^C$ if and only if $\Delta(V) \subseteq C \otimes V$ and $\Delta(V) \subseteq V \otimes C$. Since $(V \otimes C) \cap (C \otimes V) = V \otimes V$, this is equivalent to the fact that V is a subcoalgebra of C. Hence the subcoalgebra V generated by c is the smallest subbicomodule of C containing c. By Theorem 2.3.3 it follows that V is the subbimodule of C generated by c, when we regard C as a left-C^*, right-C^* bimodule, so $V = C^* \rightharpoonup c \leftharpoonup C^*$. Theorem 2.2.6 shows that $C^* \rightharpoonup c$ is

finite dimensional, hence $C^* \rightharpoonup c = \sum_{i=1,n} kc_i$ for some $c_i \in C$, and using the right hand version of the cited theorem, it follows that every $c_i \leftharpoonup C^*$ is finite dimensional. We obtain that

$$V = C^* \rightharpoonup c \leftharpoonup C^* = \sum_{i=1,n} c_i \leftharpoonup C^*$$

is finite dimensional, which ends the proof.

Exercise 2.3.10 *Let C and D be two coalgebras. Show that the categories ${}^D\mathcal{M}^C$, $\mathcal{M}^{C\otimes D^{cop}}$, $\mathcal{M}^{D^{cop}\otimes C}$, ${}^{D\otimes C^{cop}}\mathcal{M}$ and ${}^{C^{cop}\otimes D}\mathcal{M}$ are isomorphic.*
Solution: If $M \in {}^D\mathcal{M}^C$ with comodule structure maps $\rho^- : M \to D\otimes M$, $\rho^-(m) = \sum m_{[-1]} \otimes m_{[0]}$ and $\rho^+ : M \to M \otimes C$, $\rho^+(m) = \sum m_{(0)} \otimes m_{(1)}$, then M becomes a right $C \otimes D^{cop}$-comodule by $\gamma : M \to M \otimes C \otimes D^{cop}$ defined by

$$\gamma(m) = \sum (m_{[0]})_{(0)} \otimes (m_{[0]})_{(0)} \otimes m_{[-1]} = \sum (m_{(0)})_{[0]} \otimes m_{(1)} \otimes (m_{(0)})_{[-1]}$$

In this way we obtain a functor $F : {}^D\mathcal{M}^C \to \mathcal{M}^{C\otimes D^{cop}}$.
Conversely, let $M \in \mathcal{M}^{C\otimes D^{cop}}$. If $\phi : C \otimes D^{cop} \to C$ and $\psi : C \otimes D^{cop} \to D^{cop}$ are the coalgebra morphisms defined by $\phi(c\otimes d) = c\varepsilon(d)$ and $\psi(c\otimes d) = d\varepsilon(c)$, then we consider the comodules $M_\phi \in \mathcal{M}^C$ and $M_\psi \in \mathcal{M}^{D^{cop}} \simeq {}^D\mathcal{M}$. These two structures make M an object of the category ${}^D\mathcal{M}^C$. Thus we can define another functor $G : \mathcal{M}^{C\otimes D^{cop}} \to {}^D\mathcal{M}^C$, and it is clear that the functors F and G define an isomorphism of categories.

Exercise 2.3.11 *Let C, D and L be cocommutative coalgebras and $\phi : C \to L$, $\psi : D \to L$ coalgebra morphisms. Regard C and D as L-comodules via the morphisms ϕ and ψ. Show that $C\Box_L D$ is a (cocommutative) subcoalgebra of $C \otimes D$, and moreover, $C\Box_L D$ is the fiber product in the category of all cocommutative coalgebras.*
Solution: C is a right L-comodule via the morphism

$$C \xrightarrow{\Delta_C} C \otimes C \xrightarrow{I\otimes\phi} C \otimes L$$

and D is a left L-comodule via the morphism

$$D \xrightarrow{\Delta_D} D \otimes D \xrightarrow{\psi\otimes I} L \otimes D$$

and

$$C\Box_L D = Ker(((I \otimes \phi)\Delta_C) \otimes I - I \otimes ((\psi \otimes I)\Delta_D)))$$

Since C and D are cocommutative we have that $C\Box_L D$ is a $C - D$-bicomodule, so it is also a left and right $C \otimes D$-comodule (since C and D are cocommutative). This implies that $C\Box_L D$ is a subcoalgebra of $C\otimes D$. The last part follows dirrectly from the definition.

Exercise 2.4.23 *Let C and D be two coalgebras and $\phi : C \to D$ a coalgebra morphism. Show that the following are equivalent.*
(i) C is an injective (coflat) left D-comodule.
(ii) Any injective (coflat) left C-comodule is also injective (coflat) as a left D-comodule.
(iii) The functor $(-)^\phi = -\Box_D C : \mathcal{M}^D \to \mathcal{M}^C$ is exact.
Solution: It follows from Proposition 2.3.8 and the properties of adjoint functors.

Exercise 2.5.4 *Let M be a finite dimensional right C-comodule with comodule structure map $\rho : M \to M\otimes C$, $(m_i)_{i=1,n}$ a basis of M and $(c_{ij})_{1\le i,j\le n}$ be elements of C such that $\rho(m_i) = \sum_{1\le j\le n} m_j\otimes c_{ji}$ for any i. Show that the coalgebra A associated to M is the subspace of C spanned by the set $(c_{ij})_{1\le i,j\le n}$, and that $\Delta(c_{ji}) = \sum_{1\le t\le n} c_{jt}\otimes c_{ti}$ and $\varepsilon(c_{ij}) = \delta_{ij}$ for any i,j.*
Solution: If we write $(\rho\otimes I)\rho(m_i) = (I\otimes\Delta)\rho(m_i)$ and use that $(m_i)_{1\le i\le n}$ is a basis of M, we find that $\Delta(c_{ji}) = \sum_{1\le t\le n} c_{jt}\otimes c_{ti}$ for any i,j. Also, if we write the counit property for m_i, we find $\varepsilon(c_{ij}) = \delta_{ij}$.
Denote by B the subspace spanned by the c_{ij}'s. If $f\in C^*$, then $f\in ann_{C^*}(M)$ if and only if $fm_i = 0$ for any $1\le i\le n$, or $\sum_{1\le j\le n} f(c_{ji})m_j = 0$ for any i. But this is equivalent to $f(c_{ji}) = 0$ for any i,j. Thus $ann_{C^*}(M) = B^\perp$, and then $A = (ann_{C^*}(M))^\perp = (B^\perp)^\perp = B$.

Exercise 2.5.8 *Let C be a coalgebra and X, Y, Z three subspaces of C. Show that $(X\wedge Y)\wedge Z = X\wedge(Y\wedge Z)$.*
Solution: We see from the definition that $X\wedge Y = Ker(\pi_{X,Y})$, where $\pi_{X,Y}$ is the composition of the morphisms

$$C \xrightarrow{\Delta} C\otimes C \xrightarrow{p_X\otimes p_Y} C/X\otimes C/Y$$

and p_X, p_Y are the natural projections. Then $\pi_{X,Y}$ induces an injective linear morphism $\phi_{X,Y} : C/(X\wedge Y) \to C/X\otimes C/Y$ and we have that

$$Ker(\pi_{X\wedge Y,Z}) = Ker((\phi_{X,Y}\otimes I)\circ\pi_{X\wedge Y,Z})$$

But $Ker(\pi_{X\wedge Y,Z}) = (X\wedge Y)\wedge Z$ and

$$(\phi_{X,Y}\otimes I)\circ\pi_{X\wedge Y,Z} = (p_X\otimes p_Y\otimes p_Z)\circ\Delta_2$$

so $(X\wedge Y)\wedge Z = Ker((p_X\otimes p_Y\otimes p_Z)\circ\Delta_2)$. Similarly $X\wedge(Y\wedge Z) = Ker((p_X\otimes p_Y\otimes p_Z)\circ\Delta_2)$, proving the required equality.

Exercise 2.5.9 *Let $f : C \to D$ be a coalgebra morphism and X, Y subspaces of C. Show that $f(X \wedge Y) \subseteq f(X) \wedge f(Y)$.*
Solution: Let us consider the linear maps $f_X : C/X \to D/f(X)$ and $f_Y : C/Y \to D/f(Y)$ induced by f. We know that $(f \otimes f) \circ \Delta_C = \Delta_D \circ f$ and $(f_X \otimes f_Y) \circ (p_X \otimes p_Y) = (p_{f(X)} \otimes p_{f(Y)}) \circ (f \otimes f)$, so then

$$\begin{aligned}(f_X \otimes f_Y) \circ (p_X \otimes p_Y) \circ \Delta_C &= (p_{f(X)} \otimes p_{f(Y)}) \circ (f \otimes f) \circ \Delta_C \\ &= (p_{f(X)} \otimes p_{f(Y)}) \circ \Delta_D \circ f\end{aligned}$$

Since $X \wedge Y = Ker((p_X \otimes p_Y) \circ \Delta_C)$, we have that

$$((p_{f(X)} \otimes p_{f(Y)}) \circ \Delta_D \circ f)(X \wedge Y) = 0$$

and then

$$f(X \wedge Y) \subseteq Ker((p_{f(X)} \otimes p_{f(Y)}) \circ \Delta_D) = f(X) \wedge f(Y)$$

Bibliographical notes

Our sources of inspiration for this chapter include again the books of M. Sweedler [218], E. Abe [1], and S. Montgomery [149], P. Gabriel's paper [85], B. Pareigis' notes [178], and F.W. Anderson and K. Fuller [3] for module theoretical aspects. Further references are R. Wisbauer [244], I. Kaplansky [104], Y. Doi [72]. We remark that the cotensor product appears for the first time in a paper by Milnor and Moore [146]. We have also used the papers by C. Năstăsescu and B. Torrecillas [159], B. Lin [122]. The reader should also consult M. Takeuchi's paper [229], where the Morita theory for categories of comodules is studied. The contexts known as Morita-Takeuchi contexts are a valuable tool for studying Galois coextensions of coalgebras, in a dual manner to the one in Chapter 6.

Chapter 3

Special classes of coalgebras

3.1 Cosemisimple coalgebras

We recall that if $\mathcal{A}$ is a Grothendieck category and M is an object of $\mathcal{A}$, the sum $s(M)$ of all simple subobjects of M is called the socle of M. If $M = 0$, we have $s(M) = 0$. An object M is called semisimple (or completely reducible) if $s(M) = M$. It is a well known fact that M is a semisimple object if and only if it is a direct sum of simple subobjects. A category $\mathcal{A}$ with the property that every object of $\mathcal{A}$ is semisimple is called a semisimple (or completely reducible) category. If $\mathcal{C}$ is a semisimple Grothendieck category, then any monomorphism (epimorphism) splits. in particular we have that any object is injective and projective. Conversely, if $\mathcal{C}$ is a Grothendieck category such that any object is injective and projective (such a category is called a spectral category) we do not necessarily have that $\mathcal{C}$ is a semisimple category. We will be interested in the situations where $\mathcal{A} = \mathcal{M}^C$, the category of right comodules over the coalgebra C, or $\mathcal{A} = {}^C\mathcal{M}$, the category of left comodules over the coalgebra C.
A coalgebra C is called simple if the only subcoalgebras of C are 0 and C. The Fundamental Theorem of Coalgebras (Theorem 1.4.7) shows that a simple coalgebra has finite dimension.

Exercise 3.1.1 *Let C be a coalgebra. Show that C is a simple coalgebra if and only if the dual algebra C^* is a simple artinian algebra. If this is the case, then C is a sum of isomorphic simple right C-subcomodules.*
Moreover, if the field k is algebraically closed, then C is isomorphic to a matrix coalgebra over k.

Exercise 3.1.2 *Let M be a simple right comodule over the coalgebra C. Show that:*
(i) The coalgebra A associated to M is a simple coalgebra.
(ii) If the field k is algebraically closed, then $A \simeq M^c(n,k)$, where $n = dim(M)$. In particular the family $(c_{ij})_{1\le i,j\le n}$ defined in Exercise 2.5.4 is a basis of A.

Exercise 3.1.3 *Let M and N be two simple right comodules over a coalgebra C. Show that M and N are isomorphic if and only if they have the same associated coalgebra.*

For an arbitrary coalgebra C we denote by C_0 the sum of all simple subcoalgebras. C_0 is a subcoalgebra of C called the coradical of C. We also use the notation $C_0 = Corad(C)$ for the coradical.

Proposition 3.1.4 *Let C be a coalgebra. Then $C_0 = s({}_CC) = s(C_C)$, where $s(C_C)$ is the socle of C as an object of $\mathcal{M}^C$, and $s({}_CC)$ is the socle of C as an object of ${}^C\mathcal{M}$.*

Proof: We will show that $C_0 = s(C_C)$. The proof of the fact that $C_0 = s({}_CC)$ is similar (or can bee seen directly by looking at the co-opposite coalgebra and applying the result about the right socle). A simple subcoalgebra A of C is a right C-subcomodule of C. Since A is a finite direct sum of simple right coideals of A, we see that A is semisimple of finite length when regarded as a right C-comodule. Thus $A \subseteq s(C_C)$, and then $C_0 \subseteq s(C_C)$.
Conversely, let $S \subseteq s(C_C)$ be a simple right C-comodule, and let A be the coalgebra associated to S. By Exercise 3.1.2 A is a simple coalgebra, so $A \subseteq C_0$. But $S \subseteq A$, since for $c \in S$ we have $c = \sum \varepsilon(c_1)c_2 \in A$. Thus $S \subseteq A \subseteq C_0$, so $s(C_C) \subseteq C_0$. ∎

A coalgebra C is called a right cosemisimple coalgebra (or right completely reducible coalgebra) if the category $\mathcal{M}^C$ is a semisimple category, i.e. if every right C-comodule is cosemisimple. Similarly, we define left cosemisimple coalgebras by the semisimplicity of the category of left comodules. In fact, the concept of cosemisimplicity is left-right symmetric, as the following shows.

Theorem 3.1.5 *Let C be a coalgebra. The following assertions are equivalent.*
(i) C is a right cosemisimple coalgebra.
(ii) C is a left cosemisimple coalgebra.
(iii) $C = C_0$.
(iv) Every left (right) rational C^*-module is semisimple.

(v) Every right (left) C-comodule is projective in the category $\mathcal{M}^C$ (resp. ${}^C\mathcal{M}$).
(vi) Every right (left) C-comodule is injective in the category $\mathcal{M}^C$ (resp. ${}^C\mathcal{M}$).
(vii) There exists a topological isomorphism between C^* and a direct topological product of finite dimensional simple artinian k-algebras (with discrete topology).

A coalgebra satisfying the above equivalent conditions is called cosemisimple.

Proof: $(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$ follows from Proposition 3.1.4.
$(i) \Leftrightarrow (iv)$ It follows from the fact that if $M \in \mathcal{M}^C$, then M is a simple object in the category $\mathcal{M}^C$ if and only if M is a simple left C^*-module.
$(i) \Rightarrow (v)$ and $(i) \Rightarrow (vi)$ follow from the general fact that in a semisimple Grothendieck category every object is projective and injective.
$(v) \Rightarrow (i)$ (and similarly $(vi) \Rightarrow (i)$) Assume that any object of $\mathcal{M}^C$ is projective. Then if $M \in \mathcal{M}^C$, any subobject N of M is a direct summand. This implies that any finite dimensional object is semisimple (of finite length). On the other hand, $\mathcal{M}^C$ has a family of finite dimensional generators, which shows that every object of $\mathcal{M}^C$ is semisimple.
$(iii) \Rightarrow (vii)$ follows from Exercise 2.2.18.
$(vii) \Rightarrow (iii)$ Assume that $C^* \simeq \prod_{i\in I} A_i$, an isomorphism of topological rings, where $(A_i)_{i\in I}$ is a family of simple artinian k-algebras of finite dimension, and each A_i is regarded as a topological ring with the discrete topology. For simplicity assume that $C^* = \prod_{i\in I} A_i$. Let $\pi_i : C^* \to A_i$ be the natural projection for any $i \in I$. Denote $K_i = Ker(\pi_i)$. Since the map π_i is continuous, K_i is a two-sided ideal of C^* of finite codimension, which is open and closed in C^*. Let $R_i = K_i^{\perp}$, which is a simple subcoalgebra of C, and denote $R = \sum_{i\in I} R_i$. We have that

$$\begin{aligned} R^{\perp} &= \cap_{i\in I} R_i^{\perp} \\ &= \cap_{i\in I} K_i^{\perp\perp} \\ &= \cap_{i\in I} K_i \\ &= 0 \end{aligned}$$

showing that $R = C$. Thus $C = C_0$. ∎

Exercise 3.1.6 *Let C be a cosemisimple coalgebra. Show that C is a direct sum of simple subcoalgebras. Moreover, show that any subcoalgebra of C is cosemisimple.*

Exercise 3.1.7 *Let C be a finite dimensional coalgebra. Show that C is cosemisimple if and only if the dual algebra C^* is semisimple.*

If $M \in {}^C\mathcal{M}$, we denote by $Cend_C(M)$ the space of all endomorphisms of the C-comodule M. Clearly $Cend_C(M)$ is a k-algebra with map composition as multiplication. In particular, if we regard C as a left C-comodule, let us take the k-algebra $A = Cend_C(C)$. The following indicates the connection between the k-algebras A and C^* and computes the Jacobson radical of C^*.

Proposition 3.1.8 *With the above notations we have that*
(i) The map $\phi : A \to C^*$, $\phi(f) = \varepsilon \circ f$ for any $f \in A = Cend_C(C)$, is a k-algebra isomorphism.
(ii) The Jacobson radical of C^* is $J(C^*) = C_0^\perp$.

Proof: (i) Let $f, g \in A$. Since g is a morphism of left C-comodules, we have $\sum c_1 \otimes g(c_2) = \sum g(c)_1 \otimes g(c)_2$ for any $c \in C$. If we apply $I \otimes \varepsilon$ we find that

$$\sum c_1(\varepsilon \circ g)(c_2) = \sum g(c)_1 \varepsilon(g(c)_2) = g(c)$$

Then

$$\begin{aligned}
(\phi(f)\phi(g))(c) &= \sum \phi(f)(c_1)\phi(g)(c_2) \\
&= \sum (\varepsilon \circ f)(c_1)(\varepsilon \circ g)(c_2) \\
&= \sum (\varepsilon \circ f)(c_1(\varepsilon \circ g)(c_2)) \\
&= (\varepsilon \circ f)(g(c)) \\
&= (\varepsilon \circ f \circ g)(c) \\
&= \phi(f \circ g)(c)
\end{aligned}$$

so ϕ is an algebra morphism. Define $\psi : C^* \to A$ by

$$\psi(u)(c) = u \rightharpoonup c = \sum u(c_2)c_1$$

for any $u \in C^*$ and $c \in C$, where $\rightharpoonup$ denotes the left action of C^* on C coming from the right C-comodule structure of C. It is clear that $\psi(u) \in A$, since

$$\begin{aligned}
\psi(u)(c \leftharpoonup v) &= u \rightharpoonup (c \leftharpoonup v) \\
&= (u \rightharpoonup c) \leftharpoonup v \\
&= \psi(u)(c) \leftharpoonup v
\end{aligned}$$

where $\leftharpoonup$ is the right action of C^* coming from the left C-comodule structure of C. Note that we used the fact that C is a left-C^*, right-C^* bimodule with the left action $\rightharpoonup$ and the right action $\leftharpoonup$. We show that ψ is an inverse of ϕ. Indeed, for any $u \in C^*$ and $c \in C$ we have

$$\begin{aligned} ((\phi\psi)(u))(c) &= (\varepsilon \circ \psi(u))(c) \\ &= \sum \varepsilon(u(c_2)c_1) \\ &= u(c) \end{aligned}$$

and for any $f \in A$, $c \in C$

$$\begin{aligned} ((\psi\phi)(f))(c) &= \sum \phi(f)(c_2)c_1 \\ &= \sum \varepsilon(f(c_2))c_1 \\ &= f(c) \end{aligned}$$

(ii) By Proposition 2.5.3(ii) we have $C_0^\perp = ann_{C^*}(C_0)$. Since $J(C^*)$ is the intersection of the annihilators of all simple left C^*-modules and C_0 is a sum of simple right C-comodules, thus a sum of simple left C^*-modules, we have $J(C^*) \subseteq C_0^\perp$.
Let now $u \in C_0^\perp$ and denote $f = \phi^{-1}(u)$. Thus $f = \varepsilon \circ u$ and $\varepsilon(f(C_0)) = u(C_0) = 0$. Then for any $c \in C_0$

$$\begin{aligned} f(c) &= \sum f(c)_1\varepsilon(f(c)_2) \\ &= \sum c_1\varepsilon(f(c_2)) \quad (\text{since } f \in A) \\ &= 0 \qquad (\text{since } c_2 \in C_0) \end{aligned}$$

so $f(C_0) = 0$. We show that $f \in J(A)$. From the fact that ϕ is an algebra isomorphism it will follow that $u \in J(C^*)$. Denote $g = 1 - f$. Then g is injective. Indeed, for $c \in Ker(g) \cap C_0$ we have $0 = g(c) = c - f(c) = c$, so $Ker(g) \cap C_0 = 0$. This implies that $Ker(g) = 0$, since C_0 is an essential left C-subcomodule of C.
Since C is an injective left C-comodule, $Im(g)$ is a direct summand in C as a left C-subcomodule, so $C = Im(g) \oplus Y$ for some left C-subcomodule Y of C. On the other hand $C_0 \subseteq Im(g)$, and since C_0 is essential in C, we must have $Y = 0$. Thus $Im(g) = C$ and g is an isomorphism. Then $g = 1 - f$ is invertible in A, so $f \in J(A)$. ∎

Let C be a coalgebra and $M \in \mathcal{M}^C$. We recall that the socle of M, denoted by $s(M)$, is the sum of all simple subcomodules of M. Then $s(M)$ is a semisimple subcomodule of M. Since any non-zero comodule contains a simple subcomodule, we see that $s(M)$ is essential in M. We can define recurrently an ascending chain $M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n \subseteq \ldots$ of

subcomodules of M as follows. Let $M_0 = s(M)$, and for any $n \geq 0$ we define M_{n+1} such that $s(M/M_n) = M_{n+1}/M_n$. This ascending chain of subcomodules is called the Loewy series of M. Since M is the union of all subcomodules of finite dimension, we have that $M = \cup_{n\geq 0} M_n$.
If I is a two-sided ideal of C^*, we denote by $ann_M(I) = \{x \in M | Ix = 0\}$, which is clearly a left C^*-submodule of M.

Lemma 3.1.9 *Let $I = J(C^*) = C_0^\perp$ and $M \in \mathcal{M}^C$. Then for any $n \geq 0$ we have $M_n = ann_M(I^{n+1})$.*

Proof: We use induction on n. For $n = 0$, we have $ann_M(I) = M_0 = s(M)$. Indeed, $IM_0 = J(C^*)M_0 = 0$, since the Jacobson radical of C^* annihilates all simple left C^*-modules. Thus $M_0 \subseteq ann_M(I)$. On the other hand $C_0^\perp ann_M(I) = Iann_M(I) = 0$, so by Proposition 2.5.3, $ann_M(I)$ is a right C_0-comodule. Since C_0 is a cosemisimple coalgebra, $ann_M(I)$ is a semisimple object of the category $\mathcal{M}^{C_0}$, and then also of the category $\mathcal{M}^C$. We obtain that $ann_M(I) \subseteq s(M) = M_0$.
Assume now that $M_{n-1} = ann_M(I^n)$ for some $n \geq 1$. Since $M_n/M_{n-1} = s(M/M_{n-1})$ is semisimple, we have that $I(M_n/M_{n-1}) = 0$, therefore $IM_n \subseteq M_{n-1}$. Then $I^{n+1}M_n = I^n(IM_n) \subseteq I^n M_{n-1} = 0$, so $M_n \subseteq ann_M(I^{n+1})$. If we denote $X = ann_M(I^{n+1})$, we have $I^{n+1}X = 0$, so $IX \subseteq ann_M(I^n) = M_{n-1}$. Then $I(X/M_{n-1}) = 0$ and by the same argument as above X/M_{n-1} is a right C_0-comodule, so X/M_{n-1} is a semisimple comodule.
We have that $s(M/M_{n-1}) = M_n/M_{n-1}$, so we obtain that $X \subseteq M_n$. Thus $M_n = ann_M(I^{n+1})$, which ends the proof. ∎

Corollary 3.1.10 *Let C be a coalgebra and $C_0, C_1, \ldots$ the Loewy series of the right (or left) C-comodule C. Then C_0 is the coradical of C, $C_n = \wedge^{n+1} C_0$ and C_n is a subcoalgebra of C for any $n \geq 0$.*

Proof: We have seen in Proposition 3.1.4 that the coradical of C is just the socle of the right C-comodule C. Lemma 3.1.9 shows that $C_n = ann_C(J(C^*)^{n+1})^\perp$. By Proposition 2.5.3(i) we have $C_n = (J(C^*)^{n+1})^\perp$, and by Lemmma 2.5.7 we see that $C_n = \wedge^{n+1} C_0$. By Lemma 1.5.23 C_n is a subcoalgebra. ∎

If C is a coalgebra, the Loewy series of the right (or left) C-comodule C is an ascending chain of subcoalgebras

$$C_0 \subseteq C_1 \subseteq \ldots \subseteq C_n \subseteq \ldots$$

which can also be regarded as the chain obtained by starting with the coradical C_0 of C and then by taking $C_n = \wedge^{n+1} C_0$ for any $n \geq 0$. This chain is also called the coradical filtration of C. Since C is the union of its finite dimensional coalgebras we have $C = \cup_{n\geq 0} C_n$.

Exercise 3.1.11 *Show that the coradical filtration is a coalgebra filtration, i.e. that* $\Delta(C_n) \subseteq \sum_{i=0,n} C_i \otimes C_{n-i}$ *for any* $n \geq 0$.

Exercise 3.1.12 *Let C be a coalgebra and D a subcoalgebra of C such that* $\cup_{n\geq 0}(\wedge^n D) = C$. *Show that* $Corad(C) \subseteq D$.

Exercise 3.1.13 *Let $f : C \to D$ be a surjective morphism of coalgebras. Show that* $Corad(D) \subseteq f(Corad(C))$.

Exercise 3.1.14 *Let X, Y and D be subspaces of the linear space C. Show that*

$$(D \otimes D) \cap (X \otimes C + C \otimes Y) = (D \cap X) \otimes D + D \otimes (D \cap Y)$$

Exercise 3.1.15 *Let C be a coalgebra and D a subcoalgebra of C. Show that* $D_n = D \cup C_n$ *for any* n.

3.2 Semiperfect coalgebras

Proposition 3.2.1 *Let C be a coalgebra. The following assertions are equivalent.*
(i) $Rat({}_{C^*}C^*)$ *is dense in* C^*.
(ii) For any simple left C-comodule S, $Rat({}_{C^*}E(S)^*)$ *is dense in* $E(S)^*$, *where $E(S)$ denotes the injective envelope of S in the category* ${}^C\mathcal{M}$.
(iii) For any injective left C-comodule Q, $Rat({}_{C^*}Q^*)$ *is dense in* Q^*.
(iv) For any left C-comodule M, $Rat({}_{C^*}M^*)$ *is dense in* M^* *(in the finite topology).*

Proof: $(i) \Rightarrow (ii)$ If S is a simple left C-comodule, then $C = E(S) \oplus X$ for some left C-subcomodule X of C. Then $C^* \simeq E(S)^* \oplus X^*$ as left C^*-modules, and $Rat({}_{C^*}C^*) = Rat({}_{C^*}E(S)^*) \oplus Rat({}_{C^*}X^*)$. Since $Rat({}_{C^*}C^*)$ is dense in C^*, we obtain by Exercise 1.2.11 that $Rat({}_{C^*}E(S)^*)$ is dense in $E(S)^*$.
$(ii) \Rightarrow (iii)$ If Q is an injective object of ${}^C\mathcal{M}$, we have that $Q = \oplus_{i\in I}E(S_i)$ for a family $(S_i)_{i\in I}$ of simple left C-comodules. Since $Q^* \simeq \prod_{i\in I} E(S_i)^*$, so $\oplus_{i\in I}E(S_i)^*$ is dense in Q^* by Exercise 1.2.17. On the other hand $Rat(\oplus_{i\in I}E(S_i)^*) = \oplus_{i\in I}Rat({}_{C^*}E(S_i)^*)$, which is dense in $\oplus_{i\in I}E(S_i)^*$ by the assumption. Then $Rat(\oplus_{i\in I}E(S_i)^*)$ is dense in Q^*, and the result follows from the fact that $Rat(\oplus_{i\in I}E(S_i)^*) \subseteq Rat({}_{C^*}Q^*)$.
$(iii) \Rightarrow (iv)$ Let $i : M \to E(M)$ the inclusion morphism, and $i^* : E(M)^* \to$

M^* the dual morphism. Since $Rat(_{C^*}M^*)$ is dense in M^*, we obtain by Exercise 1.2.18 that $i^*(Rat(_{C^*}M^*))$ is dense in M^*. But i^* is a morphism of left C^*-modules, so $i^*(Rat(_{C^*}M^*)) \subseteq Rat(_{C^*}M^*)$, showing that $Rat(_{C^*}M^*)$ is dense in M^*.
$(iv) \Rightarrow (i)$ is obvious. ∎

Proposition 3.2.2 *For any $M \in {}^C\mathcal{M}$ the following assertions are equivalent.*
(i) $Rat(_{C^*}M^*) \neq 0$.
(ii) There exists a maximal subcomodule N of M, $N \neq M$.
(iii) $J(M) \neq M$, where $J(M)$ is the Jacobson radical of the object M (i.e. the intersection of all maximal subobjects of M).
Moreover, if (i) – (iii) are true, then $M/J(M)$ is a semisimple left C_0-comodule.

Proof: $(i) \Rightarrow (ii)$ Since $Rat(_{C^*}M^*) \neq 0$, there exists a simple C^*-submodule $X \leq Rat(_{C^*}M^*)$. Since X has finite dimension, X is closed in the finite topology. Let $N = X^\perp$, which is a subcomodule of M. Moreover, since $X \neq 0$ we have that $N \neq M$. If P is a subcomodule of M such that $N \subseteq P \neq M$, then $P^\perp \subseteq N^\perp = X^{\perp\perp} = X$. Since $P^{\perp\perp} = P \neq M$, we have that $P^\perp \neq 0$, so we must have $P^\perp = X$. Then $N = X^\perp = P^{\perp\perp} = P$, which shows that N is a maximal subcomodule of M.
$(ii) \Rightarrow (i)$ If N is a maximal subcomodule of M, then M/N is a simple object in the category $\mathcal{M}^C$, in particular it is finite dimensional. Then $(M/N)^*$ is a rational left C^*-module and the projection $p : M \to M/N$ induces an injective morphism of left C^*-modules $p^* : (M/N)^* \to M^*$. Then $0 \neq Im(p^*) \subseteq Rat(_{C^*}M^*)$, so $Rat(_{C^*}M^*) \neq 0$.
$(iii) \Leftrightarrow (ii)$ is obvious.
Assume now that (i) – (iii) hold. Since $C_0^\perp = J(C^*)$, we have

$$(M/J(M))C_0^\perp = (M/J(M))J(C^*) = 0$$

Then by Proposition 2.5.3 we obtain that $M/J(M)$ is a left C_0-comodule, which is semisimple since C_0 is cosemisimple. ∎

We say that a right C-comodule M has a projective cover if there exist a projective object P in the category of right C-comodules and a surjective morphism of comodules $f : P \to M$ such that $Ker(f)$ is a superfluous subobject of P, i.e. if $X + Ker(f) = P$ for some subobject X of P, we must have $X = P$.

Theorem 3.2.3 *Let C be a coalgebra. The following statements are equivalent.*
(i) The category $\mathcal{M}^C$ of right C-comodules has enough projectives.

(ii) $Rat({}_{C^*}C^*)$ *is a dense subset of* C^*.
(iii) The injective envelope of any simple left C*-comodule is finite dimensional.*
(iv) Any finite dimensional right C*-comodule has a projective cover.*

Proof: $(i) \Rightarrow (ii)$ By Proposition 3.2.1 it is enough to show that for any simple left C-comodule S, $Rat(E(S)^*)$ is dense in $E(S)^*$. We know that S^* is a simple right C-comodule. By (i), there exist a projective object $P \in \mathcal{M}^C$ and an epimorphism $P \longrightarrow S^*$. Then we have a monomorphism $S \simeq S^{**} \longrightarrow P^*$, therefore $S \subseteq Rat({}_{C^*}P^*)$. By Corollary 2.4.18 $Rat({}_{C^*}P^*)$ is injective as a left C-comodule, so we have an injective morphism of left C-comodules $E(S) \to Rat({}_{C^*}P^*)$. Let $u : E(S) \to P^*$ be the injection obtained by composing this injective morphism with the inclusion $Rat(P^*_{C^*}) \to P^*$. Then $u^* : P^{**} \to E(S)^*$ is surjective, and $u^*(Rat({}_{C^*}P^{**})) \subseteq Rat({}_{C^*}E(S)^*)$. But P is dense in P^{**} (through the natural embedding), and $P \subseteq Rat({}_{C^*}P^{**})$, so $Rat({}_{C^*}P^{**})$ is dense in P^{**}. It follows that $u^*(Rat({}_{C^*}P^{**}))$ is dense in $E(S)^*$, and then $Rat({}_{C^*}E(S)^*)$ is dense in $E(S)^*$.
$(ii) \Rightarrow (iii)$ Let S be a simple left C-comodule. We may assume that S is a left subcomodule of C_0, and then $C_0 = S \oplus M$ for some left C-comodule M. Since $C = E(C_0) = E(S) \oplus E(M)$ we obtain the following commutative diagram with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & C_0^{\perp} & \longrightarrow & C^* & \longrightarrow & C_0^* & \longrightarrow & 0 \\
 & & & & \downarrow{\scriptstyle \pi} & & \downarrow & & \\
0 & \longrightarrow & S^{\perp} & \longrightarrow & E(S)^* & \longrightarrow & S^* & \longrightarrow & 0
\end{array}$$

where π is the projection from C^* to $E(S)^*$. Clearly $E(S)^* = C^*x$, where $x = \pi(\varepsilon_C)$. On the other hand, since the diagram is commutative, we have $\pi(C_0^{\perp}) \subseteq S^{\perp}$. Let $f \in E(S)^*$ such that $f(S) = 0$. Then we can regard f as an element of C^* for which $f(E(M)) = 0$. Then $f(C_0) = f(S \oplus M) = 0$, so $f \in C_0^{\perp}$. We have obtained that $\pi(C_0^{\perp}) = S^{\perp}$.
Now $\pi(C_0^{\perp}) = C_0^{\perp}\pi(\varepsilon_C) = C_0^{\perp}x$, so $C_0^{\perp}x = S^{\perp}$. We have that $Rat(E(S)^*)$ is not contained in $S^{\perp}$, since $Rat(E(S)^*)$ is dense in $E(S)^*$ and $S^{\perp}$ is closed in $E(S)^*$. Thus $S^{\perp} \neq S^{\perp} + Rat(E(S)^*)$, and since $E(S)^*/S^{\perp} \simeq S^*$ is simple, we must have $S^{\perp} + Rat(E(S)^*) = E(S)^* = C^*x$. Therefore

$$C_0^{\perp}x + Rat(E(S)^*) = E(S)^* = C^*x$$

Since $C_0^\perp = J(C^*)$, we have by Nakayama Lemma that $E(S)^* = C^*x = Rat(E(S)^*)$. Thus $E(S)^*$ is a rational left C^*-module, so it is finite dimensional as a cyclic C^*-module. We obtain that $E(S)$ is finite dimensional too.
$(iii) \Rightarrow (iv)$ Let M be a finite dimensional right C-comodule. Since M^* is a finite dimensional left C-comodule, the injective envelope $E(M^*)$ of M^* has finite dimension. It is easy to see that by taking the dual of the exact sequence $0 \longrightarrow M^* \longrightarrow E(M^*)$, we find a projective cover $E(M^*)^* \longrightarrow M \longrightarrow 0$ of M.
$(iv) \Rightarrow (i)$ is obvious, since any comodule is a homomorphic image of a direct sum of finite dimensional comodules. ∎

Definition 3.2.4 *A coalgebra C is called right semiperfect if one of the equivalent conditions of Theorem 3.2.3 is satisfied. A coalgebra C is called left semiperfect if C^{cop} is right semiperfect, i.e. if C satisfies one of the conditions of Theorem 3.2.3 with the left and right hand sides switched.* ∎

Remark 3.2.5 *The equivalence of assertions $(i), (ii)$ and (iv) of Theorem 3.2.3 is also proved in Corollary 2.4.21. We note that a finite dimensional coalgebra is left and right semiperfect since the category of right (left) C-comodules is isomorphic to the category of left (right) C^*-modules, which has enough projectives.* ∎

Corollary 3.2.6 *Let C be a right semiperfect coalgebra. Then any nonzero left C-comodule contains a maximal subcomodule.*

Proof: We know from Theorem 3.2.3 that $Rat(_{C^*}C^*)$ is dense in C^*. Then Proposition 3.2.1 shows that $Rat(_{C^*}M^*)$ is dense in M^* for any nonzero left C-comodule M. In particular $Rat(_{C^*}M^*) \neq 0$ and we can use Proposition 3.2.2. ∎

Example 3.2.7 *Let H be a k-vector space with basis $\{c_m \mid m \in \mathbf{N}\}$. Then H is a coalgebra with comultiplication Δ and counit ε defined by*

$$\Delta(c_m) = \sum_{i=0,m} c_i \otimes c_{m-i}, \quad \varepsilon(c_m) = \delta_{0,m}$$

for any $m \in \mathbf{N}$ (see Example 1.1.4.2)).
By Example 1.3.8.2) we know that the dual algebra H^* is isomorphic to the algebra $k[[X]]$ of formal power series in the indeterminate X. Also, the category $\mathcal{M}^H$ is the class of all torsion left modules over $k[[X]]$. But in this category the only projective object is 0, so H is not a right semiperfect coalgebra. Since H is cocommutative, H is not a left semiperfect coalgebra either. ∎

Example 3.2.8 *Let C be the coalgebra defined in Example 1.1.4.6). C has a basis $\{ g_i, d_i \mid i \in \mathbf{N}^* \}$, and coalgebra structure defined by*

$$\begin{aligned}\Delta(g_i) &= g_i \otimes g_i \\ \Delta(d_i) &= g_i \otimes d_i + d_i \otimes g_{i+1} \\ \varepsilon(g_i) &= 1 \\ \varepsilon(d_i) &= 0\end{aligned}$$

We define the elements $g_j^*, d_j^* \in C^*$ by

$$\begin{aligned}g_j^*(g_i) &= \delta_{ij} \\ g_j^*(d_i) &= 0 \\ d_j^*(g_i) &= 0 \\ d_j^*(d_i) &= \delta_{ij}\end{aligned}$$

Clearly $g_i^* g_j^* = \delta_{ij} g_i^*$ and $\varepsilon = \sum_{i=1,\infty} g_i^*$, i.e. for any $c \in C$ $g_i^*(c) \neq 0$ for only finitely many i's, and $\varepsilon(c) = \sum_{i=1,\infty} g_i^*(c)$. Then $C = \oplus_{i \geq 1} C \leftharpoonup g_i^*$ as left C^*-modules, and $C = \oplus_{i \geq 1} g_i^* \rightharpoonup C$ as right C^*-modules. It is straightforward to check that

$$\begin{aligned}g_i^* \rightharpoonup g_j &= \delta_{ij} g_i \\ d_i^* \rightharpoonup g_j &= 0 \\ g_i^* \rightharpoonup d_j &= \delta_{i,j+1} d_j \\ d_i^* \rightharpoonup d_j &= \delta_{ij} g_i\end{aligned}$$

$$\begin{aligned}g_j \leftharpoonup g_i^* &= \delta_{ij} g_j \\ g_j \leftharpoonup d_i^* &= 0 \\ d_j \rightharpoonup g_i^* &= \delta_{i,j} d_j \\ d_j^* \rightharpoonup d_i^* &= \delta_{ij} g_{j+1}\end{aligned}$$

for any i, j. These relations show that $g_i^* \rightharpoonup C =< g_i, d_{i-1} >$ (the vector space spanned by g_i and d_{i-1}) for $i > 1$, and $g_1^* \rightharpoonup C =< g_1 >$. Similarly $C \leftharpoonup g_i^* =< g_i, d_i >$. The coradical of C is the space spanned by the set $\{g_i | i \geq 1\}$, and then a simple (left or right) subcomodule of C is of the form kg_i for some i. Indeed, let X be a simple right C-subcomodule of C, and pick a non-zero $c = \sum_j \alpha_j g_j + \sum_j \beta_j d_j \in X$. If there exists i such that $\beta_i \neq 0$, the relation $d_i^* \rightharpoonup c = \beta_i g_i$ shows that $g_i \in X$, and then $X = kg_i$, a contradiction. If $\beta_j = 0$ for any j, then pick some i with $\alpha_i \neq 0$, and then

$g_i^* \rightharpoonup c = \alpha_i g_i$, so $X = kg_i$. Thus any simple (left or right) C-comodule is isomorphic to some kg_i.
For any i we have that $C \leftharpoonup g_i^*$ is the injective envelope of the right C-comodule kg_i. Indeed, since $C = \oplus_{i\geq 1} C \leftharpoonup g_i^*$ as right C-comodules and C is an injective right C-comodule, we see that $C \leftharpoonup g_i^*$ is an injective right C-comodule. Moreover, kg_i is an essential right C-subcomodule (or equivalently a left C^*-submodule) of $C \leftharpoonup g_i^* =< g_i, d_i >$, since $0 \neq g_i^* \rightharpoonup (\alpha g_i + \beta d_i) = \alpha g_i \in kg_i$ for $\alpha \neq 0$, and $d_i^* \rightharpoonup d_i = g_i$.
Similarly $g_i^* \rightharpoonup C$ is the injective envelope of the left C-comodule kg_i. Therefore C is a left and right semiperfect coalgebra. ∎

Example 3.2.9 *We modify Example 3.2.8 for obtaining a right semiperfect coalgebra which is not a left semiperfect coalgebra. Let C be a vector space with basis $\{ g_i, d_i \mid i \in \mathbf{N}^* \}$. C becomes a coalgebra by defining the comultiplication and counit as follows.*

$$\begin{aligned} \Delta(g_i) &= g_i \otimes g_i \\ \Delta(d_i) &= g_1 \otimes d_i + d_i \otimes g_{i+1} \\ \varepsilon(g_i) &= 1 \\ \varepsilon(d_i) &= 0 \end{aligned}$$

We define the elements $g_j^*, d_j^* \in C^*$ as in Exercise 3.2.8. Also, as in Exercise 3.2.8 we have that $\varepsilon = \sum_{i=1,\infty} g_i^*$, $g_i^* g_j^* = \delta_{ij} g_i^*$, $C = \oplus_{i\geq 1} C \leftharpoonup g_i^*$ as left C^*-modules, and $C = \oplus_{i\geq 1} g_i^* \rightharpoonup C$ as right C^*-modules. We see that $C \leftharpoonup g_i^* = kg_i$ for $i > 1$, and $C \leftharpoonup g_1^* =< g_1, d_1, d_2, \ldots >$. Also $g_i^* \rightharpoonup C =< g_i, d_{i-1} >$ for $i > 1$, and $g_1^* \rightharpoonup C =< g_1 >$.
As in Example 3.2.8 we can see that the coradical of C is the space spanned by the set $\{g_i | i \geq 1\}$ and a simple (left or right) subcomodule of C is of the form kg_i for some i. Also $C \leftharpoonup g_1^*$ (which is infinite dimensional) is the injective envelope of the left C^*-module kg_1, and $g_i^* \rightharpoonup C$ (which has finite dimension) is the injective envelope of the right C^*-module kg_i. Therefore C is a right semiperfect coalgebra, but it is not a left semiperfect coalgebra.
∎

Corollary 3.2.10 *Let C be a coalgebra. Then the following assertions are equivalent.*
(i) C is left and right semiperfect.
(ii) Every right (or left) C-comodule has a projective cover in $\mathcal{M}^C$ (or ${}^C\mathcal{M}$).

Proof: $(ii) \Rightarrow (i)$ is obvious from the definition of a semiperfect coalgebra.
$(i) \Rightarrow (ii)$ Let $M \in \mathcal{M}^C$. Corollary 3.2.6 shows that $J(M) \neq M$. Moreover,

$M/J(M)$ is a direct sum of simple right comodules, say $M/J(M) = \oplus_{i\in I}S_i$. If $f_i : P_i \to S_i$ is a projective cover of S_i, let $P = \oplus_{i\in I}P_i$, which is a projective object of $\mathcal{M}^C$, and denote $f = \oplus_{i\in I}f_i : P \to M/J(M)$. If $\pi : M \to M/J(M)$ is the natural projection, then there exists a morphism $g : P \to M$ such that $f = \pi g$ (use that P is projective). This implies that $J(M) + Im(g) = M$. Proposition 3.2.2 shows that $Im(g) = M$, thus $g : P \to M$ is surjective. Since $Ker(f)$ is superfluous in P and $Ker(g) \subseteq Ker(f)$, we obtain that $Ker(g)$ is superfluous in P, and then $f : P \to M$ is a projective cover of M. ∎

Corollary 3.2.11 *Let C be a right semiperfect coalgebra and A a subcoalgebra of C. Then A is also right semiperfect.*

Proof: Let M be a simple left A-comodule. Then M is simple when regarded as a left C-comodule. By Theorem 3.2.3 the injective cover $E(M)$ of M in ${}^C\mathcal{M}$ is finite dimensional. If $\mathcal{C}_A$ is the closed subcategory associated to the subcoalgebra A (see Theorem 2.5.5), and t_A the preradical associated to $\mathcal{C}_A$, let $E'(M) = t_A(E(M))$. Then $E'(M)$ is the injective envelope of M in the category ${}^A\mathcal{M}$. Therefore $dim(E'(M)) \leq dim(E(M)) < \infty$. ∎

Corollary 3.2.12 *Let C be a coalgebra and $Rat : {}_{C^*}\mathcal{M} \to Rat({}_{C^*}\mathcal{M})$ the functor which takes every C^*-module to its rational part. Then the following are equivalent.*
(i) C is right semiperfect.
(ii) Rat is an exact functor.
Moreover, if C is right semiperfect, then $Rat({}_{C^*}\mathcal{M})$ is a localizing subcategory of ${}_{C^*}\mathcal{M}$.

Proof: $(i) \Rightarrow (ii)$ Assume that C is right semiperfect. We already know that the functor Rat is left exact. Let

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

be an exact sequence in ${}_{C^*}\mathcal{M}$. Then we have the commutative digram

$$\begin{array}{ccccccccc}
0 & \to & Rat(M') & \to & Rat(M) & \to & Rat(M") & & \\
 & & \downarrow{\scriptstyle i'} & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i"} & & \\
0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M" & \longrightarrow & 0
\end{array}$$

where i', i and i'' are the inclusion maps. Since $Rat(_{C^*}\mathcal{M})$ has enough projectives, there exists an epimorphism $f : P \to Rat(M'')$ for some projective object $P \in Rat(_{C^*}\mathcal{M})$. By Corollary 2.4.22, P is also projective in $_{C^*}\mathcal{M}$, and then there exists $g : P \to M$ such that $vg = i''f$. We have that $Im(g) \subseteq Rat(M)$, and denote by $g' : P \to Rat(M)$ the corestriction of g. Then $g = ig'$, and $vig' = i''f$. Since $vi = i''v'$, we have $i''v'g' = i''f$, so $v'g' = f$. Since f is an epimorphism, we see that v' is an epimorphism, therefore Rat is exact.
$(ii) \Rightarrow (i)$ Let $M \in \mathcal{M}^C = Rat(_{C^*}\mathcal{M})$. We show that $Rat(M^*)$ is dense in M^*. Let $m \in M, m \neq 0$ and N a finite dimensional subcomodule of M such that $m \in N$. If $j : N \to M$ is the inclusion map, then $j^* : M^* \to N^*$ is a surjective morphism of C^*-modules. The hypothesis implies that we have an exact sequence

$$Rat(M^*) \longrightarrow Rat(N^*) \longrightarrow 0$$

But $Rat(N^*) = N^*$ since N is finite dimensional. Pick $f \in N^*$ such that $f(m) \neq 0$. The exactness of the above sequence shows that there exists $g \in Rat(M^*)$ such that $f = j^*(g) = gj$. Then $g(m) = f(m) \neq 0$, which shows that $Rat(M^*)$ is dense in M^*.
We prove now that if C is right semiperfect, then $Rat(_{C^*}\mathcal{M})$ is a localizing subcategory of $_{C^*}\mathcal{M}$. Indeed, it is enough to prove that $Rat(_{C^*}\mathcal{M})$ is closed under extensions. If

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is an exact sequence in $_{C^*}\mathcal{M}$ such that $M', M'' \in Rat(_{C^*}\mathcal{M})$, we obtain a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & Rat(M') \arrow[r] \arrow[d, equal] & Rat(M) \arrow[r] \arrow[d, "i"] & Rat(M'') \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0
\end{tikzcd}$$

The Serpent Lemma shows that $Coker(i) = 0$, so i is surjective. ∎

Remark 3.2.13 *If the category of rational C^*-modules is a localizing subcategory of the category of modules over C^* it does not necessarily follow that C is right semiperfect, as it can be seen by looking at the coalgebra from Example 3.2.7.* ∎

Since $\mathcal{M}^C$ is a Grothendieck category, it has arbitrary direct products, i.e. for any family of objects there exists a direct product of the family in $\mathcal{M}^C$. The direct product functor is left exact, but it is not always exact. However, for semiperfect coalgebras it is exact.

Corollary 3.2.14 *Let C be a right semiperfect coalgebra. Then the direct product functor in the category $\mathcal{M}^C$ is an exact functor (i.e. the category $\mathcal{M}^C$ has the property Ab4* of Grothendieck).*

Proof: It is enough to prove the fact for the subcategory $Rat({}_{C^*}\mathcal{M})$ of ${}_{C^*}\mathcal{M}$. If $(M_i)_{i\in I}$ is a family of rational left C^*-modules, then the direct product of this family in the category $Rat({}_{C^*}\mathcal{M})$ is $Rat(\prod_{i\in I}^* M_i)$, where by $\prod^*$ we denote here the direct product in the category ${}_{C^*}\mathcal{M}$. Since $\prod_{i\in I}^* -$ is an exact functor in ${}_{C^*}\mathcal{M}$, we obtain from Corollary 3.2.12 that $\prod_{i\in I} -$ is an exact functor in $Rat({}_{C^*}\mathcal{M})$. ∎

Lemma 3.2.15 *Let $M \in \mathcal{M}^C$, X a subspace of C^*, and Y a subspace of M. Then $\overline{X}Y = XY$, where $\overline{X}$ is the closure of X in the finite topology.*

Proof: We obviously have $XY \subseteq \overline{X}Y$. Let $f \in \overline{X}$ and $y \in Y$. If $\rho : M \to M \otimes C$ is the comodule structure map of M, $\rho(y) = \sum y_0 \otimes y_1$, then $fy = \sum f(y_1)y_0$. Since X is dense in $\overline{X}$, there exists $g \in X$ such that $g(y_1) = f(y_1)$ for all y_1's. Then $gy = \sum g(y_1)y_0 = fy$, so $fy = gy \in XY$. Thus $\overline{X}Y \subseteq XY$, which ends the proof. ∎

We can give now some properties of coalgebras which are left and right semiperfect.

Corollary 3.2.16 *Let C be a right semiperfect coalgebra. Then $Rat({}_{C^*}C^*)$ is an idempotent two-sided ideal of C^*. Moreover, if C is left and right semiperfect then $Rat({}_{C^*}C^*) = Rat(C^*_{C^*})$.*

Proof: Clearly $I = Rat({}_{C^*}C^*)$ is a two-sided ideal of the ring C^*. By Theorem 3.2.3 we have $\overline{I} = C^*$. Then Lemma 3.2.15 shows that

$$II = \overline{I}I = C^*I = I$$

so $I^2 = I$.

Assume now that C is also left semiperfect and let $J = Rat(C^*_{C^*})$, which is also a two-sided ideal of C^*. We know that $I \in \mathcal{M}^C$ and $J \in {}^C\mathcal{M}$. Since C is left and right semiperfect we have $\overline{I} = \overline{J} = C^*$, and then by Lemma 3.2.15 we have

$$JI = \overline{J}I = C^*I = I$$

On the other hand, by a version of Lemma 3.2.15 for left comodules we have

$$JI = J\overline{I} = JC^* = J$$

We obtain $I = J$. ∎

Let C be a coalgebra. We know that the coradical $C_0 = s({}_CC) = s(C_C)$, where $s({}_CC)$, respectively $s(C_C)$, is the socle of C as a left, respectively right, C-comodule. Let $s(C_C) = \oplus_{j\in J}M_j$ and $s({}_CC) = \oplus_{p\in P}N_p$ be representations of the socles as direct sum of simple comodules (the M_j's are right comodules and the N_p's are left comodules). Then $C = \oplus_{j\in J}E(M_j)$ as right C-comodules, where $E(M_j)$ is the injective envelope of M_j as a right C-comodule. Then

$$C^* \simeq \prod_{j\in J} E(M_j)^*$$

as right C^*-modules. We will identify these two C^*-modules. An element $c^* \in C^*$ is thus identified to the set $(c^*_{|E(M_j)})_{j\in J}$ of the restrictions of c^* to the subspaces $E(M_j)$'s.
Similarly we have $C = \oplus_{p\in P}E(N_p)$, and

$$C^* \simeq \prod_{p\in P} E(N_p)^*$$

as left C^*-modules, isomorphism which we also regard as an identification.

Corollary 3.2.17 *Let C be a left and right semiperfect coalgebra and keep the above notation. Then the following assertions are true.*
i) $Rat({}_{C^*}C^*) = Rat(C^*_{C^*}) = \oplus_{p\in P}E(N_p)^* = \oplus_{j\in J}E(M_j)^*$. In particular the ideal $C^{*rat} = Rat({}_{C^*}C^*) = Rat(C^*_{C^*})$ is left and right projective over the ring C^*.
ii) C^{*rat} is a ring with local units, i.e. for any finite subset X of C^{*rat} there exists an idempotent $e \in C^{*rat}$ such that $ex = xe = x$ for any $x \in X$ (we say that the set consisiting of all these idempotents e appearing from finite subsets X is a system of local units).

Proof: i) Since C is left and right semiperfect we have that $E(M_j)$ and $E(N_p)$ are finite dimensional for any j and p. Then $E(M_j)^*$ is a finite dimensional right ideal of C^*, so we obtain from Corollary 2.2.16 that $E(M_j)^* \subseteq Rat(C^*_{C^*})$. Thus $\oplus_{j\in J}E(M_j)^* \subseteq Rat(C^*_{C^*})$.
Let $h^* \in Rat({}_{C^*}C^*)$. Then there exist two families of elements $h_i^* \in C^*$ and $h_i \in C$ such that

$$g^*h^* = \sum_i g^*(h_i)h_i^*$$

for any $g^* \in C^*$. We can find a finite subset $F \subseteq J$ such that $h_i \in \oplus_{j\in F}E(M_j)$ for any i. Then we define $g^* \in C^*$ such that $g^* = \varepsilon$ on $E(M_j)$

if $j \notin F$ and $g^* = 0$ on any $E(M_j)$ with $j \in F$. Then $g^*h^* = 0$, since $g^*(h_i) = 0$ for any i.
On the other hand, for any $j \notin F$ and any $h \in E(M_j)$ we have $\Delta(h) \in E(M_j) \otimes C$, therefore

$$\begin{aligned}(g^*h^*)(h) &= \sum g^*(h_1)h^*(h_2) \\ &= \sum \epsilon(h_1)h^*(h_2) \\ &= h^*(h)\end{aligned}$$

Since $h^* = 0$ on any $E(M_j)$ with $j \notin F$, we have

$$h^* \in \oplus_{j\in F} E(M_j)^* \subseteq \oplus_{j\in J} E(M_j)^*$$

Thus we have showed that

$$Rat({}_{C^*}C^*) \subseteq \oplus_{j\in J} E(M_j)^* \subseteq Rat(C^*_{C^*})$$

Similarly, working with simple left comodules we obtain

$$Rat(C^*_{C^*}) \subseteq \oplus_{p\in P} E(N_p)^* \subseteq Rat({}_{C^*}C^*)$$

which ends the proof of the first part. Note that this provides a proof of the fact that $Rat(C^*_{C^*}) = Rat({}_{C^*}C^*)$ different from the one given in Corollary 3.2.16.
The fact that C^{*rat} is left and right projective over C^* follows from the fact that $E(M_j)^*$ are projective right ideals in C^* and $E(N_p)^*$ are projective left ideals of C^*.
ii) For any $i \in J$ we define $\varepsilon_i \in C^*$ to be ε on $E(M_i)$ and 0 on any $E(M_j)$ with $j \neq i$. Since $(\varepsilon_i c^*)(c) = \sum \varepsilon_i(c_1)c^*(c_2)$ and $\Delta(E(M_j)) \subseteq E(M_j) \otimes C$, we see that $(\varepsilon_i c^*)(c) = c^*(c)$ for $c \in E(M_i)$ and $(\varepsilon_i c^*)(c) = 0$ for $c \in E(M_j)$, $j \neq i$. Thus $\varepsilon_i c^* = c^*$ for $c^* \in E(M_i)^*$ and $\varepsilon_i c^* = 0$ for $c^* \in E(M_j)^*$, $j \neq i$. In particular $\varepsilon_i^2 = \varepsilon_i$ and $\varepsilon_i \varepsilon_j = 0$ for $i \neq j$.
For a fixed $i \in I$ there exists a finite set $F \subseteq J$ such that $\Delta(E(M_i)) \subseteq E(M_i) \otimes (\oplus_{j\in F} E(M_j))$. Then clearly for any $c^* \in E(M_i)^*$ we have that $c^*(\sum_{j\in F} \varepsilon_j) = c^*$. It is obvious now that the set consisting of all finite sums of ε_i's is a system of local units of C^{*rat}. ∎

3.3 Quasi-co-Frobenius and co-Frobenius coalgebras

Definition 3.3.1 *Let C be a coalgebra. Then C is called a left (right) quasi-co-Frobenius coalgebra (shortly QcF coalgebra) if there exists an injective morphism of left (right) C^*-modules from C to a free left (right)*

C^*-module. The coalgebra C is called left (right) co-Frobenius if there exists a monomorphism of left (right) C^*-modules from C to C^*. ∎

Clearly, if C is a left co-Frobenius coalgebra, then it is also a left QcF coalgebra. Conversely, if C is left QcF, then C is not necessarily co-Frobenius, as we will see in Remark 3.3.12.
Let C be a coalgebra. To any bilinear form $b : C \times C \to k$ we associate the linear maps $b_l, b_r : C \to C^*$ defined by

$$b_l(y)(x) = b(x,y)$$

$$b_r(x)(y) = b(x,y)$$

for any $x, y \in C$. Conversely, to any linear map $\phi : C \to C^*$ we associate two bilinear forms $b, b' : C \times C \to k$ defined by

$$b(x,y) = \phi(y)(x)$$

$$b'(x,y) = \phi(x)(y)$$

for any $x, y \in C$. In this case we clearly have $\phi = b_l = b'_r$.

Proposition 3.3.2 *Let C be a coalgebra and $b : C \times C \to k$ a bilinear form. The following assertions are equivalent.*
(i) b is C^*-balanced, i.e. $b(x \leftharpoonup c^*, y) = b(x, c^* \rightharpoonup y)$ for any $x, y \in C$ and $c^* \in C^*$.
(ii) b_l is a morphism of left C^*-modules.
(iii) b_r is a morphism of right C^*-modules.

Proof: Let $x, y \in C$ and $c^* \in C^*$. Then $b_l(c^* \rightharpoonup y)(x) = b(x, c^* \rightharpoonup y)$. On the other hand

$$\begin{aligned}(c^* \rightharpoonup b_l(y))(x) &= b_l(y)(x \leftharpoonup c^*)\\ &= b(x \leftharpoonup c^*, y)\end{aligned}$$

showing the equivalence of (i) and (ii). The equivalence of (i) and (iii) can be proved similarly. ∎

Corollary 3.3.3 *The correspondence $b \mapsto b_l$ (respectively $b \mapsto b_r$) defines a bijection between all C^*-balanced bilinear forms and all morphisms of left (respectively right) C^*-modules from C to C^*.* ∎

A bilinear form $b : C \times C \to k$ is called left (respectively right) nondegenerate if $b(c, y) = 0$ for any $c \in C$ (respectively $b(x, c) = 0$ for any $c \in C$) implies that $y = 0$ (respectively $x = 0$).
A left C^*-module M is torsionless if M embeds in a direct product of copies of C^*. The following characterizes QcF coalgebras.

Theorem 3.3.4 *Let C be a coalgebra. Then the following assertions are equivalent.*
(i) C is left QcF.
(ii) C is a torsionless left C^*-module.
(iii) There exists a family of C^*-balanced bilinear forms $(b_i)_{i\in I}$, $b_i : C\times C \to k$, such that for any non-zero $x \in C$ there exists $i \in I$ such that $b_i(C,x) \neq 0$.
(iv) Every injective right C-comodule is projective.
(v) C is a projective right C-comodule.
(vi) C is a projective left C^*-module.

Proof: $(i) \Rightarrow (ii)$ is obvious.
$(ii) \Rightarrow (iii)$ Let $\theta : C \to (C^*)^I$ be an injective morphism of left C^*-modules, where by $(C^*)^I$ we mean a direct product of copies of C^*. For any $i \in I$, let $p_i : (C^*)^I \to C^*$ be the natural projection on the i-th component of this direct product. Define $b_i : C \times C \to k$ by

$$b_i(x,y) = p_i(\theta(y))(x)$$

for any $x, y \in C$. By Proposition 3.3.2, b_i is a C^*-balanced bilinear form. If $y \in C$, $y \neq 0$, then $\theta(y) \neq 0$, so there exists $i \in I$ such that $p_i(\theta(y)) \neq 0$, i.e. $0 \neq p_i(\theta(y))(c) = b_i(c,y)$ for some $c \in C$.
$(iii) \Rightarrow (ii)$ Define $\theta : C \to (C^*)^I$ by $\theta(c) = (\theta_i(c))_{i\in I}$, where $\theta_i(c) : C \to k$ is given by $\theta_i(c)(d) = b_i(d,c)$. Since b_i is C^*-balanced, θ_i is a morphism of left C^*-modules. If $\theta(c) = 0$, then $\theta_i(c) = 0$ for any $i \in I$, so $b_i(d,c) = 0$ for any $i \in I$ and $d \in C$. This shows that $c = 0$, so θ is a monomorphism and then C is a torsionless left C^*-module.
(ii) and $(iii) \Rightarrow (vi)$ We know that $C = \oplus_{i\in I} E(S_i)$ as right C-comodules, for some simple right C-comodules S_i ($E(S)$ denotes the injective envelope of S). Thus it is enough to show that for any simple right C-comodule S, the injective envelope $E(S)$ of S in the category $\mathcal{M}^C$ is a projective left C^*-module. We can assume that S is a minimal right coideal of C, say $S = C^* \rightharpoonup x$ for some non-zero $x \in C$. Then there exist $i \in I$ and $c \in C$ such that $b_i(c,x) \neq 0$. Denote by

$$U = \{y \in C | b_i(z,y) = 0 \text{ for all } z \in c \leftharpoonup C^*\}$$

Since b_i is C^*-balanced, U is a left C^*-submodule of C, i.e. a right coideal of C. If $S \cap U \neq 0$, since S is minimal we see that $S \subseteq U$. In particular $x \in U$, so $b_i(c,x) = 0$, a contradiction. Thus $S \cap U = 0$. Since S is essential in $E(S)$ (we consider an injective envelope $E(S)$ of S such that $E(S) \subseteq C$), we must have $E(S) \cap U = 0$. Let $(b_i)_l : C \to C^*$ be the morphism of left C^*-modules defined by b_i, i.e. $(b_i)_l(y)(z) = b_i(z,y)$ for any $z, y \in C$. Define the map $\alpha_i : C \to (c \leftharpoonup C^*)^*$ such that for any $y \in C$, $\alpha_i(y)$ is the restriction of $(b_i)_l$ to $c \leftharpoonup C^*$, i.e. $\alpha_i(y)(z) = b_i(z,y)$ for any $z \in c \leftharpoonup C^*$. Clearly $(c \leftharpoonup C^*)^*$ is a left C^*-module. If $c^* \in C^*$ we have

$$\begin{aligned}
\alpha_i(c^* \rightharpoonup y)(z) &= b_i(z, c^* \rightharpoonup y) \\
&= b_i(z \leftharpoonup c^*, y) \\
&= \alpha_i(y)(z \leftharpoonup c^*) \\
&= (c^*\alpha_i(y))(z)
\end{aligned}$$

so α_i is a morphism of left C^*-modules. On the other hand we clearly have $Ker(\alpha_i) = U$. Since $dim(U)$ is finite, then $dim(C/U)$ is finite. Since $E(S) \cap U = 0$, there exists a monomorphism $E(S) \longrightarrow C/U$, in particular $E(S)$ has finite dimension.

We have an injective morphism of left C^*-modules

$$f : E(S) \longrightarrow C \longrightarrow (C^*)^I$$

Since $E(S)$ is finite dimensional, it is an artinian left C^*-module, so $E(S)$ embeds in a finitely generated free left C^*-module. But $E(S)$ is injective as a left C^*-module (see Corollary 2.4.19), so $E(S)$ is isomorphic to a direct summand of a free left C^*-module, and then it is a projective left C^*-module.

$(vi) \Rightarrow (v)$ is obvious.

$(v) \Rightarrow (iv)$ If Q is injective in $\mathcal{M}^C$, there exists a non-empty set I such that Q is isomorphic to a direct summand of $C^{(I)}$ as a right C-comodule. The hypothesis tells that $C^{(I)}$ is projective in $\mathcal{M}^C$, and then so is Q.

$(iv) \Rightarrow (i)$ Let $C = \oplus_{i\in I} E(S_i)$ as right C-comodules, where S_i are simple C-comodules. By hypothesis any $E(S_i)$ is projective in the category $\mathcal{M}^C$, and it is also indecomposable. Let us fix some $i \in I$. There exist a family $(M_j)_{j\in J}$ of finite dimensional right C-comodules and an epimorphism

$$\oplus_{j\in J} M_j \longrightarrow E(S_i) \longrightarrow 0$$

Since $E(S_i)$ is projective, then it is isomorphic to a direct summand of $\oplus_{j\in J} M_j$. The Krull-Schmidt Theorem shows now that $E(S_i)$ is isomorphic to an indecomposable direct summand of some M_j. Thus $E(S_i)$ is finite dimensional. Corollary 2.4.22 shows that $E(S_i)$ is a projective left C^*-module, thus isomorphic to a direct summand of a free left C^*-module. Then C is isomorphic to a direct summand of a free left C^*-module, i.e. C is a left QcF coalgebra. ∎

The proof of Theorem 3.3.4 gives also the following characterization of co-Frobenius coalgebras.

Theorem 3.3.5 *Let C be a coalgebra. Then the following assertions are equivalent.*

(i) C is a left co-Frobenius coalgebra.
(ii) There exists a C^*-balanced bilinear form which is left nondegenerate. ∎

Corollary 3.3.6 *Let C be a left QcF coalgebra. Then*
(i) C is a left semiperfect coalgebra.
(ii) $Rat({}_{C^*}C^*) \neq 0$

Proof: (i) It follows from the proof of (ii) *and* $(iii) \Rightarrow (vi)$ in Theorem 3.3.4 that the injective envelope of a simple right comodule is finite dimensional.
(ii) Since C is a left QcF coalgebra, there exists a monomorphism of left C^*-modules

$$0 \longrightarrow C \longrightarrow (C^*)^{(I)}$$

for some set I. Then $Rat((C^*)^{(I)})$ contains C. On the other hand

$$Rat((C^*)^{(I)}) = (Rat({}_{C^*}C^*))^{(I)},$$

so $Rat({}_{C^*}C^*) \neq 0$. ∎

Example 3.3.7 *Let C be the coalgebra from Example 3.2.8. We keep the same notation and define the linear map $\theta : C \to C^*$ by $\theta(g_i) = d_i^*$ and $\theta(d_i) = g_{i+1}^*$ for any i. It is easy to see that θ is an injective morphism of left C^*-modules, so C is a left co-Frobenius coalgebra.*
On the other hand C is not right co-Frobenius. Indeed, if $b : C \times C \to k$ is a C^*-balanced bilinear form, then

$$\begin{aligned} b(g_1, g_i) &= b(g_1, d_i^* \rightharpoonup d_i) \\ &= b(g_1 \leftharpoonup d_i^*, d_i) \\ &= b(0, d_i) \\ &= 0 \end{aligned}$$

and

$$\begin{aligned} b(g_1, d_i) &= b(g_1, g_{i+1}^* \rightharpoonup d_i) \\ &= b(g_1 \leftharpoonup g_{i+1}^*, d_i) \\ &= b(0, d_i) \\ &= 0 \end{aligned}$$

so $b(g_1, c) = 0$ for any $c \in C$, i.e. b is not right nondegenerate.
We also show that C is left QcF (obviously, since C is left co-Frobenius), but C is not right QcF. Indeed, if C were right QcF, then C would be a projective right C^*-module. Then $g_1^* \rightharpoonup C$ is projective, too. If we denote $M = g_1^* \rightharpoonup C = kg_1$, then the left C^*-module M^* is indecomposable and injective. Thus $M^* \simeq C \leftharpoonup g_j^*$ for some j. But $dim(C \leftharpoonup g_j^*) = 2$ for any j, while $dim(M^*) = 1$, a contradiction. ∎

Lemma 3.3.8 *Let C be a coalgebra. Then the algebra C^* is right selfinjective if and only if C is flat as a left C^*-module.*

Proof: We know that $C^*_{C^*}$ is injective $\Leftrightarrow$ the functor $Hom_{C^*}(-, C^*_{C^*})$ is exact, and ${}_{C^*}C^*$ is flat if and only if the functor $- \otimes_{C^*} C$ is exact. Now the result follows from the fact that for any right C^*-module M we have that

$$Hom_{C^*}(M, C^*_{C^*}) \simeq Hom_k(M \otimes_{C^*} C, k)$$

This last isomorphism follows from the fact that the functor $- \otimes_{C^*} C : \mathcal{M}_{C^*} \to {}_k\mathcal{M}$ is a left adjoint of the functor $Hom_k(C, -) : {}_k\mathcal{M} \to \mathcal{M}_{C^*}$. ∎

Corollary 3.3.9 *If C is a left QcF coalgebra, then C^* is a right selfinjective algebra, i.e. C^* is an injective right C^*-module.*

Proof: By Theorem 3.3.4, C is a projective left C^*-module, in particular a flat C^*-module. Now apply Lemma 3.3.8. ∎

Corollary 3.3.10 *If C is a left QcF coalgebra, then C is a generator of the category ${}^C\mathcal{M}$.*

Proof: It is enough to show that any finite dimensional $M \in {}^C\mathcal{M}$ is generated by C. Since M is finite dimensional, there exists an epimorphism of right C^*-modules

$$(C^*)^n \longrightarrow M \longrightarrow 0$$

for some positive integer n. Since C is left semiperfect, the functor $Rat : \mathcal{M}_{C^*} \to \mathcal{M}_{C^*}$ is exact. We obtain an exact sequence

$$(Rat(C^*_{C^*}))^n \longrightarrow M \longrightarrow 0$$

By Corollary 3.3.9 the object $Rat(C^*_{C^*})$ is injective in the category $Rat(\mathcal{M}_{C^*})$, i.e. $Rat(C^*_{C^*})$ is injective in the category ${}^C\mathcal{M}$. Since any left comodule embeds in a direct sum of copies of C, $Rat(C^*_{C^*})$ is a direct summand (as a left C-comodule) of a direct sum $C^{(I)}$ of copies of C. In particular there exists an epimorphism

$$C^{(I)} \longrightarrow Rat(C^*_{C^*}) \longrightarrow 0$$

in the category ${}^C\mathcal{M}$. This shows that C generates M. ∎

Corollary 3.3.11 *The following conditions are equivalent for a coalgebra C.*
(i) C is left and right QcF.
(ii) C is a projective generator in the category ${}^C\mathcal{M}$.
(iii) C is a projective generator in the category $\mathcal{M}^C$.
(iv) C^* is a left and right selfinjective algebra and C is a generator for the categories ${}^C\mathcal{M}$ and $\mathcal{M}^C$.

Proof: $(i) \Rightarrow (ii)$ follows from Theorem 3.3.4 and Corollary 3.3.10.
$(ii) \Rightarrow (i)$ By Theorem 3.3.4 we have that C is a left QcF coalgebra. Moreover, C is right QcF if and only if C_{C^*} is torsionless. But C_{C^*} is an essential extension of its socle $s(C_{C^*}) = s({}_CC) = C_0$, the coradical of C. Since $C^*_{C^*}$ is injective by Corollary 3.3.9, we have that C_{C^*} is torsionless if and only if so is every simple right C^*-subcomodule of C. Let M be a rational simple right C^*-module, i.e. a simple left C-comodule. Then $M \simeq N^*$ for a simple right C-comodule N. Since C is generator in $\mathcal{M}^C$, there exists an epimorphism

$$C^{(I)} \longrightarrow N \longrightarrow 0$$

for a finite set I. Then $M \simeq N^*$ embeds in $(C^*)^I$, so M is torsionless.
$(i) \Leftrightarrow (iii)$ is proved similarly.
$(i) \Rightarrow (iv)$ follows from Corollaries 3.3.9 and 3.3.10.
$(iv) \Rightarrow (i)$ is proved in the same way as $(ii) \Rightarrow (i)$. ∎

Remark 3.3.12 *An algebra A is called quasi-Frobenius if A is left artinian and A is an injective left A-module. If A is so, then A is also right artinian and injective as a right A-module (see for instance [65, section 58]), thus the concept of quasi-Frobenius is left-right symmetric. A finite dimensional algebra A is called Frobenius if A and A^* are isomorphic as left (or equivalently right) A-modules. It is known that a Frobenius algebra is necessarily quasi-Frobenius, while there exist finite dimensional algebras which are quasi-Frobenius but not Frobenius (such an example was given by T. Nakayama in [157] and [158]).*
Let C be a finite dimensional coalgebra. It follows immediatelly from the definition that C is left co-Frobenius if and only if the dual algebra C^* is Frobenius, and this is also equivalent to the fact that C is right co-Frobenius. Also, by Corollary 3.3.9, Theorem 3.3.4 and Corollary 2.4.20 we see that C is left QcF if and only if the dual algebra C^* is quasi-Frobenius, and this is also equivalent to C being right QcF.
Now we can see that there exist coalgebras which are left QcF but not left co-Frobenius. Indeed, if we take A to be a finite dimensional algebra which is quasi-Frobenius but not Frobenius, then the dual coalgebra A^* is QcF but not co-Frobenius. ∎

Exercise 3.3.13 *Let C be a right semiperfect coalgebra. Show that if the category $\mathcal{M}^C$ (or ${}^C\mathcal{M}$) has finitely many isomorphism types of simple objects, then C is finite dimensional.*

Exercise 3.3.14 *Let C be a coalgebra. Show that the category $\mathcal{M}^C$ is equivalent to the category of modules ${}_A\mathcal{M}$ for some ring with identity A if and only if C has finite dimension.*

Exercise 3.3.15 *Let $(C_i)_{i\in I}$ be a family of coalgebras and $C = \oplus_{i\in I}C_i$. Show that C is right semiperfect if and only if C_i is right semiperfect for any $i \in I$.*

Exercise 3.3.16 *Let C be a cocommutative coalgebra. Show that C is right (left) semiperfect if and only if $C = \oplus_{i\in I}C_i$ for some family $(C_i)_{i\in I}$ of finite dimensional coalgebras.*

Exercise 3.3.17 *(a) Let $(C_i)_{i\in I}$ be a family of left co-Frobenius (respectively left QcF) coalgebras and $C = \oplus_{i\in I}C_i$. Show that C is left co-Frobenius (respectively left QcF).*
(b) Show that a cosemisimple coalgebra is left (and right) co-Frobenius.

3.4 Solutions to exercises

Exercise 3.1.1 *Let C be a coalgebra. Show that C is a simple coalgebra if and only if the dual algebra C^* is a simple artinian algebra. If this is the case, then C is a sum of isomorphic simple right C-subcomodules.*
Moreover, if the field k is algebraically closed, then C is isomorphic to a matrix coalgebra over k.
Solution: Assume that C is a simple coalgebra. If I is a two-sided ideal of C^*, then $I^\perp$ is a subcoalgebra of C, so either $I^\perp = 0$ or $I^\perp = C$. In the first case we obtain $I = C^*$ and in the second case we have $I = 0$. Thus C^* is a simple algebra. On the other hand C is finite dimensional since it is simple, and then C^* is finite dimensional, in particular artinian.
Conversely, assume that C^* is simple artinian and let J be a subcoalgebra of C. Then $J^\perp$ is a two-sided ideal of C^*, so either $J^\perp = 0$ or $J^\perp = C^*$. This shows that J is either 0 or the whole of C.
If C is simple, then C^* is simple artinian, thus any left C^*-module is semisimple. In particular, C is a semisimple left C^*-module, so C is a sum of simple left C^*-submodules, i.e. a sum of simple right C-subcomodules.
For the last assertion, we have that C^* is isomorphic to a matrix algebra over a finite extension of k. Since k is algebraically closed, this implies that the extension must be k, and then $C^* \simeq M_n(k)$, where $n = dim(M)$. This shows that $C \simeq M^c(n,k)$.

Exercise 3.1.2 *Let M be a simple right comodule over the coalgebra C. Show that:*
(i) The coalgebra A associated to M is a simple coalgebra.
(ii) If the field k is algebraically closed, then $A \simeq M^c(n,k)$, where $n = dim(M)$. In particular the family $(c_{ij})_{1\le i,j\le n}$ defined in Exercise 2.5.4 is a basis of A.

Solution: (i) We know from Proposition 2.5.3 that A is the smallest subcoalgebra of C such that M is a right A-comodule. We regard M as an object in the category $\mathcal{M}^A$. Since A is the coalgebra associated to M, we have that $A = (ann_{A^*}(M))^{\perp}$, so then $ann_{A^*}(M) = 0$. Thus M is a simple faithful left A^*-module, so A^* is a simple artinian algebra. By Exercise 3.1.1 we see that A is a simple coalgebra.
(ii) follows from (i) and Exercise 3.1.1.

Exercise 3.1.3 *Let M and N be two simple right comodules over a coalgebra C. Show that M and N are isomorphic if and only if they have the same associated coalgebra.*
Solution: If M and N are isomorphic as right C-comodules, they are also isomorphic as left C^*-modules, so then $ann_{C^*}(M) = ann_{C^*}(N)$, and the associated coalgebras $(ann_{C^*}(M))^{\perp}$ and $(ann_{C^*}(N))^{\perp}$ are clearly equal. Conversely, if M and N have the same associated coalgebra A, then A is a simple subcoalgebra and any two simple A-comodules are isomorphic. In particular M and N are isomorphic.

Exercise 3.1.6 *Let C be a cosemisimple coalgebra. Show that C is a direct sum of simple subcoalgebras. Moreover, show that any subcoalgebra of C is cosemisimple.*
Solution: Let $(C_i)_{i\in I}$ be the family of all simple subcoalgebras of C. Then the sum $\sum_{i\in I} C_i$ is direct. Indeed, if for some $j \in I$ we have $C_j \subseteq \sum_{i\in I-\{j\}} C_i$, then by Exercise 2.2.19 we have that $C_j \subseteq C_t$ for some $t \in I - \{j\}$. Since C_t is simple we see that $C_t = C_j$, a contradiction.
If D is a subcoalgebra of $C = \oplus_{i\in I} C_i$, then by Exercise 2.2.18(iv) we have that $D = \oplus_{i\in I} A_i$, where A_i is a subcoalgebra of C_i for any i. Then either $A_i = 0$ or $A_i = C_i$, and we are done.

Exercise 3.1.7 *Let C be a finite dimensional coalgebra. Show that C is cosemisimple if and only if the dual algebra C^* is semisimple.*
Solution: We know that C is cosemisimple if and only if the category of right C-comodules $\mathcal{M}^C$ is semisimple. Also, C^* is semisimple if and only if the category of left C^*-modules ${}_{C^*}\mathcal{M}$ is semisimple. The result follows now from the fact that the categories $\mathcal{M}^C$ and ${}_{C^*}\mathcal{M}$ are isomorphic.

Exercise 3.1.11 *Show that the coradical filtration is a coalgebra filtration, i.e. that $\Delta(C_n) \subseteq \sum_{i=0,n} C_i \otimes C_{n-i}$ for any $n \geq 0$.*
Solution: Exercise 2.5.8 shows that $C_n = C_i \wedge C_{n-i-1}$ for any $0 \leq i \leq n-1$, so $\Delta(C_n) \subseteq C_i \otimes C + C \otimes C_{n-i-1}$. Then

$$\Delta(C_n) \subseteq (\cap_{i=0,n-1}(C_i \otimes C + C \otimes C_{n-i-1})) \cap (C_n \otimes C_n)$$

We prove that

$$(\cap_{i=0,n-1}(C_i \otimes C + C \otimes C_{n-i-1})) \cap (C_n \otimes C_n) = \sum_{i=0,n} C_i \otimes C_{n-i}$$

The right hand side is contained in the left hand side since for any $0 \leq i \leq n$ we have $C_i \otimes C_{n-i} \subseteq C_j \otimes C$ for $i \leq j$, and $C_i \otimes C_{n-i} \subseteq C \otimes C_{n-1-j}$ for $j \leq i-1$.
For proving the other inclusion, let us take $C_{i,i+1}$ be a complement of C_i in C_{i+1}, and denote $C_{i,\infty} = \oplus_{i \leq j} C_{j,j+1}$. Clearly

$$C_n \otimes C_n = (C_0 \otimes C_n) \oplus (C_{0,1} \otimes C_n) \oplus \ldots \oplus (C_{n-1,n} \otimes C_n)$$

If $z \in (\cap_{i=0,n-1}(C_i \otimes C + C \otimes C_{n-i-1})) \cap (C_n \otimes C_n) = S$, write $z = z_0 + z_1 + \ldots + z_n$, with $z_0 \in C_0 \otimes C_n$, $z_1 \in C_{0,1} \otimes C_n, \ldots, z_n \in C_{n-1,n} \otimes C_n$. We prove by induction on $0 \leq i \leq n$ that $z_i \in C_i \otimes C_{n-i}$. This is clear for $i = 0$. Assume it is true for $i < j$ (where $1 \leq j$). We show that $z_j \in C_j \otimes C_{n-j}$. Since $z \in S$ we have that

$$z \in C_{j-1} \otimes C + C \otimes C_{n-j} = (C_{j-1} \otimes C) \oplus (C_{j-1,j} \otimes C_{n-j}) \oplus (C_{j,\infty} \otimes C_{n-j})$$

The induction hypothesis shows that $z_1 + \ldots + z_{j-1} \in C_{j-1} \otimes C$. We have that $z_j \in C_{j-1,j} \otimes C_n$ and obviously $z_{j+1} + \ldots + z_n \in C_{j,\infty} \otimes C_n$. Thus we must have

$$z_j \in (C_{j-1,j} \otimes C_n) \cap (C_{j-1,j} \otimes C_{n-j}) = C_{j-1,j} \otimes C_{n-j} \subseteq C_j \otimes C_{n-j}$$

which ends the proof.

Exercise 3.1.12 *Let C be a coalgebra and D a subcoalgebra of C such that $\cup_{n \geq 0}(\wedge^n D) = C$. Show that $Corad(C) \subseteq D$.*
Solution: Denote by $I = D^\perp$, which is an ideal in C^*. We know from Lemma 2.5.7 that $\wedge^{n+1} D = (I^{n+1})^\perp$. Let $f \in I$. We define $g : C \to k$ by $g(c) = \varepsilon(c) + \sum_{n \geq 1} f^n(c)$. The definition is correct since for any $c \in C$, $c \in \wedge^{n+1} D$ for some n, and then $c \in (I^{n+1})^\perp$, showing that $f^m(c) = 0$ for any $m \geq n+1$. Moreover, on $\wedge^{n+1} D$ we have

$$(\varepsilon - f)g = (\varepsilon - f)(\varepsilon + f + \ldots + f^n) = \varepsilon - f^{n+1} = \varepsilon$$

Since $\cup_{n \geq 0}(\wedge^n D) = C$, we have that $\varepsilon - f$ is invertible in C^*. Thus $D^\perp \subseteq J(C^*)$, and then $Corad(C) = J(C^*)^\perp \subseteq D$.

Exercise 3.1.13 *Let $f : C \to D$ be a surjective morphism of coalgebras. Show that $Corad(D) \subseteq f(Corad(C))$.*

Solution: We know from Exercise 2.5.9 that $f(\wedge^n C_0) \subseteq \wedge^n f(C_0)$ for any n. Then we have

$$D = f(C) = f(\cup_{n\geq 0}(\wedge^n C_0)) \subseteq \cup_{n\geq 0}(\wedge^n f(C_0))$$

and since $f(C_0)$ is a subcoalgebra we get by Exercise 3.1.12 that $Corad(D) \subseteq f(Corad(C))$.

Exercise 3.1.14 *Let X, Y and D be subspaces of the linear space C. Show that*

$$(D \otimes D) \cap (X \otimes C + C \otimes Y) = (D \cap X) \otimes D + D \otimes (D \cap Y)$$

Solution: Let D' and X' be complements of $D \cap X$ in $D + X$, and U a complement of $D + X$ in C. Also let D'' and Y' complements of D and Y in $D + Y$, and V a complement of $D + Y$ in C. We have that

$$D\otimes D = ((D\cap X)\otimes(D\cap Y))\oplus((D\cap X)\otimes D'')\oplus(D'\otimes(D\cap Y))\oplus(D'\otimes D'')$$

and

$$\begin{aligned} & X \otimes C + C \otimes Y = \\ = \; & ((D \cap X) \otimes (D \cap Y)) \oplus ((D \cap X) \otimes D'') \oplus \\ & \oplus((D \cap X) \otimes Y') \oplus ((D \cap X) \otimes V) \oplus (X' \otimes (D \cap Y)) \oplus \\ & \oplus(X' \otimes D'') \oplus (X' \otimes Y') \oplus (X' \otimes V) \oplus (D' \otimes (D \cap Y)) \oplus \\ & \oplus(U \otimes (D \cap Y)) \oplus (D' \otimes Y') \oplus (X' \otimes Y') \oplus (U \otimes Y') \end{aligned}$$

These show that

$$(D \otimes D) \cap (X \otimes C + C \otimes Y) =$$
$$= (D \cap X) \otimes (D \cap Y)) \oplus ((D \cap X) \otimes D'') \oplus (D' \otimes (D \cap Y))$$

and this is clearly equal to $(D \cap X) \otimes D + D \otimes (D \cap Y)$.

Exercise 3.1.15 *Let C be a coalgebra and D a subcoalgebra of C. Show that $D_n = D \cup C_n$ for any n.*
Solution: We prove by induction on n. For $n = 0$, the inclusion $D_0 \subseteq D \cap C_0$ is clear, since any simple subcoalgebra of D is also a simple subcoalgebra of C. On the other hand $D \cap C_0$ is a subcoalgebra of C_0, so by Exercise 3.1.6, $D \cap C_0$ is a cosemisimple coalgebra. Thus $D \cap C_0$ is a sum of simple subcoalgebras, which are obviously subcoalgebras of D. This shows that $D \cap C_0 \subseteq D_0$.
Assume now that $D_n = D \cap C_n$ for some n. We prove that $D_{n+1} = D \cap C_{n+1}$. Since

$$\Delta(D_{n+1}) \subseteq D_n \otimes D + D \otimes D_0 \subseteq C_n \otimes C + C \otimes C_0$$

we see that $D_{n+1} \subseteq C_{n+1}$, so $D_{n+1} \subseteq D \cap C_{n+1}$. Conversely, if $d \in D \cap C_{n+1}$, then

$$\begin{aligned}\Delta(d) &\in (D \otimes D) \cap (C_n \otimes C + C \otimes C_0) \\ &= (D \cap C_n) \otimes D + D \otimes (D \cap C_0) \text{ (by Exercise 3.1.14)} \\ &= D_n \otimes D + D \otimes D_0 \text{ (by the induction hypothesis)}\end{aligned}$$

thus $d \in D_{n+1}$, which ends the proof.

Exercise 3.3.13 *Let C be a right semiperfect coalgebra. Show that if the category $\mathcal{M}^C$ (or ${}^C\mathcal{M}$) has finitely many isomorphism types of simple objects, then C is finite dimensional.*
Solution: If S is a simple object in the category $\mathcal{M}^C$, then

$$Com_C(S, C) \simeq Hom_k(S, k) \simeq S^*$$

Since S is finite dimensional, the above isomorphism shows that in the representation of C_0 as a direct sum of simple right C-comodules there exist only finitely many objects isomorphic to S. By the hypothesis we obtain that C_0 is finite dimensional. Since C is right semiperfect we have that the injective envelope $E(S)$ of S is finite dimensional. We conclude that C is finite dimensional since C is the injective envelope of C_0 in ${}^C\mathcal{M}$.

Exercise 3.3.14 *Let C be a coalgebra. Show that the category $\mathcal{M}^C$ is equivalent to the category of modules ${}_A\mathcal{M}$ for some ring with identity A if and only if C has finite dimension.*
Solution: If C has finite dimension, then the category $\mathcal{M}^C$ is even isomorphic to the category ${}_{C^*}\mathcal{M}$ of modules over the dual algebra of C. Conversely, assume that $\mathcal{M}^C$ is equivalent to ${}_A\mathcal{M}$ for a ring with identity A. Let $F : {}_A\mathcal{M} \to \mathcal{M}^C$ be an equivalence functor. Then $P = F({}_AA)$ is a finitely generated projective generator of the category $\mathcal{M}^C$ since so is ${}_AA$ in the category ${}_A\mathcal{M}$. Since any object of $\mathcal{M}^C$ is the sum of subobjects of finite dimension, we obtain that P has finite dimension. Since P is also a generator we have that C is a right semiperfect coalgebra. Since P has finite dimension, $\mathcal{M}^C$ has a finite number of isomorphism types of simple objects. Since C is semiperfect, this implies that C has finite dimension.

Exercise 3.3.15 *Let $(C_i)_{i\in I}$ be a family of coalgebras and $C = \oplus_{i\in I}C_i$. Show that C is right semiperfect if and only if C_i is right semiperfect for any $i \in I$.*
Solution: The claim follows immediately from the equivalence of categories $\mathcal{M}^C \simeq \prod_{i\in I} \mathcal{M}^{C_i}$, proved in Exercise 2.2.18.

Exercise 3.3.16 *Let C be a cocommutative coalgebra. Show that C is right (left) semiperfect if and only if $C = \oplus_{i\in I}C_i$ for some family $(C_i)_{i\in I}$ of finite* *dimensional coalgebras.*

Solution: Assume that C is right semiperfect. Then $C = \oplus_{i\in I}E(S_i)$ for some simple left C-subcomodules $(S_i)_{i\in I}$ of C (as usual $E(S_i)$ denotes the injective envelope of S_i inside C). Since C is right semiperfect, any $E(S_i)$ is finite dimensional, and since C is cocommutative, any $C_i = E(S_i)$ is a subcoalgebra of C. Thus we can write $C = \oplus_{i\in I}C_i$ with all C_i's finite dimensional.

Conversely, if $C = \oplus_{i\in I}C_i$ with any C_i finite dimensional, then any C_i is right semiperfect, and Exercise 3.3.15 shows that C is right semiperfect.

Exercise 3.3.17 *(a) Let $(C_i)_{i\in I}$ be a family of left co-Frobenius (respectively left QcF) coalgebras and $C = \oplus_{i\in I}C_i$. Show that C is left co-Frobenius (respectively left QcF).*

(b) Show that a cosemisimple coalgebra is left (and right) co-Frobenius.

Solution: (a) Assume that each C_i is left co-Frobenius. Then there exists a C_i^*-balanced bilinear form $b_i : C_i \times C_i \to k$ which is left nondegenerate. We construct a bilinear form $b : C \times C \to k$ by $b(c,d) = b_i(c,d)$ for any $i \in I$ and $c, d \in C_i$, and $b(c,d) = 0$ for any $c \in C_i, d \in C_j$ with $i \neq j$. Then clearly b is C^*-balanced and left nondegenerate, so C is left co-Frobenius. One proceeds similarly for the QcF property.

(b) A cosemisimple coalgebra is a direct sum of simple subcoalgebras. On the other hand a simple coalgebra is left and right co-Frobenius since it is finite dimensional and its dual is a simple artinian algebra, thus a Frobenius algebra. By (a) we conclude that a cosemisimple coalgebra is left and right co-Frobenius.

Bibliographical notes

Besides the books of M. Sweedler [218], E. Abe [1], and S. Montgomery [149], we have used for the presentation of this chapter the papers by Y. Doi [72], C. Năstăsescu and J. Gomez Torrecillas [162], B. Lin [123], H. Allen and D. Trushin [2]. We have also used [28], R. Wisbauer's notes [244], and the paper by C. Menini, B. Torrecillas and R. Wisbauer [145], where coalgebras are over rings.

Chapter 4

Bialgebras and Hopf algebras

4.1 Bialgebras

Let H be a k-vector space which is simultaneously endowed with an algebra structure (H, M, u) and a coalgebra structure (H, Δ, ε). The following result describes the situation in which the two structures are compatible. We recall that on $H \otimes H$ we have the structure of a tensor product of coalgebras, and the tensor product of algebras structure, while on k there exists a canonical structure of a coalgebra given in Example 1.1.4 4).

Proposition 4.1.1 *The following assertions are equivalent:*
i) The maps M and u are morphisms of coalgebras.
ii) The maps Δ and ε are morphisms of algebras.

Proof: M is a morphism of coalgebras if and only if the following diagrams are commutative

$$\begin{tikzcd}
H \otimes H \arrow[rr, "M"] \arrow[d, "\Delta \otimes \Delta"'] & & H \arrow[dd, "\Delta"] \\
H \otimes H \otimes H \otimes H \arrow[d, "I \otimes T \otimes I"'] & & \\
H \otimes H \otimes H \otimes H \arrow[rr, "M \otimes M"] & & H \otimes H
\end{tikzcd}$$

$$\begin{tikzcd} H \otimes H \arrow[r, "M"] \arrow[d, "\varepsilon \otimes \varepsilon"'] & H \arrow[dd, "\varepsilon"] \\ k \otimes k \arrow[d, "\phi"'] & \\ k \arrow[r, "Id"] & k \end{tikzcd}$$

The map u is a morphism of coalgebras if and only if the following two diagrams are commutative

$$\begin{tikzcd} k \arrow[r, "u"] \arrow[d, "\phi^{-1}"'] & H \arrow[d, "\Delta"] \\ k \otimes k \arrow[r, "u \otimes u"] & H \otimes H \end{tikzcd}$$

$$\begin{tikzcd} k \arrow[rr, "u"] \arrow[dr, "Id"'] & & H \arrow[dl, "\varepsilon"] \\ & k & \end{tikzcd}$$

We note that Δ is a morphism of algebras if and only if the first and the third diagrams are commutative, and ε is a morphism of algebras if and only if the second and the fourth diagrams are commutative. Therefore, the equivalence of i) and ii) is clear. ∎

Remark 4.1.2 *In the sigma notation, the conditions in which Δ and ε are morphisms of algebras becomes*

$$\Delta(hg) = \sum h_1 g_1 \otimes h_2 g_2, \ \varepsilon(hg) = \varepsilon(h)\varepsilon(g)$$

$$\Delta(1) = 1 \otimes 1, \ \varepsilon(1) = 1$$

Definition 4.1.3 *A* bialgebra *is a k-vector space H, endowed with an algebra structure (H, M, u), and with a coalgebra structure (H, Δ, ε) such that M and u are morphisms of coalgebras (and then by Proposition 4.1.1 it follows that Δ and ε are morphisms of algebras).* ∎

Remark 4.1.4 *We will say that a bialgebra has a property P, if the underlying algebra or coalgebra has property P. Thus we will talk about commutative (or cocommutative) bialgebras, semisimple (or cosemisimple) bialgebras, etc.*
Note for example that if the bialgebra H is commutative, then the multiplication is also a morphism of algebras, and if it is cocommutative, then the comultiplication of H is a morphism of coalgebras too. ∎

Example 4.1.5 *1) The field k, with its algebra structure, and with the canonical coalgebra structure, is a bialgebra.*
2) If G is a monoid, then the semigroup algebra kG endowed with a coalgebra structure as in Example 1.1.4.1) (in which $\Delta(g) = g \otimes g$ and $\varepsilon(g) = 1$ for any $g \in G$) is a bialgebra.
3) If H is a bialgebra, then H^{op}, H^{cop} and $H^{op,cop}$ are bialgebras, where H^{op} has an algebra structure opposite to the one of H, and the same coalgebra structure as H, H^{cop} has the same algebra structure as H, and the coalgebra structure co-opposite to the one of H, and $H^{op,cop}$ has the algebra structure opposite to the one of H, and the coalgebra structure co-opposite to the one of H. ∎

A possible way of constructing new bialgebras is to consider the dual of a finite dimensional bialgebra.

Proposition 4.1.6 *Let H be a finite dimensional bialgebra. Then H^*, together with the algebra structure which is dual to the coalgebra structure of H, and with the coalgebra structure which is dual to the algebra structure of H is a bialgebra, which is called the dual bialgebra of H.*

Proof: We denote by Δ and ε the comultiplication and the counit of H, and by δ and E the comultiplication and the counit of H^*. We recall that for $h^* \in H^*$ we have $E(h^*) = h^*(1)$ and $\delta(h^*) = \sum h_1^* \otimes h_2^*$, where $h^*(hg) = \sum h_1^*(h)h_2^*(g)$ for any $h, g \in H$. Let us show that δ is a morphism of algebras. Indeed, if $h^*, g^* \in H^*$ and $\delta(h^*) = \sum h_1^* \otimes h_2^*$, $\delta(g^*) = \sum g_1^* \otimes g_2^*$, then for any $h, g \in H$ we have

$$(h^*g^*)(hg) = \sum h^*(h_1g_1)g^*(h_2g_2)$$

$$\begin{aligned} &= \sum h_1^*(h_1)h_2^*(g_1)g_1^*(h_2)g_2^*(g_2) \\ &= \sum (h_1^*g_1^*)(h)(h_2^*g_2^*)(g) \end{aligned}$$

which shows that

$$\delta(h^*g^*) = \sum h_1^*g_1^* \otimes h_2^*g_2^* = \delta(h^*)\delta(g^*)$$

Also $\varepsilon(hg) = \varepsilon(h)\varepsilon(g)$ for any $h, g \in H$, hence $\delta(\varepsilon) = \varepsilon \otimes \varepsilon$, and so δ is an algebra map. We show now that E is a morphism of algebras. This is clear, since

$$E(h^*g^*) = (h^*g^*)(1) = h^*(1)g^*(1) = E(h^*)E(g^*)$$

and

$$E(\varepsilon) = \varepsilon(1) = 1,$$

which ends the proof. ∎

Numerous other examples of bialgebras will be given later in this chapter.

Definition 4.1.7 *Let H and L be two k-bialgebras. A k-linear map $f : H \to L$ is called a morphism of bialgebras if it is a morphism of algebras and a morphism of coalgebras between the underlying algebras, respectively coalgebras of the two bialgebras.* ∎

We can now define a new category having as objects all k-bialgebras, and as morphisms the morphisms of bialgebras defined above. It is important to know how to obtain factor objects in this category.

Proposition 4.1.8 *Let H be a bialgebra, and I a k-subspace of H which is an ideal (in the underlying algebra of H) and a coideal (in the underlying coalgebra of H). Then the structures of factor algebra and of factor coalgebra on H/I define a bialgebra, and the canonical projection $p : H \to H/I$ is a bialgebra map. Moreover, if the bialgebra H is commutative (respectively cocommutative), then the factor bialgebra H/I is also commutative (respectively cocommutative).*

Proof: Denoting by $\overline{h}$ the coset of an element $h \in H$ modulo I, the coalgebra structure on H/I is defined by $\overline{\Delta}(\overline{h}) = \sum \overline{h_1} \otimes \overline{h_2}$ and $\overline{\varepsilon}(\overline{h}) = \varepsilon(h)$ for any $h \in H$. Then it is clear that $\overline{\Delta}$ and $\overline{\varepsilon}$ are morphisms of algebras. The rest is clear. ∎

Exercise 4.1.9 *Let k be a field and $n \geq 2$ a positive integer. Show that there is no bialgebra structure on $M_n(k)$ such that the underlying algebra structure is the matrix algebra.*

4.2 Hopf algebras

Let (C, Δ, ε) be a coalgebra, and (A, M, u) an algebra. We define on the set $Hom(C, A)$ an algebra structure in which the multiplication, denoted by $*$ is given as follows: if $f, g \in Hom(C, A)$, then

$$(f * g)(c) = \sum f(c_1)g(c_2)$$

for any $c \in C$. The multiplication defined above is associative, since for $f, g, h \in Hom(C, A)$ and $c \in C$ we have

$$\begin{aligned} ((f * g) * h)(c) &= \sum (f * g)(c_1)h(c_2) \\ &= \sum f(c_1)g(c_2)h(c_3) \\ &= \sum f(c_1)(g * h)(c_2) \\ &= (f * (g * h))(c) \end{aligned}$$

The identity element of the algebra $Hom(C, A)$ is $u\varepsilon \in Hom(C, A)$, since

$$(f * (u\varepsilon))(c) = \sum f(c_1)(u\varepsilon)(c_2) = \sum f(c_1)\varepsilon(c_2)1 = f(c)$$

hence $f * (u\varepsilon) = f$. Similarly, $(u\varepsilon) * f = f$.
Let us note that if $A = k$, then $*$ is the convolution product defined on the dual algebra of the coalgebra C. This is why in the case A is an arbitrary algebra we will also call $*$ the convolution product.

Let us consider a special case of the above construction. Let H be a bialgebra. We denote by H^c the underlying coalgebra H, and by H^a the underlying algebra of H. Then we can define as above an algebra structure on $Hom(H^c, H^a)$, in which the multiplication is defined by $(f * g)(h) = \sum f(h_1)g(h_2)$ for any $f, g \in Hom(H^c, H^a)$ and $h \in H$, and the identity element is $u\varepsilon$. We remark that the identity map $I : H \to H$ is an element of $Hom(H^c, H^a)$.

Definition 4.2.1 *Let H be a bialgebra. A linear map $S : H \to H$ is called an* antipode *of the bialgebra H if S is the inverse of the identity map $I : H \to H$ with respect to the convolution product in $Hom(H^c, H^a)$.* ∎

Definition 4.2.2 *A bialgebra H having an antipode is called a* Hopf algebra. ∎

Remarks 4.2.3 *1. In a Hopf algebra, the antipode is unique, being the inverse of the element I in the algebra $Hom(H^c, H^a)$. The fact that S :*

$H \to H$ is the antipode is written as $S * I = I * S = u\varepsilon$, and using the sigma notation

$$\sum S(h_1)h_2 = \sum h_1 S(h_2) = \varepsilon(h)1$$

for any $h \in H$. ∎

Since a Hopf algebra is a bialgebra, we keep the convention from Remark 4.1.4, and we will say that a Hopf algebra has a property P, if the underlying algebra or coalgebra has property P.
In order to define the category of Hopf algebras over the field k, we need the concept of morphism of Hopf algebras.

Definition 4.2.4 *Let H and B be two Hopf algebras. A map $f : H \to B$ is called a morphism of Hopf algebras if it is a morphism of bialgebras.* ∎

It is natural to ask whether a morphism of Hopf algebras should preserve antipodes. The following result shows that this is indeed the case.

Proposition 4.2.5 *Let H and B be two Hopf algebras with antipodes S_H and S_B. If $f : H \to B$ is a bialgebra map, then $S_B f = f S_H$.*

Proof: Consider the algebra $Hom(H, B)$ with the convolution product, and the elements $S_B f$ and $f S_H$ from this algebra. We show that they are both invertible, and that they have the same inverse f, and so it will follow that they are equal. Indeed,

$$\begin{aligned}
((S_B f) * f)(h) &= \sum S_B f(h_1) f(h_2) \\
&= \sum S_B(f(h)_1) f(h)_2 \\
&= \varepsilon_B(f(h))1_B \\
&= \varepsilon_H(h)1_B
\end{aligned}$$

so $S_B f$ is a left inverse for f. Also

$$\begin{aligned}
(f * (f S_H))(h) &= \sum f(h_1) f(S_H(h_2)) \\
&= f(\sum h_1 S_H(h_2)) \\
&= f(\varepsilon_H(h)1_H) \\
&= \varepsilon_H(h)1_B
\end{aligned}$$

hence $f S_H$ is also a right inverse for f. It follows that f is (convolution) invertible, and that the left and right inverses are equal. ∎

We can now define the category of k-Hopf algebras, in which the objects are Hopf algebras over the field k, and the morphisms are the ones defined in Definition 4.2.4. This category will be denoted by $k - HopfAlg$.

We will provide examples of Hopf algebras in the following section. For the time being, we give some basic properties of the antipode.

Proposition 4.2.6 *Let H be a Hopf algebra with antipode S. Then:*
i) $S(hg) = S(g)S(h)$ for any $g, h \in H$.
ii) $S(1) = 1$.
iii) $\Delta(S(h)) = \sum S(h_2) \otimes S(h_1)$.
iv) $\varepsilon(S(h)) = \varepsilon(h)$.
Properties i) and ii) mean that S is an antimorphism of algebras, and iii) and iv) that S is an antimorphism of coalgebras.

Proof: i) Consider $H \otimes H$ with the tensor product of coalgebras structure, and H with the algebra structure. Then it makes sense to talk about the algebra $Hom(H \otimes H, H)$, with the multiplication given by convolution, defined as in the beginning of this section. The identity element of this algebra is $u_H \varepsilon_{H\otimes H} : H \otimes H \to H$.
Consider the maps $F, G, M : H \otimes H \to H$ defined by

$$F(h \otimes g) = S(g)S(h), G(h \otimes g) = S(hg) \text{ and } M(h \otimes g) = hg$$

for any $h, g \in H$. We show that M is a left inverse (with respect to convolution) for F, and a right inverse for G. Indeed, for $h, g \in H$ we have

$$\begin{aligned}
(M * F)(h \otimes g) &= \sum M((h \otimes g)_1)F((h \otimes g)_2) \\
&= \sum M(h_1 \otimes g_1)F(h_2 \otimes g_2) \\
&= \sum h_1 g_1 S(g_2)S(h_2) \\
&= \sum h_1 \varepsilon(g) 1 S(h_2) \quad \text{(definition of } S \text{ for } g) \\
&= \varepsilon(h)\varepsilon(g)1 \qquad \text{(definition of } S \text{ for } h) \\
&= \varepsilon_{H\otimes H}(h \otimes g)1 \\
&= u_H \varepsilon_{H\otimes H}(h \otimes g)
\end{aligned}$$

which shows that $M * F = u_H \varepsilon_{H\otimes H}$. Also

$$\begin{aligned}
(G * M)(h \otimes g) &= \sum G((h \otimes g)_1)M((h \otimes g)_2) \\
&= \sum G(h_1 \otimes g_1)M(h_2 \otimes g_2) \\
&= \sum S(h_1 g_1) h_2 g_2
\end{aligned}$$

$$\begin{aligned} &= \sum S((hg)_1)(hg)_2 \\ &= \varepsilon(hg)1 \quad \text{(definition of } S \text{ for } hg) \\ &= u_H\varepsilon_{H\otimes H}(h\otimes g) \end{aligned}$$

and thus $G * M = u_H\varepsilon_{H\otimes H}$. Hence M is a left inverse for F and a right inverse for G in an algebra, and therefore $F = G$. This means that i) holds.
ii) We apply the definition of the antipode for the element $1 \in H$. We get $S(1)1 = \varepsilon(1)1$. Applying ε it follows that $\varepsilon(S(1)) = \varepsilon(1) = 1$.
iii) Consider now H with the coalgebra structure, and $H \otimes H$ with the structure of tensor product of algebras, and define the algebra $Hom(H, H \otimes H)$, with the multiplication given by the convolution product. The identity element of this algebra is $u_{H\otimes H}\varepsilon_H$. Consider the maps $F, G : H \to H \otimes H$ defined by

$$F(h) = \Delta(S(h)) \text{ and } G(h) = \sum S(h_2) \otimes S(h_1)$$

for any $h \in H$. We show that Δ is a left inverse for F and a right inverse for G with respect to convolution. Indeed, for any $h \in H$ we have

$$\begin{aligned} (\Delta * F)(h) &= \sum \Delta(h_1)F(h_2) \\ &= \sum \Delta(h_1)\Delta(S(h_2)) \\ &= \Delta(\sum h_1S(h_2)) = \Delta(\varepsilon(h)1) = \varepsilon(h)1\otimes 1 \\ &= u_{H\otimes H}\varepsilon_H(h) \end{aligned}$$

and

$$\begin{aligned} (G * \Delta)(h) &= \sum G(h_1)\Delta(h_2) \\ &= \sum (S((h_1)_2) \otimes S((h_1)_1)((h_2)_1 \otimes (h_2)_2) \\ &= \sum (S(h_2) \otimes S(h_1))(h_3 \otimes h_4) \\ &= \sum S(h_2)h_3 \otimes S(h_1)h_4 \\ &= \sum S((h_2)_1)(h_2)_2 \otimes S(h_1)h_3 \\ &= \sum \varepsilon(h_2)1 \otimes S(h_1)h_3 \quad \text{(definition of } S) \\ &= \sum 1 \otimes S(h_1)\varepsilon((h_2)_1)(h_2)_2 \\ &= \sum 1 \otimes S(h_1)h_2 \quad \text{(the counit property)} \\ &= 1 \otimes \varepsilon(h)1 \\ &= u_{H\otimes H}\varepsilon_H(h) \end{aligned}$$

which ends the proof.
iv) We apply ε to the relation $\sum h_1S(h_2)=\varepsilon(h)1$ to get $\sum\varepsilon(h_1)\varepsilon(S(h_2))=\varepsilon(h)$. Since ε and S are linear maps, we obtain $\varepsilon(S(\sum\varepsilon(h_1)h_2))=\varepsilon(h)$. Using the counit property we get $\varepsilon(S(h))=\varepsilon(h)$. ∎

Proposition 4.2.7 *Let H be a Hopf algebra with antipode S. Then the following assertions are equivalent:*
i) $\sum S(h_2)h_1=\varepsilon(h)1$ for any $h\in H$.
ii) $\sum h_2S(h_1)=\varepsilon(h)1$ for any $h\in H$.
iii) $S^2=I$ (by S^2 we mean the composition of S with itself).

Proof: i)$\Rightarrow$iii) We know that I is the inverse of S with respect to convolution. We show that S^2 is a right convolution inverse of S, and by the uniqueness of the inverse it will follow that $S^2=I$. We have

$$\begin{aligned}(S*S^2)(h) &= \sum S(h_1)S^2(h_2)\\ &= \sum S(S(h_2)h_1)\quad (S \text{ is an antimorphism of algebras})\\ &= S(\varepsilon(h)1)\\ &= \varepsilon(h)1\end{aligned}$$

which shows that indeed $S*S^2=u\varepsilon$.
iii)$\Rightarrow$ii) We know that $\sum h_1S(h_2)=\varepsilon(h)1$. Applying the antimorphism of algebras S we obtain $\sum S^2(h_2)S(h_1)=\varepsilon(h)1$. Since $S^2=I$, this becomes $\sum h_2S(h_1)=\varepsilon(h)1$.
ii)$\Rightarrow$iii) We proceed as in i)$\Rightarrow$iii), and we show that S^2 is a left convolution inverse for S. Indeed,

$$(S^2*S)(h)=\sum S^2(h_1)S(h_2)=S(\sum h_2S(h_1))=S(\varepsilon(h)1)=\varepsilon(h)1.$$

iii)$\Rightarrow$i) We apply S to the equality $\sum S(h_1)h_2=\varepsilon(h)1$, and using $S^2=I$ we obtain $\sum S(h_2)h_1=\varepsilon(h)1$. ∎

Corollary 4.2.8 *Let H be a commutative or cocommutative Hopf algebra. Then $S^2=I$.*

Proof: If H is commutative, then by $\sum S(h_1)h_2=\varepsilon(h)1$ it follows that $\sum h_2S(h_1)=\varepsilon(h)1$, i.e. ii) from the preceding proposition.
If H is cocommutative, then

$$\sum h_1\otimes h_2=\sum h_2\otimes h_1,$$

and then by $\sum S(h_1)h_2=\varepsilon(h)1$ it follows that $\sum S(h_2)h_1=\varepsilon(h)1$, i.e. i) from the preceding proposition. ∎

Remark 4.2.9 *If H is a Hopf algebra, then the set $G(H)$ of grouplike elements of H is a group with the multiplication induced by the one of H. Indeed, we first see that $1 \in G(H)$ (this will be the identity element of $G(H)$). If $g, h \in G(H)$, then $gh \in G(H)$ by the fact that Δ is an algebra map. Finally, if g is a grouplike element, then $S(g)$ is also a grouplike element since the antipode is an antimorphism of coalgebras, and the property of the antipode shows that g is invertible with inverse $g^{-1} = S(g)$.* ∎

Remark 4.2.10 *Let H be a Hopf algebra with antipode S. Then the bialgebra $H^{op,cop}$ is a Hopf algebra with the same antipode S. If moreover S is bijective, then the bialgebras H^{op} and H^{cop} are Hopf algebras with antipode S^{-1}.* ∎

In Proposition 4.1.6 we saw that if H is a finite dimensional bialgebra, then its dual is a bialgebra. The following result shows that if H is even a Hopf algebra, then its dual also has a Hopf algebra structure.

Proposition 4.2.11 *Let H be a finite dimensional Hopf algebra, with antipode S. Then the bialgebra H^* is a Hopf algebra, with antipode S^*.*

Proof: We know already that H^* is a bialgebra. It remains to prove that it has an antipode. Let $h^* \in H^*$ and $\delta(h^*) = \sum h_1^* \otimes h_2^*$, where δ is the comultiplication of H^*. Then for $h \in H$ we have

$$\begin{aligned}
\sum (S^*(h_1^*)h_2^*)(h) &= \sum S^*(h_1^*)(h)h_2^*(h_2) \\
&= \sum h_1^*(S(h_1))h_2^*(h_2) \\
&= \sum h^*(S(h_1)h_2) \\
&= h^*(\varepsilon(h)1) \\
&= \varepsilon(h)h^*(1) \\
&= E(h^*)\varepsilon(h)
\end{aligned}$$

where E is the counit of H^*. We proved that $\sum S^*(h_1^*)h_2^* = E(h^*)\varepsilon$. Similarly, one can show that $\sum h_1^* S^*(h_2^*) = E(h^*)\varepsilon$, and the proof is complete. ∎

Definition 4.2.12 *Let H be a Hopf algebra. A subspace A of H is called a Hopf subalgebra if A is a subalgebra, a subcoalgebra, and $S(A) \subseteq A$.*
We note that if A is a Hopf subalgebra of H, then A is itself a Hopf algebra with the induced structures. This concept is just the concept of subobject in the category $k - HopfAlg$. ∎

In order to define the concept of factor Hopf algebra of a Hopf algebra H, we need subspaces of H which are ideals (in order to define a natural algebra structure on the factor space), coideals (to be able to define a natural coalgebra structure on the factor space), and also to be stabilized by the antipode (so that the factor bialgebra which we obtain has an antipode). The following result is immediate.

Proposition 4.2.13 *Let H be a Hopf algebra, and I a Hopf ideal of H, i.e. I is an ideal of the algebra H, a coideal of the coalgebra H, and $S(I) \subseteq I$, where S is the antipode of H. Then on the factor space H/I we can introduce a natural structure of a Hopf algebra. When this structure is defined, the canonical projection $p : H \to H/I$ is a morphism of Hopf algebras.*

Proof: We saw in Proposition 4.1.8 that H/I has a bialgebra structure. Since $S(I) \subseteq I$, the morphism $S : H \to H$ induces a morphism $\overline{S} : H/I \to H/I$ by $\overline{S}(\overline{h}) = \overline{S(h)}$, where $\overline{h}$ denotes the coset of an element $h \in H$ in the factor space H/I. The $\overline{S}$ is an antipode in the factor bialgebra H/I, since

$$\sum \overline{S}(\overline{h_1})\overline{h_2} = \overline{\sum S(h_1)h_2} = \varepsilon(h)\overline{h} = \overline{\varepsilon}(\overline{h})\overline{1}$$

and similarly, $\sum \overline{h_1}\ \overline{S}(\overline{h_2}) = \overline{\varepsilon}(\overline{h})\overline{1}$. ∎

If A is an algebra, and M is a left A-module, then M has a right module structure over A^{op}, but in general M does not have a natural right module structure over A. Also, if C is a coalgebra, and M is a right C-comodule, then M has a natural left comodule structure over the co-opposite coalgebra C^{cop}, but not over C. The following result shows that if we work with a Hopf algebra, then all these are possibile. The role of the antipode is essential in this matter.

Proposition 4.2.14 *Let H be a Hopf algebra with antipode S. The following hold:*
i) If M is a left H-module (with action denoted by hm for $h \in H, m \in M$), then M has a structure of a right H-module given by $m \cdot h = S(h)m$ for any $m \in M, h \in H$.
ii) If M is a right H-comodule (with structure map $\rho : M \to M \otimes H$, $\rho(m) = \sum m_{(0)} \otimes m_{(1)}$), then M has a left H-comodule structure with the morphism giving the structure $\rho' : M \to H \otimes M$, $\rho'(m) = \sum S(m_{(1)}) \otimes m_{(0)}$.

Proof: The checking is immediate, using the fact that S is an antimorphism of algebras, and an antimorphism of coalgebras. ∎

Example 4.2.15 *If H and L are two bialgebras, then it is easy to check that we have a bialgebra structure on $H \otimes L$ if we consider the tensor product of algebras and the tensor product of coalgebras structures. Moreover, if H and L are Hopf algebras with antipodes S_H and S_L, then $H \otimes L$ is a Hopf algebra with the antipode $S_H \otimes S_L$. This bialgebra (Hopf algebra) is called the tensor product of the two bialgebras (Hopf algebras).* ∎

Let H be a Hopf algebra and $G(H)$ the group of grouplike elements of H. If $g, h \in G(H)$, then an element $x \in H$ is called (g, h)-primitive if $\Delta(x) = x \otimes g + h \otimes x$. The set of all (g, h)-primitive elements of H is denoted by $P_{g,h}(H)$. A $(1,1)$-primitive is simply called a primitive element. We denote $P(H) = P_{1,1}(H)$.

Exercise 4.2.16 *Let H be a finite dimensional Hopf algebra over a field k of characteristic zero. Show that if $x \in H$ is a primitive element, i.e. $\Delta(x) = x \otimes 1 + 1 \otimes x$, then $x = 0$.*

Exercise 4.2.17 *Let H be a Hopf algebra over the field k and let K be a field extension of k. Show that one can define on $\overline{H} = K \otimes_k H$ a natural structure of a Hopf algebra by taking the extension of scalars algebra structure and the coalgebra structure as in Proposition 1.4.25. Moreover, if $\overline{S}$ is the antipode of $\overline{H}$, then for any positive integer n we have that $S^n = Id$ if and only if $\overline{S}^n = Id$.*

4.3 Examples of Hopf algebras

In this section we give some relevant examples of Hopf algebras.

1) The group algebra. Let G be a (multiplicative) group, and kG the associated group algebra. This is a k-vector space with basis $\{g \mid g \in G\}$, so its elements are of the form $\sum_{g \in G} \alpha_g g$ with $(\alpha_g)_{g \in G}$ a family of elements from k having only a finite number of non-zero elements. The multiplication is defined by the relation

$$(\alpha g)(\beta h) = (\alpha\beta)(gh)$$

for any $\alpha, \beta \in k, g, h \in G$, and extended by linearity.
On the group algebra kG we also have a coalgebra structure as in Example 1.1.4 1), in which $\Delta(g) = g \otimes g$ and $\varepsilon(g) = 1$ for any $g \in G$. We already know that the group algebra becomes in this way a bialgebra. We note that until now we only used the fact that G is a monoid. The existence of the antipode is directly related to the fact that the elements of G are invertible.

Indeed, the map $S : kG \to kG$, defined by $S(g) = g^{-1}$ for any $g \in G$, and then extended linearly, is an antipode of the bialgebra kG, since

$$\sum S(g_1)g_2 = S(g)g = g^{-1}g = 1 = \varepsilon(g)1$$

and similarly, $\sum g_1 S(g_2) = \varepsilon(g)1$ for any $g \in G$.
It is clear that if G is a monoid which is not a group, then the bialgebra kG is not a Hopf algebra.
If G is a finite group, then Proposition 4.2.11 shows that on $(kG)^*$ we also have a Hopf algebra structure, which is dual to the one on kG. We recall that the algebra $(kG)^*$ has a complete system of orthogonal idempotents $(p_g)_{g\in G}$, where $p_g \in (kG)^*$ is defined by $p_g(h) = \delta_{g,h}$ for any $g, h \in G$. Therefore,

$$p_g^2 = p_g,\ p_g p_h = 0 \text{ for } g \neq h,\ \sum_{g\in G} p_g = 1_{(kG)^*}$$

The coalgebra structure of $(kG)^*$ can be described using Remark 1.3.10, and is given by

$$\Delta(p_g) = \sum_{x\in G} p_x \otimes p_{x^{-1}g},\ \varepsilon(p_g) = \delta_{1,g}$$

The antipode of $(kG)^*$ is defined by $S(p_g) = p_{g^{-1}}$ for any $g \in G$.

2) The tensor algebra. We recall first the categorical definition of the tensor algebra, since it will help us construct some maps enriching its structure.

Definition 4.3.1 *Let M be a k-vector space. A* tensor algebra *of M is a pair (X, i), where X is a k-algebra, and $i : M \to X$ is a morphism of k-vector spaces such that the following universal property is satisfied: for any k-algebra A, and any k-linear map $f : M \to A$, there exists a unique morphism of algebras $\overline{f} : X \to A$ such that $\overline{f}i = f$, i.e. the following diagram is commutative.*

$$\begin{tikzcd} M \arrow[rr, "i"] \arrow[dr, "f"'] & & X \arrow[dl, "\overline{f}"] \\ & A & \end{tikzcd}$$

∎

The tensor algebra of a vector space exists and is unique up to isomorphism. We briefly present its construction. Denote by $T^0(M) = k$, $T^1(M) = M$, and for $n \geq 2$ by $T^n(M) = M \otimes M \otimes \ldots \otimes M$, the tensor product of n copies of the vector space M. Now denote by $T(M) = \oplus_{n \geq 0} T^n(M)$, and $i : M \to T(M)$, defined by $i(m) = m \in T^1(M)$ for any $m \in M$. On $T(M)$ we define a multiplication as follows: if $x = m_1 \otimes \ldots \otimes m_n \in T^n(M)$, and $y = h_1 \otimes \ldots \otimes h_r \in T^r(M)$, then define the product of the elements x and y by

$$x \cdot y = m_1 \otimes \ldots \otimes m_n \otimes h_1 \otimes \ldots \otimes h_r \in T^{n+r}(M).$$

The multiplication of two arbitrary elements from $T(M)$ is obtained by extending the above formula by linearity. In this way, $T(M)$ becomes an algebra, with identity element $1 \in T^0(M)$, and the pair $(T(M), i)$ is a tensor algebra of M.

Remark 4.3.2 *The existence of the tensor algebra shows that the forgetful functor $U : k-Alg \to {}_k\mathcal{M}$ has a left adjoint, namely the functor associating to a k-vector space its tensor algebra.* ∎

We define now a coalgebra structure on $T(M)$. To avoid any possible confusion we introduce the following notation: if α and β are tensor monomials from $T(M)$ (i.e. each of them lies in a component $T^n(M)$), then the tensor monomial $T(M) \otimes T(M)$ having α on the first tensor position, and β on the second tensor position will be denoted by $\alpha \overline{\otimes} \beta$. Without this notation, for example for $\alpha = m \otimes m \in T^2(M)$ and $\beta = m \in T^1(M)$, the elements $\alpha \otimes \beta$ and $\beta \otimes \alpha$ from $T(M) \otimes T(M)$ would be both written as $m \otimes m \otimes m$, causing confusion. In our notation, $\alpha \otimes \beta = m \otimes m \overline{\otimes} m$, and $\beta \otimes \alpha = m \overline{\otimes} m \otimes m$.

Consider the linear map $f : M \to T(M) \otimes T(M)$ defined by $f(m) = m \overline{\otimes} 1 + 1 \overline{\otimes} m$ for any $m \in M$. Applying the universal property of the tensor algebra, it follows that there exists a morphism of algebras $\Delta : T(M) \to T(M) \otimes T(M)$ for which $\Delta i = f$. Let us show that Δ is coassociative, i.e. $(\Delta \otimes I)\Delta = (I \otimes \Delta)\Delta$. Since both sides of the equality we want to prove are morphisms of algebras, it is enough to check the equality on a system of generators (as an algebra) of $T(M)$, thus on $i(M)$. Indeed, if $m \in M$, then

$$\begin{aligned}(\Delta \otimes I)\Delta(m) &= (\Delta \otimes I)(m \overline{\otimes} 1 + 1 \overline{\otimes} m)\\ &= m \overline{\otimes} 1 \overline{\otimes} 1 + 1 \overline{\otimes} m \overline{\otimes} 1 + 1 \overline{\otimes} 1 \overline{\otimes} m\end{aligned}$$

and

$$\begin{aligned}(I \otimes \Delta)\Delta(m) &= (I \otimes \Delta)(m \overline{\otimes} 1 + 1 \overline{\otimes} m)\\ &= m \overline{\otimes} 1 \overline{\otimes} 1 + 1 \overline{\otimes} m \overline{\otimes} 1 + 1 \overline{\otimes} 1 \overline{\otimes} m\end{aligned}$$

which shows that Δ is coassociative.
We now define the counit, using the universal property of the tensor algebra for the null morphism $0 : M \to k$. We obtain a morphism of algebras $\varepsilon : T(M) \to k$ with the property that $\varepsilon(m) = 0$ for any $m \in i(M)$. To show that $(\varepsilon \otimes I)\Delta = \phi$, where $\phi : T(M) \to k \otimes T(M)$, $\phi(z) = 1 \otimes z$ is the canonical isomorphism, it is enough to check the equality on $i(M)$, and here it is clear that

$$(\varepsilon \otimes I)\Delta(m) = \varepsilon(m) \otimes 1 + \varepsilon(1) \otimes m = 1 \otimes m = \phi(m).$$

Similarly, one can show that $(I \otimes \varepsilon)\Delta = \phi'$, where $\phi' : T(M) \to T(M) \otimes k$ is the canonical isomorphism.
So far, we know that $T(M)$ is a bialgebra. We construct an antipode. Consider the opposite algebra $T(M)^{op}$ of $T(M)$, and let $g : M \to T(M)^{op}$ be the linear map defined by $g(m) = -m$ for any $m \in M$. The universal property of the tensor algebra shows that there exists a morphism of algebras $S : T(M) \to T(M)^{op}$ such that $S(m) = -m$ for any $m \in i(M)$. For an arbitrary element $m_1 \otimes \ldots \otimes m_n \in T^n(M)$ we have $S(m_1 \otimes \ldots \otimes m_n) = (-1)^n m_n \otimes \ldots \otimes m_1$. We regard now $S : T(M) \to T(M)$ as an antimorphism of algebras. We show that for any $m \in T^1(M)$ we have

$$\sum S(m_1)m_2 = \sum m_1 S(m_2) = \varepsilon(m)1$$

Indeed, since $\Delta(m) = m\overline{\otimes}1 + 1\overline{\otimes}m$ we have

$$\sum S(m_1)m_2 = S(m)1 + S(1)m = -m + m = 0,$$

and similarly the other equality. Therefore, the property the antipode should satisfy is checked for S on a system of (algebra) generators of $T(M)$. The fact that S verifies the property for any element in $T(M)$ will follow from the next lemma.

Lemma 4.3.3 *Let H be a bialgebra, and $S : H \to H$ an antimorphism of algebras. If for $a, b \in H$ we have $(S * I)(a) = (I * S)(a) = u\varepsilon(a)$ and $(S * I)(b) = (I * S)(b) = u\varepsilon(b)$, then also $(S * I)(ab) = (I * S)(ab) = u\varepsilon(ab)$.*

Proof: We know that

$$\sum S(a_1)a_2 = \sum a_1 S(a_2) = \varepsilon(a)1$$

and

$$\sum S(b_1)b_2 = \sum b_1 S(b_2) = \varepsilon(b)1.$$

Then

$$
\begin{aligned}
(S*I)(ab) &= \sum S((ab)_1)(ab)_2 \\
&= \sum S(a_1b_1)a_2b_2 \\
&= \sum S(b_1)S(a_1)a_2b_2 \quad (S \text{ is an antimorphism of algebras}) \\
&= \sum \varepsilon(a)S(b_1)b_2 \quad (\text{ from the property of } a) \\
&= \sum \varepsilon(a)\varepsilon(b)1 \quad (\text{ from the property of } b) \\
&= u\varepsilon(ab)
\end{aligned}
$$

∎

Similarly, one can prove the second equality, and therefore we know now that $T(M)$ is a Hopf algebra with antipode S. We show that $T(M)$ is cocommutative, i.e. $\tau\Delta = \Delta$, where $\tau : T(M)\otimes T(M) \to T(M)\otimes T(M)$ is defined by $\tau(z\otimes v) = v\otimes z$ for any $z, v \in T(M)$. Indeed, it is enough to check this on a system of algebra generators of $T(M)$, hence on $i(M)$ (because $\tau\Delta$ and Δ are both morphisms of algebras), but on $i(M)$ the equality is clear.

3) The symmetric algebra. We recall the definition of the symmetric algebra of a vector space.

Definition 4.3.4 *Let M be a k-vector space. A* symmetric algebra *of M is a pair (X, i), where X is a commutative k-algebra, and $i : M \to X$ is a k-linear map such that the following universal property holds: for any commutative k-algebra A, and any k-linear map $f : M \to A$, there exists a unique morphism of algebras $\overline{f} : X \to A$ such that $\overline{f}i = f$, i.e. the following diagram is commutative.*

$$
\begin{tikzcd}
M \arrow[rr, "i"] \arrow[dr, "f"'] & & X \arrow[dl, "\overline{f}"] \\
& A &
\end{tikzcd}
$$

∎

The symmetric algebra of a k-vector space M exists and is unique up to isomorphism. It is constructed as follows: consider the ideal I of the tensor algebra $T(M)$ generated by all elements of the form $x\otimes y - y\otimes x$

with $x, y \in M$. Then $S(M) = T(M)/I$, together with the map pi, where $i : M \to T(M)$ is the canonical inclusion, and $p : T(M) \to T(M)/I$ is the canonical projection, is a symmetric algebra of M.

Remark 4.3.5 *The existence of the symmetric algebra shows that the forgetful functor from the category of commutative k-algebras to the category of k-vector spaces has a left adjoint.* ∎

We show that the symmetric algebra M has a Hopf algebra structure. By Proposition 4.2.13, this will follow if we show that I is a Hopf ideal of the Hopf algebra $T(M)$. Since Δ and ε are morphisms of algebras, and S is an antimorphism of algebras, it is enough to show that

$$\Delta(x \otimes y - y \otimes x) \in I \otimes T(M) + T(M) \otimes I$$

$$\varepsilon(x \otimes y - y \otimes x) = 0 \text{ and } S(x \otimes y - y \otimes x) \in I$$

for any $x, y \in M$. Indeed,

$$\begin{aligned} & \Delta(x \otimes y - y \otimes x) \\ = \; & \Delta(x)\Delta(y) - \Delta(y)\Delta(x) \\ = \; & (x\overline{\otimes}1 + 1\overline{\otimes}x)(y\overline{\otimes}1 + 1\overline{\otimes}y) - (y\overline{\otimes}1 + 1\overline{\otimes}y)(x\overline{\otimes}1 + 1\overline{\otimes}x) \\ = \; & (x \otimes y - y \otimes x)\overline{\otimes}1 + 1\overline{\otimes}(x \otimes y - y \otimes x) \end{aligned}$$

and this is clearly an element of $I \otimes T(M) + T(M) \otimes I$. Moreover,

$$\varepsilon(x \otimes y - y \otimes x) = \varepsilon(x)\varepsilon(y) - \varepsilon(y)\varepsilon(x) = 0$$

and

$$\begin{aligned} S(x \otimes y - y \otimes x) &= S(y)S(x) - S(x)S(y) = \\ &= (-y) \otimes (-x) - (-x) \otimes (-y) \in I. \end{aligned}$$

We obtained that $S(M)$ has a Hopf algebra structure, it is a factor Hopf algebra of $T(M)$ modulo the Hopf ideal I. It is clear that $S(M)$ is a commutative Hopf algebra, and also cocommutative, since it is a factor of a cocommutative Hopf algebra.

4) The enveloping algebra of a Lie algebra. Let L be a Lie k-algebra, with bracket $[\ ,\ ]$. The enveloping algebra of the Lie algebra L is the factor algebra $U(L) = T(L)/I$, where $T(L)$ is the tensor algebra of the k-vector space L, and I is the ideal of $T(L)$ generated by the elements of the form $[x, y] - x \otimes y + y \otimes x$ with $x, y \in L$. A computation similar to the one performed for the symmetric algebra shows that

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

$$= ([x,y] - x \otimes y + y \otimes x)\overline{\otimes}1 + 1\overline{\otimes}([x,y] - x \otimes y + y \otimes x)$$

which is in $I \otimes T(M) + T(M) \otimes I$,

$$\varepsilon([x,y] - x \otimes y + y \otimes x) = 0$$

and

$$S([x,y] - x \otimes y + y \otimes x) = -([x,y] - x \otimes y + y \otimes x) \in I,$$

so I is a Hopf ideal in $T(L)$. It follows that $U(L)$ has a Hopf algebra structure, the factor Hopf algebra of $T(L)$ modulo the Hopf ideal I. Since $T(L)$ is cocommutative, $U(L)$ is also cocommutative.

5) Divided power Hopf algebras Let H be a k-vector space with basis $\{c_i | i \in \mathbf{N}\}$ on which we consider the coalgebra structure defined in Example 1.1.4 2). Hence

$$\Delta(c_m) = \sum_{i=0}^{m} c_i \otimes c_{m-i}, \quad \varepsilon(c_m) = \delta_{0,m}$$

for any $m \in \mathbf{N}$. We define on H an algebra structure as follows. We put

$$c_n c_m = \binom{n+m}{n} c_{n+m}$$

for any $n, m \in \mathbf{N}$, and then extend it by linearity on H. We note first that c_0 is the identity element, so we will write $c_0 = 1$. In order to show that the multiplication is associative it is enough to check that $(c_n c_m)c_p = c_n(c_m c_p)$ for any $m, n, p \in \mathbf{N}$. This is true because

$$\begin{aligned}
(c_n c_m)c_p &= \binom{n+m}{n} c_{n+m} c_p \\
&= \binom{n+m}{n}\binom{n+m+p}{n+m} c_{n+m+p} \\
&= \frac{(n+m+p)!}{n!m!p!} c_{n+m+p} \\
&= \binom{n+m+p}{n}\binom{m+p}{m} c_{n+m+p} \\
&= \binom{m+p}{m} c_n c_{m+p} \\
&= c_n(c_m c_p)
\end{aligned}$$

We show now that H is a bialgebra with the above coalgebra and algebra structures. Since the counit is obviously an algebra map, it is enough to show that $\Delta(c_n c_m) = \Delta(c_n)\Delta(c_m)$ for any $n, m \in \mathbf{N}$. We have

$$\begin{aligned}
\Delta(c_n)\Delta(c_m) &= (\sum_{t=0}^{n} c_t \otimes c_{n-t})(\sum_{j=0}^{m} c_j \otimes c_{m-j}) \\
&= \sum_{t=0}^{n}\sum_{j=0}^{m} \binom{t+j}{t}\binom{n+m-t-j}{n-t} c_{t+j} \otimes c_{n+m-t-j} \\
&= \sum_{i=0}^{n+m}\sum_{t=0}^{i} \binom{i}{t}\binom{n+m-i}{n-t} c_i \otimes c_{n+m-i} \\
&= \sum_{i=0}^{n+m} \binom{n+m}{n} c_i \otimes c_{n+m-i} \\
&= \Delta(\binom{n+m}{n} c_{n+m}) \\
&= \Delta(c_n c_m)
\end{aligned}$$

It remains to prove that the bialgebra H has an antipode. Since H is cocommutative, it suffices to show that there exists a linear map $S : H \to H$ such that $\sum S(h_1)h_2 = \varepsilon(h)1$ for any h in a basis of H. We define $S(c_n)$ recurrently. For $n = 0$ we take $S(c_0) = S(1) = 1$. We assume that $S(c_0), \ldots, S(c_{n-1})$ were defined such that the property of the antipode checks for $h = c_i$ with $0 \leq i \leq n-1$. Then we define

$$S(c_n) = -S(c_0)c_n - S(c_1)c_{n-1} - \ldots - S(c_{n-1})c_1,$$

and it is clear that the property of the antipode is then verified for $h = c_n$ too. In conclusion, H is a Hopf algebra, which is clearly commutative and cocommutative.

6. Sweedler's 4-dimensional Hopf algebra.

Assume that $char(k) \neq 2$. Let H be the algebra given by generators and relations as follows: H is generated as a k-algebra by c and x satisfying the relations

$$c^2 = 1,\ x^2 = 0,\ xc = -cx$$

Then H has dimension 4 as a k-vector space, with basis $\{ 1, c, x, cx \}$. The coalgebra structure is induced by

$$\Delta(c) = c \otimes c,\ \Delta(x) = c \otimes x + x \otimes 1$$

$$\varepsilon(c) = 1, \ \varepsilon(x) = 0$$

In this way, H becomes a bialgebra, which also has an antipode S given by $S(c) = c^{-1}, S(x) = -cx$.
This was the first example of a non-commutative and non-cocommutative Hopf algebra.

7. The Taft algebras.

Let $n \geq 2$ be an integer, and λ a primitive n-th root of unity. Consider the algebra $H_{n^2}(\lambda)$ defined by the generators c and x with the relations

$$c^n = 1, \ x^n = 0, \ xc = \lambda cx$$

On this algebra we can introduce a coalgebra structure induced by

$$\Delta(c) = c \otimes c, \ \Delta(x) = c \otimes x + x \otimes 1$$

$$\varepsilon(c) = 1, \ \varepsilon(x) = 0.$$

In this way, $H_{n^2}(\lambda)$ becomes a bialgebra of dimension n^2, having the basis $\{ \ c^i x^j \mid 0 \leq i, j \leq n-1 \ \}$. The antipode is defined by $S(c) = c^{-1}$ and $S(x) = -c^{-1}x$. We note that for $n = 2$ and $\lambda = -1$ we obtain Sweedler's 4-dimensional Hopf algebra.

8. On the polynomial algebra $k[X]$ we introduce a coalgebra structure as follows: using the universal property of the polynomial algebra we find a unique morphism of algebras $\Delta : k[X] \rightarrow k[X] \otimes k[X]$ for which $\Delta(X) = X \otimes 1 + 1 \otimes X$. It is clear that

$$(\Delta \otimes I)\Delta(X) = (I \otimes \Delta)\Delta(X) =$$

$$= X \otimes 1 \otimes 1 + 1 \otimes X \otimes 1 + 1 \otimes 1 \otimes X,$$

and then again using the universal property of the polynomial algebra it follows that Δ is coassociative. Similarly, there is a unique morphism of algebras $\varepsilon : k[X] \rightarrow k$ with $\varepsilon(X) = 0$. It is clear that together with Δ and ε, the algebra $k[X]$ becomes a bialgebra. This is even a Hopf algebra, with antipode $S : k[X] \rightarrow k[X]$ constructed again by the universal property of the polynomial algebra, such that $S(X) = -X$. This Hopf algebra is in fact isomorphic to the tensor (or symmetric, or universal enveloping) algebra of a one dimensional vector space (or Lie algebra).

We take this opportunity to justify the use of the name *convolution*. The polynomial ring $\mathbf{R}[X]$ is a coalgebra as above, and hence its dual,

$U = \mathbf{R}[X]^* = Hom(\mathbf{R}[X], \mathbf{R})$ is an algebra with the convolution product. If f is a continuous function with compact support, then $f^* \in U$, where f^* is given by

$$f^*(P) = \int f(x)\tilde{P}(x)dx,$$

and $\tilde{P}$ is the polynomial function associated to $P \in \mathbf{R}[X]$. We have that $\Delta(P) \in \mathbf{R}[X] \otimes \mathbf{R}[X] \simeq \mathbf{R}[X, Y]$,

$$\Delta(P) = \sum P_1 \otimes P_2 = P(X + Y).$$

If g is another continuous function with compact support, the convolution product of f^* and g^* is given by

$$\begin{aligned}
(f^* * g^*)(P) &= \sum \int f(x)\tilde{P}_1(x)dx \int g(y)\tilde{P}_2(y)dy \\
&= \sum \int (\int f(x)\tilde{P}_1(x)dx) g(y)\tilde{P}_2(y)dy \\
&= \int (\int f(x)g(y)dx)\tilde{P}(x + y)dy \\
&= \int (\int f(x)g(t - x)dx)\tilde{P}(t)dt = h^*(P),
\end{aligned}$$

where $h(t) = \int f(x)g(t - x)dx$ is what is usually called the convolution product (see [199]).

9. Let k be a field of characteristic $p > 0$. On the polynomial algebra $k[X]$ we consider the Hopf algebra structure described in example 8, in which $\Delta(X) = X \otimes 1 + 1 \otimes X$, $\varepsilon(X) = 0$ and $S(X) = -X$. Since $\Delta(X^p) = X^p \otimes 1 + 1 \otimes X^p$ (we are in characteristic p, and all the binomial coefficients $\binom{p}{i}$ with $1 \le i \le p-1$ are divisible by p, hence zero), $\varepsilon(X^p) = 0$ and $S(X^p) = -X^p$ (remark: if $p = 2$, then $1 = -1$), it follows that the ideal generated by X^p is a Hopf ideal, and it makes sense to construct the factor Hopf algebra $H = k[X]/(X^p)$. This has dimension p, and denoting by x the coset of X, we have $\Delta(x) = x \otimes 1 + 1 \otimes x$ and $x^p = 0$. This is the restricted enveloping algebra of the 1-dimensional p-Lie algebra.

10. The cocommutative cofree coalgebra over a vector space.

Let V be a vector space, and (C, π) a cocommutative cofree coalgebra over V. We show that C has a natural structure of a Hopf algebra. Let $p : C \otimes C \to V \oplus V$ be the map defined by $p(c \otimes d) = (\pi(c)\varepsilon(d), \pi(d)\varepsilon(c))$ for any $c, d \in C$. Proposition 1.6.14 shows that $(C \otimes C, p)$ is a cocommutative cofree coalgebra over $V \oplus V$. The same result shows that if we denote by $\gamma : (C \otimes C) \otimes C \rightarrow (V \oplus V) \oplus V$ the map defined by

$$\gamma(c \otimes d \otimes e) = (p(c \otimes d)\varepsilon(e), \pi(e)\varepsilon(c \otimes d)) =$$

$$= (\pi(c)\varepsilon(d)\varepsilon(e), \pi(d)\varepsilon(c)\varepsilon(e), \pi(e)\varepsilon(c)\varepsilon(d))$$

we have that $(C \otimes C \otimes C, \gamma)$ is a cocommutative cofree coalgebra over $V \oplus V \oplus V$.

Let $m : V \oplus V \rightarrow V$ be the map defined by $m(x, y) = x + y$. Then the linear map $m : V \oplus V \rightarrow V$ induces a morphism of coalgebras $M : C \otimes C \rightarrow C$ between the cocommutative cofree coalgebra over these spaces. Also the linear map $m \oplus I : V \oplus V \oplus V \rightarrow V \oplus V$ induces the morphism $M \otimes I : C \otimes C \otimes C \rightarrow C \otimes C$ of coalgebras between the cocommutative cofree coalgebras over the two spaces (this follows from the relation $p(M \otimes I) = (m \oplus I)\gamma$, which checks immediately). By composition it follows that $M(M \otimes I) : C \otimes C \otimes C \rightarrow C$ is the morphism of coalgebras associated to the linear map $m(m \oplus I) : V \oplus V \oplus V \rightarrow V$ (using the universal property of the cocommutative cofree coalgebra).

Consider now the map $\gamma' : C \otimes C \otimes C \rightarrow V \oplus V \oplus V$ as in Proposition 1.6.14, for which $(C \otimes (C \otimes C), \gamma')$ is a cocommutative cofree coalgebra over $V \oplus (V \oplus V)$. Similar to the above procedure, one can show that $M(I \otimes M)$ is the morphism of coalgebras associated to the linear map $m(I \oplus m)$. But it is easy to see that $\gamma = \gamma'$, and that $m(I \oplus m) = m(m \oplus I)$, hence $M(M \otimes I) = M(I \otimes M)$, i.e. M is associative.

Using Proposition 1.6.13, the zero morphism between the null space and V induces a morphism of coalgebras $u : k \rightarrow C$. Also the linear map $s : V \rightarrow V, s(x) = -x$, induces a map $S : C \rightarrow C$, using again the universal property. As in the verification of the associativity of M, one can check that u is a unit for C, which thus becomes a bialgebra, and that S is an antipode for this bialgebra.

In conclusion, the cocommutative cofree coalgebra over V has a Hopf algebra structure.

Exercise 4.3.6 *(i) Let k be a field which contains a primitive n-th root of 1 (in particular this requires that the characteristic of k does not divide n) and let C_n be the cyclic group of order n. Show that the Hopf algebra kC_n is selfdual, i.e. the dual Hopf algebra $(kC_n)^*$ is isomorphic to kC_n.*

(ii) Show that for any finite abelian group C of order n and any field k which contains a primitive n-th root of order n, the Hopf algebra kC is selfdual.

Exercise 4.3.7 *Let k be a field. Show that*
(i) If $char(k) \neq 2$, then any Hopf algebra of dimension 2 is isomorphic to kC_2, the group algebra of the cyclic group with two elements.
(ii) If $char(k) = 2$, then there exist precisely three isomorphism types of Hopf algebras of dimension 2 over k, and these are kC_2, $(kC_2)^*$, and a certain selfdual Hopf algebra.

Exercise 4.3.8 *Let H be a Hopf algebra over the field k, such that there exists an algebra isomorphism $H \simeq k \times k \times \ldots \times k$ (k appears n times). Then H is isomorphic to $(kG)^*$, the dual of a group algebra of a group G with n elements.*

Two more examples of Hopf algebras, the finite dual of a Hopf algebra, and the representative Hopf algebra of a group, are treated in the next exercises.

Exercise 4.3.9 *Let H be a bialgebra. Then the finite dual coalgebra H° is a subalgebra of the dual algebra H^*, and together with this algebra structure it is a bialgebra. Moreover, if H is a Hopf algebra, then H° is a Hopf algebra.*

Exercise 4.3.10 *Let G be a monoid. Then the representative coalgebra $R_k(G)$ is a subalgebra of k^G, and even a bialgebra. If G is a group, then $R_k(G)$ is a Hopf algebra. If G is a topological group, then*

$$\tilde{R}_{\mathbf{R}}(G) = \{f \in R_{\mathbf{R}}(G) \mid f \ continuous\}$$

is a Hopf subalgebra of $R_{\mathbf{R}}(G)$.

4.4 Hopf modules

Throughout this section H will be a Hopf algebra.

Definition 4.4.1 *A k-vector space M is called a right H-*Hopf module *if H has a right H-module structure (the action of an element $h \in H$ on an element $m \in M$ will be denoted by mh), and a right H-comodule structure, given by the map $\rho : M \to M \otimes H$, $\rho(m) = \sum m_{(0)} \otimes m_{(1)}$, such that for any $m \in M$, $h \in H$*

$$\rho(mh) = \sum m_{(0)}h_1 \otimes m_{(1)}h_2.$$

∎

Remark 4.4.2 *It is easy to check that $M \otimes H$ has a right module structure over $H \otimes H$ (with the tensor product of algebras structure) defined by $(m \otimes h)(g \otimes p) = mg \otimes hp$ for any $m \otimes h \in M \otimes H$, $g \otimes p \in H \otimes H$. Considering then the morphism of algebras $\Delta : H \to H \otimes H$, we obtain that $M \otimes H$ becomes a right H-module by restriction of scalars via Δ. This structure is given by $(m \otimes h)g = \sum mg_1 \otimes hg_2$ for any $m \otimes h \in M \otimes H$, $g \in H$. With this structure in hand, we remark that the compatibility relation from the preceding definition means that ρ is a morphism of right H-modules.*
There is a dual interpretation of this relation. Consider $H \otimes H$ with the tensor product of coalgebras structure. Then $M \otimes H$ has a natural structure of a right comodule over $H \otimes H$, defined by $m \otimes h \mapsto \sum m_{(0)} \otimes h_1 \otimes m_{(1)} \otimes h_2$. The multipliction $\mu : H \otimes H \to H$ of the algebra H is a morphism of coalgebras, and then by corestriction of scalars $M \otimes H$ becomes a right H-comodule, with $m \otimes h \mapsto \sum m_{(0)} \otimes h_1 \otimes m_{(1)}h_2$. Then the compatibility relation from the preceding definition may be expressed by the fact that the map $\phi : M \otimes H \to H$, giving the right H-module structure of M, is a morphism of H-comodules. ∎

We can define a category having as objects the right H-Hopf modules, and as morphisms between two such objects all linear maps which are also morphisms of right H-modules and morphisms of right H-comodules. This category is denoted by $\mathcal{M}_H^H$, and will be called the category of right H-Hopf modules. It is clear that in this category a morphism is an isomorphism if and only if it is bijective.

Example 4.4.3 *Let V be a k-vector space. Then we define on $V \otimes H$ a right H-module structure by $(v \otimes h)g = v \otimes hg$ for any $v \in V$, $h, g \in H$, and a right H-comodule structure given by the map $\rho : V \otimes H \to V \otimes H \otimes H$, $\rho(v \otimes h) = \sum v \otimes h_1 \otimes h_2$ for any $v \in V, h \in H$. Then $V \otimes H$ becomes a right H-Hopf module with these two structures. Indeed*

$$\begin{aligned}
\rho((v \otimes h)g) &= \rho(v \otimes hg) \\
&= \sum v \otimes (hg)_1 \otimes (hg)_2 \\
&= \sum v \otimes h_1 g_1 \otimes h_2 g_2 \\
&= \sum ((v \otimes h_1) g_1) \otimes h_2 g_2 \\
&= \sum (v \otimes h)_{(0)} g_1 \otimes (v \otimes h)_{(1)} g_2
\end{aligned}$$

proving the compatibility relation. ∎

We will show that the examples of H-Hopf modules from the preceding example are (up to isomorphism) all H-Hopf modules. We need first a definition.

Definition 4.4.4 *Let M be a right H-comodule, with comodule structure given by the map $\rho : M \to M \otimes H$. The set*

$$M^{coH} = \{m \in M \mid \rho(m) = m \otimes 1\}$$

is a vector subspace of M which is called the subspace of coinvariants *of M.* ∎

Example 4.4.5 *Let H be given the right H-comodule structure induced by $\Delta : H \to H \otimes H$. Then $H^{coH} = k1$ (where 1 is the identity element of H). Indeed, if $h \in H^{coH}$, then $\Delta(h) = \sum h_1 \otimes h_2 = h \otimes 1$. Applying ε on the first position we obtain $h = \varepsilon(h)1 \in k1$. Conversely, if $h = \alpha 1$ for a scalar α, then $\Delta(h) = \alpha 1 \otimes 1 = h \otimes 1$.* ∎

Theorem 4.4.6 *(The fundamental theorem of Hopf modules) Let H be a Hopf algebra, and M a right H-Hopf module. Then the map $f : M^{coH} \otimes H \to M$, defined by $f(m \otimes h) = mh$ for any $m \in M^{coH}$ and $h \in H$, is an isomorphism of Hopf modules (on $M^{coH} \otimes H$ we consider the H-Hopf module structure defined as in Example 4.4.3 for the vector space M^{coH}).*

Proof: We denote the map giving the comodule structure of M by $\rho : M \to M \otimes H$, $\rho(m) = \sum m_{(0)} \otimes m_{(1)}$. Consider the map $g : M \to M$, defined by $g(m) = \sum m_{(0)} S(m_{(1)})$ for any $m \in M$. If $m \in M$, we have

$$\begin{aligned}
\rho(g(m)) &= \rho(\sum m_{(0)} S(m_{(1)})) \\
&= \sum (m_{(0)})_{(0)} (S(m_{(1)}))_1 \otimes (m_{(0)})_{(1)} (S(m_{(1)}))_2 \\
&\qquad \text{(definition of Hopf modules)} \\
&= \sum (m_{(0)})_{(0)} S((m_{(1)})_2) \otimes (m_{(0)})_{(1)} S((m_{(1)})_1) \\
&\qquad \text{(the antipode is an antimorphism of coalgebras)} \\
&= \sum m_{(0)} S(m_{(3)}) \otimes m_{(1)} S(m_{(2)}) \\
&\qquad \text{(using the sigma notation for comodules)} \\
&= \sum m_{(0)} S(m_{(2)}) \otimes (m_{(1)})_1 S((m_{(1)})_2) \\
&\qquad \text{(using the sigma notation for comodules)} \\
&= \sum m_{(0)} S(m_{(2)}) \otimes \varepsilon(m_{(1)}) 1 \quad \text{(definition of the antipode)} \\
&= \sum m_{(0)} S(m_{(2)} \varepsilon(m_{(1)})) \otimes 1 \\
&= \sum m_{(0)} S((m_{(1)})_2 \varepsilon((m_{(1)})_1)) \otimes 1 \\
&\qquad \text{(using the sigma notation for comodules)}
\end{aligned}$$

$$\begin{aligned}
&= \sum m_{(0)}S(m_{(1)}) \otimes 1 \quad \text{(the counit property)} \\
&= g(m) \otimes 1,
\end{aligned}$$

which shows that $g(m) \in M^{coH}$ for any $m \in M$.
It makes then sense to define the map $F : M \to M^{coH} \otimes H$ by $F(m) = \sum g(m_{(0)}) \otimes m_{(1)}$ for any $m \in M$. We will show that F is the inverse of f. Indeed, if $m \in M^{coH}$ and $h \in H$ we have

$$\begin{aligned}
Ff(m \otimes h) &= F(mh) \\
&= \sum g((mh)_{(0)}) \otimes (mh)_{(1)} \\
&= \sum g(m_{(0)}h_1) \otimes m_{(1)}h_2 \\
&\quad \text{(definition of Hopf modules)} \\
&= \sum g(mh_1) \otimes h_2 \quad (\text{since } m \in M^{coH}) \\
&= \sum (mh_1)_{(0)}S((mh_1)_{(1)}) \otimes h_2 \\
&= \sum m_{(0)}(h_1)_1 S(m_{(1)}(h_1)_2) \otimes h_2 \\
&\quad \text{(definition of Hopf modules)} \\
&= \sum m(h_1)_1 S((h_1)_2) \otimes h_2 \quad (\text{since } m \in M^{coH}) \\
&= \sum m\varepsilon(h_1) \otimes h_2 \quad \text{(by the antipode property)} \\
&= m \otimes h \quad \text{(by the counit property)}
\end{aligned}$$

hence $Ff = Id$. Conversely, if $m \in M$, then

$$\begin{aligned}
fF(m) &= f(\sum m_{(0)}S(m_{(1)}) \otimes m_{(2)}) \\
&= \sum m_{(0)}S(m_{(1)})m_{(2)} \\
&= \sum m_{(0)}S((m_{(1)})_1)(m_{(1)})_2 \\
&\quad \text{(using the sigma notation for comodules)} \\
&= \sum m_{(0)}\varepsilon(m_{(1)}) \quad \text{(by the antipode property)} \\
&= m \quad \text{(by the counit property)}
\end{aligned}$$

which shows that $fF = Id$ too. It remains to show that f is a morphism of H-Hopf modules, i.e. it is a morphism of right H-modules and a morphism of right H-comodules. The first assertion is clear, since

$$f((m \otimes h)h') = f(m \otimes hh') = mhh' = f(m \otimes h)h'.$$

In order to show that f is a morphism of right H-comodules, we have to prove that the diagram

$$
\begin{tikzcd}
M^{coH} \otimes H \arrow[r, "f"] \arrow[d, "I \otimes \Delta"'] & M \arrow[d, "\rho"] \\
M^{coH} \otimes H \otimes H \arrow[r, "f \otimes I"] & M \otimes H
\end{tikzcd}
$$

is commutative. This is immediate, since

$$
\begin{aligned}
(\rho f)(m \otimes h) &= \rho(mh) \\
&= \sum mh_1 \otimes h_2 \ \ (\text{since } m \in M^{coH}) \\
&= \sum (f \otimes I)(m \otimes h_1 \otimes h_2) \\
&= (f \otimes I)(I \otimes \Delta)(m \otimes h)
\end{aligned}
$$

which ends the proof. ∎

Exercise 4.4.7 *Let H be a Hopf algebra. Show that for any right (left) H-comodule M, the injective dimension of M in the category $\mathcal{M}^H$ is less than or equal the injective dimension of the trivial right H-comodule k. In particular, the global dimension of the category $\mathcal{M}^H$ is equal to the injective dimension of the trivial right H-comodule k.*

Exercise 4.4.8 *Let H be a Hopf algebra. Show that for any right (left) H-module M, the projective dimension of M in the category $\mathcal{M}_H$ is less than or equal the projective dimension of the trivial right H-module k (with action defined by $\alpha \leftarrow h = \varepsilon(h)\alpha$ for any $\alpha \in k$ and $h \in H$). In particular the global dimension of the category $\mathcal{M}_H$ is equal to the projective dimension of the right H-module k.*

4.5 Solutions to exercises

Exercise 4.1.9 *Let k be a field and $n \geq 2$ a positive integer. Show that there is no bialgebra structure on $M_n(k)$ such that the underlying algebra structure is the matrix algebra.*

Solution: The argument is similar to the one that was used in Example 1.4.17. Suppose there is a bialgebra structure on $M_n(k)$, then the counit $\varepsilon : M_n(k) \to k$ is an algebra morphism. Then the kernel of ε is a two-sided ideal of $M_n(k)$, so it is either 0 or the whole of $M_n(k)$. Since $\varepsilon(1) = 1$, we have $Ker(\varepsilon) = 0$ and we obtain a contradiction since $dim(M_n(k)) > dim(k)$.

Exercise 4.2.16 *Let H be a finite dimensional Hopf algebra over a field k of characteristic zero. Show that if $x \in H$ is a primitive element, i.e. $\Delta(x) = x \otimes 1 + 1 \otimes x$, then $x = 0$.*

Solution: If there were a non-zero primitive element x, we prove by induction that the $1, x, \ldots, x^n$ are linearly independent for any positive integer n, and this will provide a contradiction, due to the finite dimension of H. The claim is clear for $n = 1$, since $a1 + bx = 0$ implies by applying ε that $a = 0$, and then, since $x \neq 0$, that $b = 0$. Assume the assertion true for $n - 1$ (where $n \geq 2$), and let $\sum_{p=0,n} a_p x^p = 0$ for some scalars $a_0, \ldots, a_p$. Then by applying Δ we find that

$$\sum_{p=0,n} \sum_{i=0,p} a_p \binom{p}{i} x^i \otimes x^{p-i} = 0$$

Choose some $1 \leq i, j \leq n-1$ such that $i + j = n$, and let $h_i^*, h_j^* \in H^*$ such that $h_i^*(x^t) = \delta_{i,t}$ for any $0 \leq t \leq n-1$ and $h_j^*(x^t) = \delta_{j,t}$ for any $0 \leq t \leq n-1$ (this is possible since $1, x, \ldots, x^{n-1}$ are linearly independent). Then by applying $h_i^* \otimes h_j^*$ to the above relation we obtain that $a_n \binom{n}{i} = 0$, and since k has characteristic zero we have $a_n = 0$. Then again by the induction hypothesis we must have $a_0, \ldots, a_{n-1} = 0$.

Exercise 4.2.17 *Let H be a Hopf algebra over the field k and let K be a field extension of k. Show that one can define on $\overline{H} = K \otimes_k H$ a natural structure of a Hopf algebra by taking the extension of scalars algebra structure and the coalgebra structure as in Proposition 1.4.25. Moreover, if $\overline{S}$ is the antipode of $\overline{H}$, then for any positive integer n we have that $S^n = Id$ if and only if $\overline{S}^n = Id$.*

Solution: The comultiplication $\overline{\Delta}$ and counit $\overline{\varepsilon}$ of $\overline{H}$ are given by

$$\overline{\Delta}(\delta \otimes_k h) = \sum (\delta \otimes_k h_1) \otimes_K (1 \otimes_k h_2)$$

$$\overline{\varepsilon}(\delta \otimes_k h) = \delta \varepsilon(h)$$

for any $\delta \in K$ and $h \in H$. It is a straightforward check that $\overline{H}$ is a bialgebra over K, and moreover, the map $\overline{S} : \overline{H} \to \overline{H}$ defined by $\overline{S}(\delta \otimes_k h) = \delta \otimes_k S(h)$ is an antipode of $\overline{H}$. The last part is now obvious.

Exercise 4.3.6 *(i) Let k be a field which contains a primitive n-th root of 1 (in particular this requires that the characteristic of k does not divide n) and let C_n be the cyclic group of order n. Show that the Hopf algebra kC_n is selfdual, i.e. the dual Hopf algebra $(kC_n)^*$ is isomorphic to kC_n.*
(ii) Show that for any finite abelian group C of order n and any field k which contains a primitive n-th root of order n, the Hopf algebra kC is

selfdual.

Solution: (i) Let $C_n =< c >$ and let ξ be a primitive n-th root of 1 in k. Then kC_n has the basis $1, c, c^2, \dots, c^{n-1}$, and let $p_1, p_c, \dots, p_{c^{n-1}}$ be the dual basis in $(kC_n)^*$. We determine $G = G((kC_n)^*)$. We know that the elements of G are just the algebra morphisms from kC_n to k. If $f \in G$, then $f(c)^n = 1$, so $f(c) = \xi^i$ for some $0 \leq i \leq n-1$. Conversely, for any such i there exists a unique algebra morphism $f_i : kC_n \to k$ such that $f_i(c) = \xi^i$. More precisely, $f_i(c^j) = \xi^{ij}$ for any j (extended linearly). Thus $f_0, f_1, \dots, f_{n-1}$ are distinct grouplike elements of $(kC_n)^*$, and then a dimension argument shows that $(kC_n)^* = kG$. On the other hand $f_i = f_1^i$ for any i, so G is cyclic, i.e. $G \simeq C_n$. We conclude that $(kC_n)^* \simeq kC_n$.
(ii) We write C as a direct product of finite cyclic groups. The assertion follows now from (i) and the fact that for any groups G and H we have that $k(G \times H) \simeq kG \otimes kH$.

Exercise 4.3.7 *Let k be a field. Show that*
(i) If $char(k) \neq 2$, then any Hopf algebra of dimension 2 is isomorphic to kC_2, the group algebra of the cyclic group with two elements.
(ii) If $char(k) = 2$, then there exist precisely three isomorphism types of Hopf algebras of dimension 2 over k, and these are kC_2, $(kC_2)^*$, and a certain selfdual Hopf algebra.

Solution: Let H be a Hopf algebra of dimension 2 and complete the set $\{1\}$ to a basis with an element x such that $\varepsilon(x) = 0$ (we can do this since $H = k1 \oplus Ker(\varepsilon)$). Since $Ker(\varepsilon)$ is a one dimensional two-sided ideal of H, we have that $x^2 = ax$ for some $a \in k$. We consider the basis $\mathcal{B} = \{1 \otimes 1, x \otimes 1, 1 \otimes x, x \otimes x\}$ of $H \otimes H$. Write

$$\Delta(x) = \alpha 1 \otimes 1 + \beta x \otimes 1 + \gamma 1 \otimes x + \delta x \otimes x$$

for some scalars $\alpha, \beta, \gamma, \delta$. If we write the counit property we obtain that $x = \alpha 1 + \gamma x$ and $x = \alpha 1 + \beta x$, so $\alpha = 0$ and $\beta = \gamma = 1$. Thus $\Delta(x) = x \otimes 1 + 1 \otimes x + \delta x \otimes x$. If we write $\Delta(x^2) = \Delta(ax)$ and express both sides in terms of the basis $\mathcal{B}$, we obtain that $a^2\delta^2 + 3a\delta + 2 = 0$, so either $a\delta = -1$ or $a\delta = -2$.
On the other hand, if S is the antipode of H, then the relation $\sum S(x_1)x_2 = \varepsilon(x)1 = 0$ shows that $S(x)(1 + \delta x) + x = 0$, and if we take $S(x) = u1 + vx$ for some $u, v \in k$, we find that $u = 0$ and $v + v\delta a = -1$. Thus the situation $\delta a = -1$ is impossible, and we must have $\delta a = -2$. Now we distinguish two cases.
(i) If $char(k) \neq 2$, then $a \neq 0$ and $\delta = -\frac{2}{a}$. Then it is easy to determine that H has precisely two grouplike elements, namely 1 and $1 - \frac{2}{a}x$. Then $H = kG(H) \simeq kC_2$.
(ii) If $char(k) = 2$, then $a\delta = 0$, so either $a = 0$ or $\delta = 0$. If $a = 0$, it is

easy to see that if $\delta \neq 0$, then H has precisely two grouplike elements, 1 and $1+\delta x$, so again $H \simeq kC_2$. If $\delta = 0$ we obtain the Hopf algebra Γ with basis $\{1, x\}$ such that $x^2 = 0$ and $\Delta(x) = x \otimes 1 + 1 \otimes x$. This has only one grouplike element, this is 1, so Γ is not isomorphic to kC_2. Finally, let us take the situation where $\delta = 0$ and $a \in k$, $a \neq 0$. If we denote by H_1 the Hopf algebra obtained in this way for $a = 1$, i.e. H_1 has basis $\{1, x\}$ such that $x^2 = x$ and $\Delta(x) = x \otimes 1 + 1 \otimes x$, then it is clear that $f : H \to H_1$, $f(1) = 1, f(x) = \frac{1}{a}x$ is an isomorphism of Hopf algebras. In fact $H_1 \simeq (kC_2)^*$. Indeed, if we take $C_2 = \{1, c\}$, then $\{1, c\}$ is a basis of kC_2 and we consider the dual basis $\{p_1, p_c\}$ of $(kC_2)^*$. Then

$$\Delta(p_c) = p_1 \otimes p_c + p_c \otimes p_1 = (p_1 + p_c) \otimes p_c + p_c \otimes (p_1 + p_c)$$

since $char(k) = 2$, so p_c is a primitive element of $(kC_2)^*$. Also $p_c^2 = p_c$, so $(kC_2)^* \simeq H_1$. On the other hand $\Gamma^* \simeq \Gamma$. This can be seen again by taking in Γ^* the dual basis $\{p_1, p_x\}$ of $\{1, x\}$, and checking that p_x is a primitive element and $p_x^2 = p_x$. Thus $H_1 \simeq (kC_2)^*$, $\Gamma \simeq \Gamma^*$, and H_1 is not isomorphic to kC_2, and this ends the proof.

Exercise 4.3.8 *Let H be a Hopf algebra over the field k, such that there exists an algebra isomorphism $H \simeq k \times k \times \ldots \times k$ (k appears n times). Then H is isomorphic to $(kG)^*$, the dual of a group algebra of a group G with n elements.*

Solution: Since $H \simeq k \times k \times \ldots \times k$, we have that there exist precisely n algebra morphisms from H to k. But we know that $G(H^*)$, the set of grouplike elements of the algebra H^* is precisely $Hom_{k-alg}(H, k)$. Therefore H^* has n grouplike elements, and since $\dim(H^*) = n$, we have that $H^* \simeq kG$, where $G = G(H^*)$. It follows that $H \simeq (kG)^*$.

Exercise 4.3.9 *Let H be a bialgebra. Then the finite dual coalgebra H° is a subalgebra of the dual algebra H^*, and together with this algebra structure it is a bialgebra. Moreover, if H is a Hopf algebra, then H° is a Hopf algebra.*

Solution: Let $f, g \in H^\circ$, $\Delta(f) = \sum f_1 \otimes f_2$, $\Delta(g) = \sum g_1 \otimes g_2$. This means that

$$f(xy) = \sum f_1(x) f_2(y), \quad g(xy) = \sum g_1(x) g_2(y)$$

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

$$\begin{aligned} (f * g)(xy) &= \sum f((xy)_1) g((xy)_2) \\ &= \sum f(x_1 y_1) g(x_2 y_2) \\ &= \sum f_1(x_1) f_2(y_1) g_1(x_2) g_2(y_2) \\ &= \sum (f_1 * g_1)(x)(g_1 * g_2)(y) \end{aligned}$$

hence $f * g \in H^\circ$ and

$$\Delta(f * g) = \sum (f * g)_1 \otimes (f * g)_2 = \sum f_1 * g_1 \otimes f_2 * g_2,$$

i.e. Δ is multiplicative. Now $1_{H^\circ} = \varepsilon$, which is an algebra map. Then it is clear that Δ is an algebra map. It is also easy to see that $\varepsilon_{H^\circ}(f) = f(1)$ is an algebra map, so H° is a bialgebra.
If H is a Hopf algebra with antipode S. We show that S^* is an antipode for H°. Let $f \in H^\circ$, $\Delta(f) = \sum f_1 \otimes f_2$, i.e. $f(xy) = \sum f_1(x) f_2(y)$ for all $x, y \in H$. First

$$S^*(f)(xy) = f(S(xy)) = f(S(y)S(x)) = \sum f_1(S(y)) f_2(S(x)) =$$

$$= \sum S^*(f_1)(x) S^*(f_2)(y),$$

so $S^*(f) \in H^\circ$. Then

$$(\sum f_1 * S^*(f_2))(x) = \sum f_1(x_1) f_2(S(x_2)) = f(\sum x_1 S(x_2)) =$$

$$= \varepsilon(x) f(1) = \varepsilon_{H^\circ}(f) 1_{H^\circ}(x).$$

The other equality is proved similarly, so H° is a Hopf algebra with antipode S^*.

Exercise 4.3.10 *Let G be a monoid. Then the representative coalgebra $R_k(G)$ is a subalgebra of k^G, and even a bialgebra. If G is a group, then $R_k(G)$ is a Hopf algebra. If G is a topological group, then*

$$\tilde{R}_{\mathbf{R}}(G) = \{f \in R_{\mathbf{R}}(G) \mid f \text{ continuous}\}$$

is a Hopf subalgebra of $R_{\mathbf{R}}(G)$.
Solution: The canonical isomorphism $\phi : k^G \to (kg)^*$ is also an algebra map, so its restriction and corestriction $\overline{\phi} : R_k(G) \to (kG)^\circ$ is an isomorphism of both algebras and coalgebras. Thus $R_k(G)$ is a bialgebra by Exercise 4.3.9. If G is a group, then kG is a Hopf algebra, so $(kG)^\circ$ is a Hopf algebra, and therefore $R_k(G)$ is a Hopf algebra, with antipode given by $S^*(f)(x) = f(x^{-1})$ for any $f \in R_k(G)$ and $x \in G$.
Finally, if G is a topological group, then it is easy to see that $\tilde{R}_{\mathbf{R}}(G)$ is an $\mathbf{R}G$-subbimodule of $R_{\mathbf{R}}(G)$, and therefore it is a Hopf subalgebra.

Exercise 4.4.7 *Let H be a Hopf algebra. Show that for any right (left) H-comodule M, the injective dimension of M in the category $\mathcal{M}^H$ is less than or equal the injective dimension of the trivial right H-comodule k.*

In particular, the global dimension of the category $\mathcal{M}^H$ is equal to the injective dimension of the trivial right H-comodule k.

Solution: Let us take a (minimal) injective resolution

$$0 \to k \to Q_0 \to Q_1 \to \dots \tag{4.1}$$

of the trivial right H-comodule k. Let M be a right H-comodule. For any right H-comodule Q the tensor product $M \otimes Q$ is a right H-comodule with the coaction given by $m \otimes q \mapsto \sum m_{(0)} \otimes q_{(0)} \otimes m_{(1)} q_{(1)}$ for any $m \in M, q \in Q$. Tensoring (4.1) with M we obtain an exact sequence of right H-comodules

$$0 \to M \simeq M \otimes k \to M \otimes Q_0 \to M \otimes Q_1 \to \dots \tag{4.2}$$

If Q is injective in $\mathcal{M}^H$, then $M \otimes Q$ is injective in $\mathcal{M}^H$. Indeed, Q is a direct summand as an H-comodule in $H^{(I)}$ for some set I, say $H^{(I)} \simeq Q \oplus X$. Then $(M \otimes H)^{(I)} \simeq (M \otimes Q) \oplus (M \otimes X)$. Everything follows now if we show that $M \otimes H$ is an injective H-comodule. But it is easy to check that $M \otimes H$ is a right H-Hopf module with the coaction given as above by $m \otimes h \mapsto \sum m_{(0)} \otimes h_1 \otimes m_{(1)} h_2$, and the action $(m \otimes h)g = m \otimes hg$ for any $m \in M, h, g \in H$. This shows that $M \otimes H$ is an injective right H-comodule. This implies that (4.2) is an injective resolution of M, thus $inj.dim(M) \leq inj.dim(k)$.

Exercise 4.4.8 *Let H be a Hopf algebra. Show that for any right (left) H-module M, the projective dimension of M in the category $\mathcal{M}_H$ is less than or equal the projective dimension of the trivial right H-module k (with action defined by $\alpha \leftarrow h = \varepsilon(h)\alpha$ for any $\alpha \in k$ and $h \in H$). In particular the global dimension of the category $\mathcal{M}_H$ is equal to the projective dimension of the right H-module k.*

Solution: Let us consider a projective resolution of k in $\mathcal{M}_H$,

$$\dots P_1 \to P_0 \to k \to 0$$

If M is a right H-module, then for any right H-module P we have a right H-module structure on $M \otimes P$ with the action given by $(m \otimes p)h = \sum m h_1 \otimes p h_2$ for any $m \in M, p \in P, h \in H$. In this way we obtain an exact sequence of right H-modules

$$\dots M \otimes P_1 \to M \otimes P_0 \to M \otimes k \simeq M \to 0$$

We show that this is a projective resolution of M, and this will end the proof. Indeed, if P is a projective right H-module, then P is a direct summand in a free right H-module, thus $P \oplus X \simeq H^{(I)}$ as right H-modules for some right H-module X and some set I. Then $(M \otimes P) \oplus (M \otimes X) \simeq$

$(M \otimes H)^{(I)}$, so it is enough to show that $M \otimes H$ is projective. But this is true since $M \otimes H$ has a right H-Hopf module structure if we take the module structure and the right H-comodule structure given by $m \otimes h \mapsto \sum m \otimes h_1 \otimes h_2$, and we are done.

Bibliographical notes

Our main sources of inspiration for this chapter were the books of M. Sweedler [218], E. Abe [1], and S. Montgomery [149]. Exercises 4.4.7 and 4.4.8 are taken from [68] and [127], respectively. The Hopf modules are structures admitting a series of generalizations. One of these, the so called relative Hopf modules, introduced by Y. Doi [73], will be presented in Chapter 6. They generalize categories such as categories of graded modules over a ring graded by a group. An even more general structure was introduced independently by M. Koppinen [107] and Y. Doi [76]. These extend categories such as categories of modules graded by a G-set, categories of Yetter-Drinfel'd modules, etc. But things do not end here, because it is possible to find even more general structures, as some recent papers of Brzeziński show [38, 39]. We also recommend the book [51].

Chapter 5

Integrals

5.1 The definition of integrals for a bialgebra

Let H be a bialgebra. Then H^* has an algebra structure which is dual to the coalgebra structure on H. The multiplication is given by the convolution product. To simplify notation, if $h^*, g^* \in H^*$ we will denote the product of h^* and g^* in H^* by h^*g^* instead of $h^* * g^*$.

Definition 5.1.1 *A map $T \in H^*$ is called a left* integral *of the bialgebra H if $h^*T = h^*(1)T$ for any $h^* \in H^*$. The set of left integrals of H is denoted by $\int_l$. Left integrals of H^{cop} are called right integrals for H, and their set is denoted by $\int_r$.* ∎

Remark 5.1.2 *It is clear that $T \in H^*$ is a left integral if and only if $\sum T(x_2)x_1 = T(x)1 \; \forall x \in H$, and it is a right integral if and only if $\sum T(x_1)x_2 = T(x)1 \; \forall x \in H$.* ∎

We discuss briefly the name given to the above notion. Let G be a compact group. A Haar integral on G is a linear functional λ on the space of continuous functions from G to $\mathbf{R}$, which is translation invariant, i.e.

$$\lambda(xf) = \lambda(f)$$

for any continuous $f : G \to \mathbf{R}$, and any $x \in G$. Then the restriction of λ to the Hopf algebra $\tilde{R}_{\mathbf{R}}(G)$ of continuous representative functions on G is an integral in the sense of the above definition. Indeed,

$$\begin{aligned} \lambda(xf) &= \lambda(f), \;\; \forall f \in \tilde{R}_{\mathbf{R}}(G),\; x \in G \Leftrightarrow \\ \lambda(\sum f_2(x) f_1) &= \lambda(f)1, \;\; \forall f \in \tilde{R}_{\mathbf{R}}(G),\; x \in G \Leftrightarrow \end{aligned}$$

$$\begin{aligned}
\sum \lambda(f_1)f_2(x) &= \lambda(f)\mathbf{1}(x),\ \forall f \in \tilde{R}_{\mathbf{R}}(G),\ x \in G \Leftrightarrow \\
\sum \lambda(f_1)f_2 &= \lambda(f)\mathbf{1},\ \forall f \in \tilde{R}_{\mathbf{R}}(G) \Leftrightarrow \\
\sum \lambda(f_1)\mu(f_2) &= \lambda(f)\mu(\mathbf{1}),\ \forall f \in \tilde{R}_{\mathbf{R}}(G),\ \mu \in \tilde{R}_{\mathbf{R}}(G)^* \Leftrightarrow \\
(\lambda\mu)(f) &= (\mu(\mathbf{1})\lambda)(f),\ \forall f \in \tilde{R}_{\mathbf{R}}(G),\ \mu \in \tilde{R}_{\mathbf{R}}(G)^* \Leftrightarrow \\
\lambda\mu &= \mu(\mathbf{1})\lambda,\ \forall \mu \in \tilde{R}_{\mathbf{R}}(G)^*
\end{aligned}$$

and this explains the use of the name "integral" for bialgebras.

Remark 5.1.3 *1) $\int_l$ is clearly a vector subspace of H^*. Moreover, $\int_l$ is an ideal in the algebra H^*. That it is a right ideal is clear, since if $g^* \in H^*$, and $T \in \int_l$, then for any $h^* \in H^*$ we have*

$$h^*(Tg^*) = (h^*T)g^* = (h^*(1)T)g^* = h^*(1)Tg^*$$

and so $Tg^* \in \int_l$. To show that $\int_l$ is also a left ideal, with the same notation we have

$$h^*(g^*T) = (h^*g^*)T = (h^*g^*)(1)T = h^*(1)g^*(1)T = h^*(1)g^*T$$

showing that $g^*T \in \int_l$.
2) Consider the rational part of H^* to the left, hence $H_l^{*\,rat}$ is the sum of rational left ideals of the algebra H^*. Then $\int_l \subseteq H_l^{*\,rat}$. This follows immediately from Remark 2.2.3. In particular, if for a bialgebra we have $H_l^{*\,rat} = 0$, then also $\int_l = 0$, hence there are no nonzero left integrals. ∎

Before looking at some more examples, we give a result which will be frequently used in Chapter 6.

Lemma 5.1.4 *If t is a left integral, and $x, y \in H$, then*

$$\sum x_1 t(x_2 S(y)) = \sum t(xS(y_1))y_2.$$

Proof: We show that the two sides are equal by applying an arbitrary $h^* \in H^*$.

$$\begin{aligned}
\sum h^*(x_1)t(x_2S(y)) &= \sum h^*(x_1S(y_2)y_3)t(x_2S(y_1)) \\
&= \sum h^*(x_1S(y_1)_1y_2)t(x_2S(y_1)_2) \\
&= \sum (y_2 \rightharpoonup h^*)(1)t(xS(y_1)) = \sum h^*(y_2)t(xS(y_1)).
\end{aligned}$$

∎

We give now some examples of bialgebras, some having nonzero integrals, and some not.

Example 5.1.5 *1) Let G be a monoid, and $H = kG$ the semigroup algebra with bialgebra structure described in Section 4.3. We denote by $p_1 \in H^*$ the map defined by $p_1(g) = \delta_{1,g}$ for any $g \in G$, where 1 means here the identity element of the monoid. Then p_1 is a left and right integral for H. Indeed, if $h^* \in H^*$, then for any $g \in G$ we have $(h^*p_1)(g) = h^*(g)p_1(g) = \delta_{1,g}h^*(g) = h^*(1)p_1(g)$. The last equality is clear if $g = 1$, and if $g \neq 1$, then both sides are zero. Since H is cocommutative, p_1 is also a right integral.*
2) Let H be the divided power Hopf algebra from example 5) in Section 4.3. Hence H is a k-vector space with basis $\{c_i | i \in \mathbf{N}\}$, the coalgebra structure is defined by

$$\Delta(c_m) = \sum_{i=0}^{m} c_i \otimes c_{m-i}, \ \varepsilon(c_m) = \delta_{0,m}$$

and the algebra structure by

$$c_n c_m = \binom{n+m}{n} c_{n+m}$$

with identity element $1 = c_0$. We know that there exists an isomorphism of algebras

$$\phi : H^* \to k[[X]], \ \phi(h^*) = \sum_{n \geq 0} h^*(c_n) X^n$$

for $h^* \in H^*$. Suppose T is a left (i.e. also right) integral of H. Then for any $h^* \in H^*$ we have $h^*T = h^*(1)T$, and applying ϕ we obtain $\phi(h^*)\phi(T) = h^*(1)\phi(T)$. Noting that $h^*(1) = \phi(h^*)(0)$, it follows that $\phi(T)$ is a formal power series for which $F\phi(T) = F(0)\phi(T)$ for any formal power series F. Choosing then $F \neq 0$ such that $F(0) = 0$ (e.g. $F = X$), we obtain that $\phi(T) = 0$ (since $k[[X]]$ is a domain), and since ϕ is an isomorphism, this implies $\int_l = 0$.
3) Let k be a field of characteristic zero, and $H = k[X]$ with the Hopf algebra structure described in example 8) of Section 4.3. Then H does not have nonzero integrals. Indeed, if $T \in H^*$ is an integral, then $h^*T = h^*(1)T$ for any $h^* \in H^*$. Since $\Delta(X) = X \otimes 1 + 1 \otimes X$, applying the above equality for X we get $h^*(X)T(1) = 0$, and choosing h^* with $h^*(X) \neq 0$ it follows that $T(1) = 0$. Then we prove by induction that $T(X^n) = 0$ for any $n \geq 0$. To go from $n-1$ to n we apply the equality $h^*T = h^*(1)T$ to X^{n+1} and we use the formula

$$\Delta(X^{n+1}) = \sum_{0 \leq i \leq n+1} \binom{n+1}{i} X^{n+1-i} \otimes X^i$$

By the induction hypothesis we obtain that $h^*(X)T(X^n) = 0$, and choosing again h^* with $h^*(X) \neq 0$ we find $T(X^n) = 0$. Consequently, $T = 0$. ∎

Exercise 5.1.6 *Let H be a Hopf algebra over the field k, K a field extension of k, and $\overline{H} = K \otimes_k H$ the Hopf algebra over K defined in Exercise 4.2.17. If $T \in H^*$ is a left integral of H, show that the map $\overline{T} \in \overline{H}^*$ defined by $\overline{T}(\delta \otimes_k h) = \delta T(h)$ is a left integral of $\overline{H}$.*

Exercise 5.1.7 *Let H and H' be two Hopf algebras with nonzero integrals. Then the tensor product Hopf algebra $H \otimes H'$ has a nonzero integral.*

5.2 The connection between integrals and the ideal $H^{*\,rat}$

Let H be a Hopf algebra. Throughout this section, by $H^{*\,rat}$ we mean the rational part of H^* to the left. Later in this section we will show that the rational parts of H^* to the left and to the right are in fact equal, which will justify our not writing the index l. We saw in the preceding section that if $H^{*\,rat} = 0$, then $\int_l = 0$. The aim of this section is to find a more precise connection between $H^{*\,rat}$ and $\int_l$.

We know that $H^{*\,rat}$ is a rational left H^*-module, and this induces a right H-comodule structure on $H^{*\,rat}$, defined by $\rho : H^{*\,rat} \to H^{*\,rat} \otimes H$, $\rho(h^*) = \sum h^*_{(0)} \otimes h^*_{(1)}$ such that $g^*h^* = \sum g^*(h^*_{(1)})h^*_{(0)}$ for any $g^* \in H^*$.

Consider the action $\rightharpoonup$ of H on H^* defined as follows: if $h \in H$ and $h^* \in H^*$, then $h \rightharpoonup h^* \in H^*$ is given by $(h \rightharpoonup h^*)(g) = h^*(gh)$ for any $g \in H$. In this way, H^* becomes a left H-module, and this structure is in fact induced by the canonical right H-module structure of H, taking into account that $H^* = Hom(H, k)$. Using Proposition 4.2.14, this left H-module structure on H^* induces a right H-module structure on H^* as follows: if $h \in H$ and $h^* \in H^*$, define $h^* \leftharpoonup h = S(h) \rightharpoonup h^*$. We then have $(h^* \leftharpoonup h)(g) = h^*(gS(h))$ for any $g \in H$.

Theorem 5.2.1 *$H^{*\,rat}$ is a right H-submodule of H^* (with action $\leftharpoonup$). This right H-module structure, and the right H-comodule structure given by ρ define on $H^{*\,rat}$ a right H-Hopf module structure.*

Proof: Let $h^* \in H^{*\,rat}$ and $h \in H$. We show that for any $g^* \in H^*$ we have the relation

$$g^*(h^* \leftharpoonup h) = \sum g^*(h^*_{(1)}h_2)(h^*_{(0)} \leftharpoonup h_1)$$

Let $g \in H$. Then

$$\begin{aligned} &(\sum g^*(h^*_{(1)}h_2)(h^*_{(0)} \leftharpoonup h_1))(g) = \\ &= \sum g^*(h^*_{(1)}h_2)h^*_{(0)}(gS(h_1)) \end{aligned}$$

$$\begin{aligned}
&= \sum (h_2 \rightharpoonup g^*)(h^*_{(1)})h^*_{(0)}(gS(h_1)) \\
&= \sum ((h_2 \rightharpoonup g^*)h^*)(gS(h_1)) \\
&\qquad \text{(by the definition of } \rho) \\
&= \sum (h_2 \rightharpoonup g^*)(gS(h_1)_1)h^*((gS(h_1))_2) \\
&\qquad \text{(by the definition of convolution)} \\
&= \sum (h_3 \rightharpoonup g^*)(g_1 S(h_2))h^*(g_2 S(h_1)) \\
&= \sum g^*(g_1 S(h_2)h_3)h^*(g_2 S(h_1)) \\
&= \sum g^*(g_1 \varepsilon(h_2))h^*(g_2 S(h_1)) \\
&= \sum g^*(g_1)h^*(g_2 S(h)) \\
&= (g^*(h^* \leftharpoonup h))(g)
\end{aligned}$$

proving the required relation. This shows that $h^* \leftharpoonup h \in H^{*\ rat}$, and moreover, that

$$\rho(h^* \leftharpoonup h) = \sum h^*_{(0)} \leftharpoonup h_1 \otimes h^*_{(1)}h_2$$

i.e. $H^{*\ rat}$ is a right H-Hopf module. ∎

The following lemma shows that there is a close connection between $H^{*\ rat}$ and $\int_l$.

Lemma 5.2.2 *The subspace of coinvariants $(H^{*\ rat})^{coH}$ is exactly $\int_l$.*

Proof: Let $h^* \in H^{*\ rat}$. Then $h^* \in (H^{*\ rat})^{coH}$ if and only if $\rho(h^*) = h^* \otimes 1$, and this is equivalent to $g^*h^* = g^*(1)h^*$ for any $g^* \in H^*$. But this is the definition of a left integral. ∎

We can now prove the result showing the complete connection between $H^{*\ rat}$ and $\int_l$.

Theorem 5.2.3 *The map $f : \int_l \otimes H \to H^{*\ rat}$ defined by $f(t \otimes h) = t \leftharpoonup h$ for any $t \in \int_l$, $h \in H$, is an isomorphism of right H-Hopf modules.*

Proof: Follows directly from the fundamental theorem of Hopf modules applied to the Hopf module $H^{*\ rat}$. ∎

We already saw that if $H^{*\ rat} = 0$, then $\int_l = 0$. The preceding theorem shows that the converse also holds.

Corollary 5.2.4 *$H^{*\ rat} = 0$ if and only if $\int_l = 0$.* ∎

Exercise 5.2.5 *Let H be a Hopf algebra. Then the following assertions are equivalent:*

i) H has a nonzero left integral.
ii) There exists a finite dimensional left ideal in H^*.
iii) There exists $h^* \in H^*$ such that $Ker(h^*)$ contains a left coideal of finite codimension in H.

Corollary 5.2.6 *Let H be a Hopf algebra with antipode S, and having a nonzero integral. Then S is injective. If moreover H is finite dimensional, then $\int_s$ has dimension 1 and S is bijective.*

Proof: From Theorem 5.2.3, if there would exist an $h \neq 0$ with $S(h) = 0$, then for a $t \in \int_l$, $t \neq 0$ we would have $f(t \otimes h) = 0$, contradicting the injectivity of f.
If H is finite dimensional, Example 2.2.4 shows that $H^{*\,rat} = H^*$. We obtain an isomorphism of Hopf modules $f : \int_l \otimes H \to H^*$ defined by $f(t \otimes h) = t \leftharpoonup h = S(h) \rightharpoonup t$. In particular, this is an isomorphism of vector spaces, and so $dim(H^*) = dim(\int_l \otimes H)$. But $dim(H^*) = dim(H)$ and $dim(\int_l \otimes H) = dim(\int_l) dim(H)$. Therefore, $dim(\int_l) = 1$. Moreover, since S is an injective endomorphism of the finite dimensional vector space H, it follows that S is an isomorphism, and so it is bijective. ∎

When H is a finite dimensional Hopf algebra, there is still another way to work with integrals. We recall that there is an isomorphism of algebras $\phi : H \to H^{**}$ defined by $\phi(h)(h^*) = h^*(h)$ for any $h \in H, h^* \in H^*$. Then it makes sense to talk about left integrals for the Hopf algebra H^*, these being elements in H^{**}. Since ϕ is bijective, there exists a nonzero element $h \in H$ such that $\phi(h) \in H^{**}$ is a left integral for H^*. Since any element in H^{**} is of the form $\phi(l)$ with $l \in H$, this means that for any $l \in H$ we have $\phi(l)\phi(h) = \phi(l)(1_{H^*})\phi(h)$. But $\phi(l)\phi(h) = \phi(lh)$ (ϕ is a morphism of algebras) and $\phi(l)(1_{H^*}) = \phi(l)(\varepsilon) = \varepsilon(l)$, hence the fact that $\phi(h)$ is a left integral for H^* is equivalent to $lh = \varepsilon(l)h$ for any $l \in H$. This justifies the following definition.

Definition 5.2.7 *Let H be a finite dimensional Hopf algebra. A* left integral *in H is an element $t \in H$ for which $ht = \varepsilon(h)t$ for any $h \in H$.* ∎

Remark 5.2.8 *i) If H is a finite dimensional Hopf algebra, there is some danger of confusion between left integrals for H (which are elements of H^*), and left integrals in H (which are elements of H). Left integrals in H are in fact left integrals for H^* when they are regarded via the isomorphism $\phi : H \to H^{**}$. This is why we will have to specify every time which of the two kind of integrals we are using.*
ii) Corollary 5.2.6 shows that in any finite dimensional Hopf algebra there

exist nonzero left integrals, and moreover, the subspace they span has dimension 1, and is therefore kt, where t is a nonzero left integral in H.
∎

Example 5.2.9 *1) Let G be a finite group, and kG the group algebra with the Hopf algebra structure described in Section 4.3 1). Then $t = \sum_{g \in G} g$ is a left (and right) integral in kG.*
2) If G is a finite group, then $(kG)^*$, the dual of kG, is a Hopf algebra, and the map $p_1 \in (kG)^*$, $p_1(g) = \delta_{1,g}$, is a left (and right) integral in $(kG)^*$.
3) Let k be a field of characteristic $p > 0$, and $H = k[X]/(X^p)$ the Hopf algebra described in Section 4.3 9). Then $t = x^{p-1}$ is a left (and right) integral in H.
4) Let H denote Sweedler's 4-dimensional Hopf algebra described in Section 4.3 6). Then $x + cx$ is a left integral in H, and $x - cx$ is a right integral in H.
5) Let $H_{n^2}(\lambda)$ be a Taft algebra described in Section 4.3 7). Then $t = (1 + c + \ldots + c^{n-1})x^{n-1}$ is a left integral in $H_{n^2}(\lambda)$. ∎

An important application of integrals in finite dimensional Hopf algebras is is the following result, known as Maschke's theorem. Here is the classical proof. For a different proof see Exercise 5.5.13.

Theorem 5.2.10 *Let H be a finite dimensional Hopf algebra. Then H is a semisimple algebra if and only if $\varepsilon(t) \neq 0$ for a left integral $t \in H$.*

Proof: Suppose first that H is semisimple. We know that $Ker(\varepsilon)$ is an ideal of codimension 1 in H. Regarding $Ker(\varepsilon)$ as a left submodule of H, by the semisimplicity of H we have that $Ker(\varepsilon)$ is a direct summand in H, hence there exists a left ideal I of H with $H = ker(\varepsilon) \oplus I$. Let $1 = z + h$, with $z \in Ker(\varepsilon), h \in H$, be the representation of 1 as a sum of two elements from $Ker(\varepsilon)$ and I. Clearly $h \neq 0$, because $1 \notin Ker(\varepsilon)$. Since I has dimension 1 (since $Ker(\varepsilon)$ has codimension 1), it follows that $I = kh$. Let now $l \in H$. Then $lh \in I$, and so the representation of lh in the direct sum $H = Ker(\varepsilon) \oplus I$ is $lh = 0 + lh$. On the other hand, we have $l = (l - \varepsilon(l)1) + \varepsilon(l)1$, and so $lh = (l - \varepsilon(l)1)h + \varepsilon(l)h$. Since $(l - \varepsilon(l)1)h \in Ker(\varepsilon)$, $\varepsilon(l)h \in I$, and the representation of an element in H as a sum of two elements in $Ker(\varepsilon)$ and I is unique, it follows that $(l - \varepsilon(l)1)h = 0$ and $\varepsilon(l)h = lh$. The last relation shows that h is a left integral in H. Since $I \cap Ker(\varepsilon) = 0$, it follows that $\varepsilon(h) \neq 0$, and the first implication is proved.

We assume now that $\varepsilon(t) \neq 0$ for a left integral t in H. We fix such an integral t with $\varepsilon(t) = 1$ (we can do this by replacing t by $t/\varepsilon(t)$). In order to show that H is semisimple, we have to show that for any left

H-module M, and any H-submodule N of M, N is a direct summand in M. Let $\pi : M \to N$ be a linear map such that $\pi(n) = n$ for any $n \in N$ (to construct such a map we write M as a direct sum of N and another subspace, and then take the projection on N). We define

$$P : M \to N,\ P(m) = \sum t_1\pi(S(t_2)m) \text{ for any } m \in M.$$

We show first that $P(n) = n$ for any $n \in N$. Indeed,

$$\begin{aligned} P(n) &= \sum t_1\pi(S(t_2)n) \\ &= \sum t_1 S(t_2)n \quad \text{(since } S(t_2)n \in N\text{)} \\ &= \varepsilon(t)1n \quad \text{(by the property of the antipode)} \\ &= n \quad \text{(since } \varepsilon(t) = 1\text{)} \end{aligned}$$

We show now that P is a morphism of left H-modules. Indeed, for $m \in M$ and $h \in H$ we have

$$\begin{aligned} hP(m) &= \sum ht_1\pi(S(t_2)m) \\ &= \sum h_1t_1\pi(S(t_2)\varepsilon(h_2)m) \text{ (by the counit property)} \\ &= \sum h_1t_1\pi(S(t_2)S(h_2)h_3m) \text{ (by the property of the antipode)} \\ &= \sum h_1t_1\pi(S(h_2t_2)h_3m) \\ &= \sum (h_1t)_1\pi(S((h_1t)_2)h_2m) \\ &= \sum \varepsilon(h_1)t_1\pi(S(t_2)h_2m) \text{ (since } h_1t = \varepsilon(h_1)t\text{)} \\ &= \sum t_1\pi(S(t_2)hm) \text{ (by the counit property)} \\ &= P(hm) \end{aligned}$$

We have showed that there exists a morphism of left H-modules $P : M \to N$ such that $P(n) = n$ for any $n \in N$. Then N is a direct summand in M as left H-modules, (in fact $M = N \oplus Ker(P)$) and the proof is finished. ∎

Remark 5.2.11 *If G is a finite group, and $H = kG$, then we saw that $t = \sum_{g\in G} g$ is a left integral in H. Then $\varepsilon(t) = |G|1_k$, where $|G|$ is the order of the group G. The preceding theorem shows that the Hopf algebra kG is semisimple if and only if $|G|1_k \neq 0$, hence if and only if the characteristic of k does not divide the order of the group G. This is the well known Maschke theorem for groups.* ∎

If H is a semisimple Hopf algebra, and $t \in H$ is a left integral with $\varepsilon(t) = 1$, then t is a central idempotent, because $S(t)$ is clearly a right integral in H (i.e. $S(t)h = \varepsilon(h)S(t)$), and we have

$$t = \varepsilon(t)t = \varepsilon(S(t))t = S(t)t = \varepsilon(t)S(t) = S(t).$$

Recall that a k-algebra A is called *separable* (see [112]) if there exists an element $\sum a_i \otimes b_i \in A \otimes A$ such that $\sum a_i b_i = 1$ and

$$\sum x a_i \otimes b_i = \sum a_i \otimes b_i x$$

for all $x \in A$. Such an element is called a separability idempotent.

Exercise 5.2.12 *A semisimple Hopf algebra is separable.*

Exercise 5.2.13 *Let H be a finite dimensional Hopf algebra over the field k, K a field extension of k, and $\overline{H} = K \otimes_k H$ the Hopf algebra over K defined in Exercise 4.2.17. If $t \in H$ is a left integral in H, show that $\bar{t} = 1_K \otimes_k t \in \overline{H}$ is a left integral in $\overline{H}$. As a consequence show that H is semisimple over k if and only if $\overline{H}$ is semisimple over K.*

5.3 Finiteness conditions for Hopf algebras with nonzero integrals

Lemma 5.3.1 *Let H be a Hopf algebra. If J is a nonzero right (left) ideal which is also a right (left) coideal of H, then $J = H$. In particular we obtain the following:*
(i) If H is a Hopf algebra that contains a nonzero right (left) ideal of finite dimension, then H has finite dimension.
(ii) A semisimple Hopf algebra (i.e. a Hopf algebra which is semisimple as an algebra) is finite dimensional.
(iii) A Hopf algebra containing a left integral in H (i.e. an element $t \in H$ with $ht = \varepsilon(h)t$ for all $h \in H$) is finite dimensional.

Proof: If J is a right ideal and a right coideal, then $\Delta(J) \subseteq J \otimes H$ and $JH = J$. If $\varepsilon(J) = 0$, then for any $h \in J$ we have $h = \sum \varepsilon(h_1)h_2 \in \varepsilon(J)H = 0$, so $J = 0$, a contradiction. Thus $\varepsilon(J) \neq 0$, and then there exists $h \in H$ with $\varepsilon(h) = 1$. Then $1 = \varepsilon(h)1 = \sum h_1 S(h_2) \in JH \subseteq J$, so $1 \in J$ and $J = H$.
We show that the assertion (i) can be deduced from the first part of the statement. Indeed, let J be a nonzero right ideal of finite dimension in a

Hopf algebra H, and let $I = H^* \rightharpoonup J$, which is a right ideal, a right coideal and has finite dimension. The fact that I is a right ideal follows from

$$\begin{aligned}(h^* \rightharpoonup x)y &= \sum h^*(x_2)x_1y \\ &= \sum h^*(x_2y_2S(y_3))x_1y_1 \\ &= \sum (h^* \leftharpoonup y_2) \rightharpoonup (xy_1)\end{aligned}$$

for any $h^* \in H^*, x \in J, y \in H$. Then $I = H$, so H is finite dimensional. For (ii), let us take a semisimple Hopf algebra H. Then $Ker(\varepsilon)$ is a left ideal of H. Since H is a semisimple left H-module, there exists a left ideal I of H such that $H = I \oplus Ker(\varepsilon)$. Since $Ker(\varepsilon)$ has codimension 1 in H, we have that I has dimension 1. Then H is finite dimensional by (i). Note that by Theorem 5.2.10, I is the ideal generated by an idempotent integral in H.
(iii) The subspace generated by t is a finite dimensional left ideal. ∎

Theorem 5.3.2 *(Lin, Larson, Sweedler, Sullivan) Let H be a Hopf algebra. Then the following assertions are equivalent.*
(i) H has a nonzero left integral.
(ii) H is a left co-Frobenius coalgebra.
(iii) H is a left QcF coalgebra.
(iv) H is a left semiperfect coalgebra.
(v) H has a nonzero right integral.
(vi) H is a right co-Frobenius coalgebra.
(vii) H is a right QcF coalgebra.
(viii) H is a right semiperfect coalgebra.
(ix) H is a generator in the category ${}^H\mathcal{M}$ (or in $\mathcal{M}^H$).
(x) H is a projective object in the category ${}^H\mathcal{M}$ (or in $\mathcal{M}^H$).

Proof: *(i)* $\Rightarrow$ *(ii)*. Let $t \in H^*$ be a nonzero left integral. We define the bilinear application $b : H \times H \to k$ by $b(x, y) = t(xS(y))$ for any $x, y \in H$. We show that b is H^*-balanced. Let $x, y \in H$ and $h^* \in H^*$. Then

$$\begin{aligned}&b(x \leftharpoonup h^*, y) = \\ =& \sum h^*(x_1)t(x_2S(y)) \\ =& \sum h^*(x_1)t(x_2S(y_1)\varepsilon(y_2)) \quad \text{(by the counit property)} \\ =& \sum\sum h^*(x_1S(y_2)y_3)t(x_2S(y_1)) \quad \text{(the property of the antipode)} \\ =& \sum (y_3 \rightharpoonup h^*)(x_1S(y_2))t(x_2S(y_1)) \\ =& \sum (y_2 \rightharpoonup h^*)(x_1S(y_1)_1)t(x_2S(y_1)_2)\end{aligned}$$

$$
\begin{aligned}
&= \sum (y_2 \rightharpoonup h^*)((xS(y_1))_1)t((xS(y_1))_2) \\
&= \sum (y_2 \rightharpoonup h^*)(1)t(xS(y_1)) \quad (t \text{ is a left integral}) \\
&= \sum h^*(y_2)t(xS(y_1)) \\
&= b(x, h^* \rightharpoonup y)
\end{aligned}
$$

Now we show that b is left non-degenerate. Assume that for some $y \in H$ we have $b(x, y) = 0$ for any $x \in H$. Then $t(xS(y)) = 0$ for any $x \in H$. But $t(xS(y)) = (t \leftharpoonup y)(x)$ and we obtain $t \leftharpoonup y = 0$. Now Theorem 5.2.3 shows that $y = 0$. This implies that H is left co-Frobenius.
$(ii) \Rightarrow (iii) \Rightarrow (iv)$ are obvious (by Corollary 3.3.6).
$(iv) \Rightarrow (v)$ Since H is left semiperfect we have that $Rat(H^*_{H^*})$ is dense in H^*. Then obviously $Rat(H^*_{H^*}) \neq 0$, and by Theorem 5.2.3 applied to $H^{op,cop}$ we have that $\int_r \neq 0$.
$(v) \Rightarrow (vi) \Rightarrow (vii) \Rightarrow (viii) \Rightarrow (i)$ are the right hand side versions of the facts proved above.
(iii) and $(vii) \Rightarrow (ix)$ and (x) follow by Corollary 3.3.11.
$(ix) \Rightarrow (i)$ If H is a generator of ${}^H\mathcal{M}$, since $k1$ is a left H-comodule, there exist a nonzero morphism $t : H \to k$ of left H-comodules. Then t is a nonzero left integral.
$(x) \Rightarrow (iv)$ (or $(x) \Rightarrow (viii)$) Since H is projective in ${}^H\mathcal{M}$, we have that $Rat({}_{H^*}H^*)$ is dense in H^* by Corollary 2.4.22. ∎

Corollary 5.3.3 *Let H be a Hopf algebra with nonzero integrals. Then any Hopf subalgebra of H has nonzero integrals.*

Proof: Let K be a Hopf subalgebra. Since H is left semiperfect as a coalgebra, then by Corollary 3.2.11 K is also left semiperfect. ∎

Remark 5.3.4 *If H has a nonzero left integral t, and K is a Hopf subalgebra of H, then the above corollary tells us that K has a nonzero left integral. However, such a nonzero integral is not necessarily the restriction of t to K. Indeed, it might be possible that the restriction of t to K to be zero, as it happens for instance in the situation where H is a co-Frobenius Hopf algebra which is not cosemisimple, and $K = k1$ (this will be clear in view of Exercise 5.5.9, where a characterization of the cosemisimplicity is given).* ∎

Exercise 5.3.5 *Let H be a finite dimensional Hopf algebra. Show that H is injective as a left (or right) H-module.*

5.4 The uniqueness of integrals and the bijectivity of the antipode

Lemma 5.4.1 *Let H be a Hopf algebra with nonzero integrals, I a dense left ideal in H^*, M a finite dimensional right H-comodule and $f : I \to M$ a morphism of left H^*-modules. Then there exists a unique morphism $h : H^* \to M$ of H^*-modules extending f.*

Proof: Let $E(M)$ be the injective envelope of M as a right H-comodule. Then $E(M)$ is also injective as a left H^*-module (see Corollary 2.4.19). Regarding f as a H^*-morphism from I to $E(M)$, we get a morphism $h : H^* \to E(M)$ of left H^*-modules extending f. If $x = h(\varepsilon) \in E(M)$, then

$$Ix = Ih(\varepsilon) = h(I\varepsilon) = h(I) = f(I) \subseteq M.$$

Since I is dense in H^*, we have that $x \in Ix$. Indeed, there exists $h^* \in I$ such that h^* agrees with ε on all the x_1's from $x \mapsto \sum x_0 \otimes x_1$ (the comodule structure map of $E(M)$). Then $x = \sum \varepsilon(x_1)x_0 = \sum h^*(x_1)x_0 = h^*x \in Ix$. We obtain $x \in M$, and hence $Im(h) \subseteq M$. Thus h is exactly the required morphism.
If h' is another morphism with the same property, then $h - h'$ is 0 on I. Then

$$I(h-h')(\varepsilon) = (h-h')(I\varepsilon) = (h-h')(I) = 0$$

and again since I is dense in H^* we have that $(h-h')(\varepsilon) \in I(h-h')(\varepsilon)$, so $(h-h')(\varepsilon) = 0$. Then clearly $h = h'$. ∎

Theorem 5.4.2 *Let H be a Hopf algebra with nonzero integral and M a finite dimensional right H-comodule. Then* $\dim Hom_{H^*}(H, M) = \dim M$. *In particular* $\dim \int_r = \dim \int_l = 1$.

Proof: $Rat({}_{H^*}H^*)$ is a dense subspace of H^* by Theorem 3.2.3. Also by Theorem 5.3.2 there exists an injective morphism $\theta : H \to H^*$ of left H^*-modules. Clearly $\theta(H) \subseteq Rat({}_{H^*}H^*)$ and since H is an injective object in the category $\mathcal{M}^H$, we obtain that H is a direct summand as a left H^*-module in $Rat({}_{H^*}H^*)$. Thus there exists a surjective k-morphism $Hom_{H^*}(H^{*\,rat}, M) \to Hom_{H^*}(H, M)$. By Lemma 5.4.1,

$$Hom_{H^*}(H^{*\,rat}, M) \simeq Hom_{H^*}(H^*, M) \simeq M.$$

We obtain an inequality

$$\dim Hom_{H^*}(H, M) \leq \dim Hom_{H^*}(H^{*\,rat}, M) = \dim M.$$

If we take $M = k$, the trivial right H-comodule, we have that $\int_r = Hom_{H^*}(H, k)$ has dimension at most 1, so this has dimension precisely 1 since $\int_r \neq 0$. Similarly $\int_l$ has dimension 1. Hence there exists even an isomorphism of left H^*-modules $\theta : H \to H^{*rat}$, $\theta(h) = t \leftharpoonup h$, where t is a fixed non-zero left integral. Then the surjective morphism $Hom_{H^*}(H^{*\,rat}, M) \to Hom_{H^*}(H, M)$ obtained above from θ is an isomorphism, showing that in fact dim $Hom_{H^*}(H, M) =$ dim M. ∎

Remark 5.4.3 *The proof of the result of the above theorem can be done in a more general setting. If C is a left and right co-Frobenius coalgebra, and M is a finite dimensional right C-comodule, then* dim $Hom_{C^*}(C, M) \leq$ dim M. ∎

We will prove now that the antipode of a co-Frobenius Hopf algebra is bijective. The next lemma is the first step in this direction.

Lemma 5.4.4 *1) Let H and K be two Hopf algebras and $\phi : H \to K$ an injective coalgebra morphism with $\phi(1) = 1$. If $t \in K^*$ is a left integral, then $t \circ \phi$ is a left integral in H^*.*
2) Let H be a Hopf algebra with a nonzero left integral t and antipode S. Then $t \circ S$ is a nonzero right integral of H.

Proof: 1) Since t is a left integral for K, for any $z \in K$ we have that $\sum t(z_2)z_1 = t(z)1$. Take $z = \phi(h)$ with $h \in H$, and use the fact that ϕ is a coalgebra morphism. We find that $\sum t(\phi(h_2))\phi(h_1) = t(\phi(h))1$. This shows that $\phi(\sum t(\phi(h_2))h_1) = \phi(t(\phi(h))1)$, which by the injectivity of ϕ implies $\sum t(\phi(h_2))h_1 = t(\phi(h))1$, i.e. $t \circ \phi$ is a left integral for H.
2) We consider $S : H \to H^{op,cop}$, an injective coalgebra morphism with $S(1) = 1$. We use 1) and see that if t is a nonzero left integral for H, then $t \circ S$ is a left integral for $H^{op,cop}$, i.e. a right integral for H. It remains to show that $t \circ S \neq 0$. Let $J \subseteq H$ be the injective envelope of $k1$, considered as a right H-comodule. Then J is finite dimensional and $H = J \oplus X$ for a right coideal X of H. Let $f \in H^*$ such that $f(X) = 0$ and $f(1) \neq 0$. Then $Ker(f)$ contains a right coideal of finite codimension, thus $f \in H^{*rat}$. Hence $f = t \leftharpoonup h$ for some $h \in H$, and $f(1) = (t \leftharpoonup h)(1) = t(S(h))$, showing that $t \circ S \neq 0$. ∎

Corollary 5.4.5 *If H is a Hopf algebra with nonzero integrals, we have that $S^*(\int_l) = \int_r$.*

Proof: It follows from the second assertion of Lemma 5.4.4 and the uniqueness of integrals. ∎

Corollary 5.4.6 *Let H be a Hopf algebra with nonzero integral. Then the antipode S of H is bijective.*

Proof: We fix a nonzero left integral t. We know from Corollary 5.2.6 that S is injective. We prove that S is also surjective. Otherwise, if we assume that $S(H) \neq H$, since $S(H)$ is a subcoalgebra of H, we have that $S(H)$ is a left H-subcomodule of H, and by Corollary 3.2.6 there exists a maximal left H-subcomodule M of H such that $S(H) \subseteq M$. Let $u \in H^*$ such that $u \neq 0$ and $u(M) = 0$. Since $Ker(u)$ contains M, we have that $u \in Rat({}_{H^*}H^*)$, thus there exists an $h \in H$ such that $u = t \leftharpoonup h$. Clearly $h \neq 0$ and for any $x \in M$ we have $(t \leftharpoonup h)(x) = u(x) = 0$. For any $y \in H$ we have $S(y) \in M$, so

$$\begin{aligned}(t \circ S)(hy) &= t(S(hy)) \\ &= t(S(y)S(h)) \\ &= (t \leftharpoonup h)(S(y)) \\ &= 0\end{aligned}$$

so $(t \circ S)(hH) = 0$. Since $t \circ S$ is a right integral, then $t \circ S$ is a morphism of left H^*-modules, so $(t \circ S)(H^* \rightharpoonup (hH)) = 0$. Lemma 5.3.1 tells us that $H^* \rightharpoonup (hH) = H$, and then $(t \circ S)(H) = 0$. This is a contradiction with Lemma 5.4.4. ∎

Remark 5.4.7 *If H is a Hopf algebra with nonzero integral and t is a non-zero left (or right) integral, we have that*

$$t \leftharpoonup H = t \leftharpoondown H = H \rightharpoonup t = H \rightharpoondown t = H^{*rat}$$

Indeed, let t be a nonzero left integral. Then the relation $t \leftharpoonup H = H^{*rat}$ follows from Theorem 5.2.3 and the uniqueness of the integrals. Also $H^{*rat} = t \leftharpoonup H = S(H) \rightharpoonup t = H \rightharpoondown t$ (we have used the bijectivity of the antipode). If we write now the relation $t \leftharpoonup H = H^{*rat}$ for H^{op}, we obtain that $t \leftharpoondown H = H^{*rat}$, which also shows that $H \rightharpoondown t = H^{*rat}$.

The next exercise provides another proof for the uniqueness of integrals.

Exercise 5.4.8 *Let $\chi \in \int_l$ and $h \in H$ be such that $\chi \circ S(h) = 1$. Then χ spans $\int_l$.*

5.5 Ideals in Hopf algebras with nonzero integrals

We recall that for a coalgebra C we denote by $G(C)$ the set of all grouplike elements of C (i.e. $g \in G(C)$ if $\Delta(g) = g \otimes g$ and $\varepsilon(g) = 1$). It is possible to have $G(C) = \emptyset$ (see Example 1.4.17).

Proposition 5.5.1 *Let C be a coalgebra. Then*
(i) Every right (left) coideal of C of dimension 1 is spanned by a grouplike element.
(ii) There exists a bijective correspondence between $G(C)$ and the set of all coalgebra morphisms from k (regarded as a coalgebra) to C. Thus any 1-dimensional subcoalgebra of C is of the form kg for some $g \in G(C)$.
(iii) There exists a bijective correspondence between $G(C)$ and the set of all continuous algebra morphisms from C^* to k.

Proof: (i) Let I be a right coideal of C of dimension 1. If $c \in I, c \neq 0$, then $I = kc$, and since $\Delta(I) \subseteq I \otimes C$ there exists $g \in C$ such that $\Delta(c) = c \otimes g$. The coassociativity of Δ shows that $c \otimes g \otimes g = c \otimes \Delta(g)$, thus $\Delta(g) = g \otimes g$. Since $c \neq 0$ we must have $g \neq 0$, so $g \in G(C)$. On the other hand the counit property shows that $c = \varepsilon(c)g$, so $I = kg$.
(ii) If $g \in G(C)$, then the map $\lambda \to \lambda g$ from k to C is a coalgebra morphism. Conversely, to any coalgebra morphism $\alpha : k \to C$ we associate the element $g = \alpha(1) \in G(C)$. In this way we define a bijective correspondence as required.
(iii) Let $g \in G(C)$ and let $\alpha : k \to C$ be the coalgebra morphism associated in (ii) to g. Then $\alpha^* : C^* \to k^* \simeq k$ is a continuous algebra morphism. Conversely, if $\beta : C^* \to k$ is a continuous algebra morphism, then $I = Ker(\beta) = \beta^{-1}(\{0\})$ is closed, so $I^{\perp\perp} = I$. Also $I^{\perp}$ is a subcoalgebra of dimension 1 of C, so $I^{\perp} = kg$ for some $g \in G(C)$. This implies that $I = (kg)^{\perp}$. We show that $\beta(c^*) = c^*(g)$ for any $c^* \in C^*$. If $c^* \in I$ we clearly have $\beta(c^*) = c^*(g) = 0$. For $c^* = \varepsilon$ we have $\beta(c^*) = c^*(g) = 1$. These imply that $\beta(c^*) = c^*(g)$ for any $c^* \in I + k\varepsilon = C^*$ (since I has codimension 1 and $\varepsilon \notin I$). ∎

A coalgebra is called pointed if any simple subcoalgebra has dimension 1. By the previous proposition, we see that for a pointed coalgebra C, we have $Corad(C) = kG(C)$.

Exercise 5.5.2 *Let $f : C \to D$ be a surjective morphism of coalgebras. Show that if C is pointed, then D is pointed and $Corad(D) = f(Corad(C))$.*

Let C be a coalgebra such that $G(C) \neq \emptyset$. For any $g \in G(C)$ we define the sets

$$L_g = \{c^* \in C^* | d^*c^* = d^*(g)c^* \text{ for any } d^* \in C^*\}$$

$$R_g = \{c^* \in C^* | c^*d^* = d^*(g)c^* \text{ for any } d^* \in C^*\}$$

If $f \in C^*$ and $c^* \in L_g$ we have

$$\begin{aligned} d^*(fc^*) &= f(g)d^*c^* \\ &= f(g)d^*(g)c^* \end{aligned}$$

$$\begin{aligned} &= d^*(g)(f(g)c^*) \\ &= d^*(g)(fc^*) \end{aligned}$$

so $fc^* \in L_g$. Also $d^*(c^*f) = d^*c^*f = d^*(g)c^*f$, so $c^*f \in L_g$, showing that L_g is a two-sided ideal of C^*. Similarly, R_g is a two-sided ideal of C^*.
For any $g \in G(C)$, Proposition 5.5.1 tells that there exists a coalgebra morphism $\alpha_g : k \to C$, $\alpha_g(\lambda) = \lambda g$. Then we can regard k as a left C, right C-bicomodule via α_g, and we denote by ${}_gk$, respectively k_g, the field k regarded as a left C-comodule, respectively as a right C-comodule. A morphism of left C-comodules (or equivalently of right C^*-modules) from C to ${}_gk$ is called a left g-integral. The space $Hom_{C^*}(C,{}_gk)$ is called the space of the left g-integrals. Similarly we define right g-integrals and the space $Hom_{C^*}(C, k_g)$ of right g-integrals.

Proposition 5.5.3 *With the above notation we have $L_g = Hom_{C^*}(C, {}_gk)$ and $R_g = Hom_{C^*}(C, k_g)$. In particular if C is a left and right co-Frobenius coalgebra, then L_g and R_g are two-sided ideals of dimension 1.*
Conversely, if I is a 1-dimensional left (right) ideal of C^*, then there exists $g \in G(C)$ such that $I = L_g$ (respectively $I = R_g$). In particular, 1-dimensional left (right) ideals are two-sided ideals.

Proof: We prove that $L_g = Hom_{C^*}(C, {}_gk)$. Let $c^* \in C^*$. Then $c^* \in Hom_{C^*}(C,{}_gk)$ if and only if $\alpha_g c^* = (I \otimes c^*)\Delta$, where $\alpha_g : k \to C \otimes {}_gk$ is the comodule structure map of ${}_gk$. This is the same with $\sum c^*(c_2)c_1 = c^*(c)g$ for any $c \in C$, which is equivalent to the fact that $u(\sum c^*(c_2)c_1) = u(c^*(c)g)$ for any $u \in C^*$ and any $c \in C$. But $u(\sum c^*(c_2)c_1) = \sum u(c_1)c^*(c_2) = (uc^*)(c)$, and $u(c^*(c)g) = u(g)c^*(c) = (u(g)c^*)(c)$. Thus $c^* \in Hom_{C^*}(C, {}_gk)$ if and only if $uc^* = u(g)c^*$ for any $u \in C^*$, which means exactly that $u \in L_g$.
Assume now that C is left and right co-Frobenius. By Corollary 3.3.11 C is a projective generator in the categories $\mathcal{M}^C$ and ${}^C\mathcal{M}$ (when regarded as a right or left C-comodule). Then $Hom_{C^*}(C,{}_gk) \neq 0$ and $Hom_{C^*}(C, k_g) \neq 0$. Remark 5.4.3 shows that $\dim(Hom_{C^*}(C,{}_gk)) = 1$ and $\dim(Hom_{C^*}(C, k_g)) = 1$, so L_g and R_g have dimension 1.
Let I be a 1-dimensional left ideal of C^*, say $I = kx$. Since I is a left ideal, there exists a k-algebra morphism $f : C^* \to k$ such that $c^*x = f(c^*)x$ for any $c^* \in C^*$. Since the map $c^* \mapsto c^*x$ is continuous we see that $Ker(f)$ is closed in C^*. Then by Proposition 5.5.1 (iii) there exists a coalgebra morphism $\alpha : k \to C$, $\alpha(\lambda) = \lambda g$, where $g \in G(C)$, such that $f = \alpha^*$. Then for any $c^* \in C^*$ we have

$$\begin{aligned} c^*x &= f(c^*)x \\ &= \alpha^*(c^*)x \end{aligned}$$

$$\begin{aligned} &= (c^*\alpha)(1)x \\ &= c^*(g)x \end{aligned}$$

i.e. $x \in L_g$. This shows that $I \subseteq L_g$ and since L_g has dimension 1 we conclude that $I = L_g$. ∎

Assume now that H is a Hopf algebra with nonzero integral. Then $G(H)$ is a group and $1 \in G(H)$ (here 1 means the identity element of the k-algebra H) and for any $g \in G(H)$ we have $g^{-1} = S(g)$, where S is the antipode of H. For any $g \in G(H)$ the maps $u_g, u'_g : H \to H$ defined by $u_g(x) = gx$ and $u'_g(x) = xg$ for any $x \in H$, are coalgebra isomorphisms. Then the dual morphisms $u_g^*, u_g'^* : H^* \to H^*$ are algebra isomorphisms. For any $a^* \in H^*$ and $x \in H$ we have that

$$\begin{aligned} u_g^*(a^*)(x) &= (a^* u_g)(x) \\ &= a^*(gx) \\ &= (a^* \leftharpoonup g)(x) \end{aligned}$$

thus $u_g(a^*) = a^* \leftharpoonup g$. Similarly $u_g'^*(a^*) = g \rightharpoonup a^*$. It is easy to see that $L_{gh^{-1}} = u_h'^*(L_g) = h \rightharpoonup L_g$, $L_{h^{-1}g} = u_h^*(L_g) = L_g \leftharpoonup h$, $R_{gh^{-1}} = u_h'^*(R_g) = h \rightharpoonup R_g$ and $R_{h^{-1}g} = u_h^*(R_g) = R_g \leftharpoonup h$. In particular by Proposition 5.5.3 there exists $a \in G(H)$ such that $R_a = L_1 = \int_l$. This element is called the *distinguished* grouplike element of H.

Proposition 5.5.4 *With the above notation we have that*
(i) $R_{ag} = L_g = R_{ga}$ for any $g \in G(H)$. In particular a lies in the center of the group $G(H)$.
(ii) $a \rightharpoonup L_g = L_g \leftharpoonup a = R_g$.
(iii) For any nonzero left integral t we have $tS = a \rightharpoonup t$, and $tS^{-1} = t \leftharpoonup a$.

Proof: (i) Since $L_1 = R_a$ we have $g^{-1} \rightharpoonup L_1 = L_g$. On the other hand $g^{-1} \rightharpoonup L_1 = g^{-1} \rightharpoonup R_a = R_{ag}$, so $L_g = R_{ag}$. Similarly $L_g = R_{ga}$. Since $R_{ag} = R_{ga}$ we obtain by Proposition 5.5.3 that $ag = ga$ for any $g \in G(H)$, and this means that a belongs to the center of $G(H)$.
(ii) We know that $a \leftharpoonup L_g = L_{ga^{-1}}$ and $ag^{-1} \rightharpoonup R_a = R_g$. Since $R_a = L_1$ then $ag^{-1} \rightharpoonup R_a = ag^{-1} \rightharpoonup L_1 = L_{ga^{-1}}$. We obtain that $a \rightharpoonup L_g = R_g$. The relation $L_g \leftharpoonup a = R_g$ follows similarly.
(iii) If $x \in H$ is such that $t(x) = 1$, then $a = x \leftharpoonup t$, because for all $h^* \in H^*$ we have $h^*(a) = h^*(a)t(x) = (th^*)(x) = h^*(x \leftharpoonup t)$.
We know from (i) that $a \rightharpoonup t$ is a right integral. So is tS, so by uniqueness there is an $\alpha \in k$ such that $tS = \alpha(a \rightharpoonup t)$. We prove $\alpha = 1$ by applying both sides of the equality to $S^{-1}(x)$. So we want $(a \rightharpoonup t)(S^{-1}(x)) = 1$, and

we compute it

$$\begin{aligned}
(a \rightharpoonup t)(S^{-1}(x)) &= \sum t(S^{-1}(x)t(x_1)x_2) \\
&= \sum t(x_1 t(S^{-1}(x)x_2)) \\
&= \sum t(x_2 t(S^{-1}(x_1)x)) \text{ (by Lemma 5.1.4 for } H^{op}) \\
&= t(x)t(S^{-1}(1)x) \text{ (since } \sum t(x_2)x_1 = t(x)1) \\
&= t(x)^2 = 1
\end{aligned}$$

and the proof is complete. ∎

If H is finite dimensional, and $0 \neq t' \in H$ is a left integral, then for all $h \in H$, $t'h$ is also a left integral and $t'h = \lambda'(h)t'$, λ' a grouplike element in H^*.

Corollary 5.5.5 *For H, λ', t' as above, $\lambda' \rightharpoonup t' = S(t')$.*

Proof: Let G be the Hopf algebra H^*. Identify G^* with H and consider t' as an element of G^*; λ' is itself a grouplike element of G and corresponds to the element g of Proposition 5.5.4 (iii). The statement follows immediately. ∎

Exercise 5.5.6 *Prove Corollary 5.5.5 directly.*

Exercise 5.5.7 *Let H be a Hopf algebra such that the coradical H_0 is a Hopf subalgebra. Show that the coradical filtration $H_0 \subseteq H_1 \subseteq \ldots H_n \subseteq \ldots$ is an algebra filtration, i.e. for any positive integers m, n we have that $H_m H_n \subseteq H_{m+n}$.*

Theorem 5.5.8 *Let H be a co-Frobenius Hopf algebra, and $H_0, H_1, \ldots$ the coradical filtration of H. If $J \subseteq H$ is an injective envelope of $k1$, considered as a left H-comodule, then $JH_0 = H$. Moreover, if H_0 is a Hopf subalgebra of H, then there exists n such that $H_n = H$.*

Proof: Since H_0 is the socle of the left H-comodule H, we can write $H_0 = k1 \oplus M$ for some left H-subcomodule M of H. We know that $H = E(k1) \oplus E(M) = J \oplus E(M)$ (where $E(M)$ is the injective envelope of M). Let $t \neq 0$ be a right integral of H. Then for $h \in E(M)$ we have $t(h)1 = \sum t(h_1)h_2 \in E(M)$, and also $t(h)1 \in J$. Therefore $t(h)1 \in E(M) \cap J = 0$, so $t(h) = 0$. Thus $t(E(M)) = 0$, and then $t(J)$ must be nonzero.
Let $a \in G(H)$ such that $\int_r = \int_l \leftharpoonup a$ (see Proposition 5.5.4). If $JH_0 \neq H$, then aJH_0 is a proper left H-subcomodule of H, so there exists a maximal left H-subcomodule N of H with $aJH_0 \subseteq N$. Then H/N is a simple left comodule, so $N^\perp \simeq (H/N)^*$ is a simple right H-comodule. This shows

that $N^\perp$ is a simple right subcomodule of H^{*rat}. We use the isomorphism of right H-comodules $\phi : H \to H^{*rat}$, $\phi(h) = (t \leftharpoonup a^{-1}) \leftharpoonup h$ (note that $t \leftharpoonup a^{-1}$ is a left integral), and find that there exists a simple right H-subcomodule V of H such that $N^\perp = \phi(V) = (t \leftharpoonup a^{-1}) \leftharpoonup V$. Then $t(a^{-1}NS(V)) = 0$. As a simple subcomodule, V is contained in the (right) socle of H, thus $V \subseteq H_0$. Also, since $\Delta(V) \subseteq V \otimes H$, the counit property shows that there is some $v \in V$ with $\varepsilon(v) \neq 0$. Then

$$1 = \varepsilon(v)^{-1} \sum v_1 S(v_2) \in VS(V) \subseteq H_0 S(V)$$

Now we have $J = a^{-1}aJ \subseteq a^{-1}aJH_0S(V) \subseteq a^{-1}NS(V)$, so $t(J) = 0$, a contradiction. Thus we must have $JH_0 = H$.
Assume that H_0 is a Hopf subalgebra of H. Since $\int_r \neq 0$, J must be finite dimensional, and then there exists n such that $J \subseteq H_n$. Then $H = JH_0 \subseteq H_nH_0 = H_n$ (by Exercise 5.5.7), thus $H = H_n$. ∎

The previous theorem shows that if H is a co-Frobenius Hopf algebra and the trivial left H-comodule k is injective, then $J = k1$ and $H = H_0$, i.e. H is cosemisimple. The following exercise gives a different proof of this fact for an arbitrary Hopf algebra (not necessarily co-Frobenius).

Exercise 5.5.9 *Let H be a Hopf algebra. Show that the following are equivalent.*
(1) H is cosemisimple.
(2) k is an injective right (or left) H-comodule.
(3) There exists a right (or left) integral $t \in H^*$ such that $t(1) = 1$.

Exercise 5.5.10 *Show that in a cosemisimple Hopf algebra H the spaces of left and right integrals are equal (such a Hopf algebra is called* unimodular*), and if t is a left integral with $t(1) = 1$, we have that $t \circ S = t$.*

Remark 5.5.11 *It is easy to see that a Hopf algebra is unimodular if and only if the distinguished grouplike is equal to 1.*

Exercise 5.5.12 *Let H be a Hopf algebra over the field k, K a field extension of k, and $\overline{H} = K \otimes_k H$ the Hopf algebra over K defined in Exercise 4.2.17. Show that if H is cosemisimple over k, then $\overline{H}$ is cosemisimple over K. Moreover, in the case where H has a nonzero integral, show that if $\overline{H}$ is cosemisimple over K, then H is cosemisimple over k.*

The equivalence between (1) and (3) in the following exercise has been already proved in Theorem 5.2.10 (Maschke's theorem for Hopf algebras). We give here a different proof.

Exercise 5.5.13 *Let H be a finite dimensional Hopf algebra. Show that the following are equivalent.*
(1) H is semisimple.
(2) k is a projective left (or right) H-module (with the left H-action on k defined by $h \cdot \alpha = \varepsilon(h)\alpha$).
(3) There exists a left (or right) integral $t \in H^*$ such that $\varepsilon(t) \neq 0$.

5.6 Hopf algebras constructed by Ore extensions

Throughout this section, k will be an algebraically closed field of characteristic 0. In fact, for most of the results we only need that k contains enough roots of unity. We will denote by $\mathbf{Z}^+ = \mathbf{N}^*$ the set of positive integers (non-zero natural numbers).

We construct now the quantum binomial coefficients and prove the quantum version of the binomial formula. Define by recurrence a family of polynomials $(P_{n,i})_{n\geq 1, 0\leq i\leq n}$ in the indeterminate X with integer coefficients as follows. We start with $P_{1,0} = P_{1,0} = 1$. If we assume that we have defined the polynomials $(P_{n,i})_{0\leq i\leq n}$ for some $n \geq 1$, then define $(P_{n+1,i})_{0\leq i\leq n+1}$ by $P_{n+1,0} = P_{n,0}$, $P_{n+1,n+1} = P_{n,n}$, and for any $1 \leq i \leq n$

$$P_{n+1,i}(X) = P_{n,i-1}(X) + X^i P_{n,i}(X)$$

Also, for any positive integer i we denote by $[i]$ the following polynomial $[i] = X^{i-1} + X^{i-2} + \ldots + X + 1$. In fact $[i] = \frac{X^i - 1}{X-1}$ if we regard the polynomial ring $\mathbf{Z}[X]$ as a subring of the field $\mathbf{Q}(X)$ of rational fractions. We also define $[0]$ to be the constant polynomial $[0] = 1$. Now for any positive integer n we define the polynomial $[n]!$ by

$$[n]! = [1] \cdot [2] \cdot \ldots \cdot [n]$$

which is also a polynomial with integer coefficients. We make the convention $[0]! = 1$, a constant polynomial. We can describe now the polynomials $P_{n,i}$ explicitely.

Proposition 5.6.1 *For any positive integer n and any $0 \leq i \leq n$ we have $P_{n,i} = \frac{[n]!}{[i]![n-i]!}$, where the polynomial ring $\mathbf{Z}[X]$ is regarded as a subring of the ring of rational fractions $\mathbf{Q}(X)$.*

Proof: We prove by induction on n that for any $0 \leq i \leq n$ the desired formula holds. For $n = 1$ it is obvious. For passing from n to $n+1$, we first note that for $i = 0$ and for $i = n + 1$ the formula holds by the definition. If $1 \leq i \leq n$, then we have

$$\begin{aligned}
P_{n+1,i}(X) &= P_{n,i-1}(X) + X^i P_{n,i}(X) \\
&= \frac{[n]!}{[i-1]![n-i+1]!} + X^i \frac{[n]!}{[i]![n-i]!} \\
&= \frac{[n]!([i] + X^i[n-i+1])}{[i]![n-i+1]!} \\
&= \frac{[n]!(\frac{X^i-1}{X-1} + X^i \cdot \frac{X^{n-i+1}-1}{X-1})}{[i]![n-i+1]!} \\
&= \frac{[n]!}{[i]![n-i+1]!} \cdot \frac{X^{n+1}-1}{X-1} \\
&= \frac{[n]!}{[i]![n-i+1]!}[n+1] \\
&= \frac{[n+1]!}{[i]![n-i+1]!}
\end{aligned}$$

∎

If q is an element of the field k, we define the element $(i)_q$ of k as being the value of the polynomial $[i]$ at q, i.e. $(i)_q = [i](q)$. Thus $(i)_q = \frac{q^i-1}{q-1}$ if $q \neq 1$, and $(i)_q = i$ if $q = 1$. Also, we define $(n)_q!$ as being the value of $[n]!$ at q, i.e. $(n)_q! = [n]!(q)$. Note that if $q = 1$, then $(n)_q! = n!$, the usual factorial. Finally, we define the q-binomial coefficients $\binom{n}{i}_q$ for any positive integer n and any $0 \leq i \leq n$ by $\binom{n}{i}_q = P_{n,i}(q)$. By Proposition 5.6.1, we have that $P_{n,i} = \frac{[n]!}{[i]![n-i]!}$, and then $\binom{n}{i}_q = \frac{(n)_q!}{(i)_q!(n-i)_q!}$ whenever the denominator of the fraction in the right hand side is nonzero. Nevertheless, we write $\binom{n}{i}_q$ to be $\frac{(n)_q!}{(i)_q!(n-i)_q!}$ in any case, but with the warning that this is a formal notation, and we have to understand in fact $P_{n,i}(q)$ by it. Obviously, if $q = 1$, then $\binom{n}{i}_q$ is the usual $\binom{n}{i}$. The recurrence relation for the polynomials $P_{n,i}$ shows that

$$\binom{n+1}{i}_q = \binom{n}{i-1}_q + q^i \binom{n}{i}_q$$

for any $n \geq 1$ and $1 \leq i \leq n$. The reason for which the $\binom{n}{i}_q$ are called q-binomial coefficients is that they appear in a version of the binomial formula where the two terms of the binomial do not commute, and instead they anticommute by q.

Lemma 5.6.2 *Let a and b two elements of a k-algebra such that $ba = qab$ for some $q \in k$. Then the following assertions hold.*

(i) (The quantum binomial formula) $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i}_q a^{n-i}b^i$ for any positive integer n.

(ii) If q is a primitive n-th root of unity, then $(a+b)^n = a^n + b^n$. ∎

Proof: (i) The proof goes by induction on n. It is obvious for $n = 1$. To pass from n to $n+1$ we have that

$$
\begin{aligned}
& (a+b)^{n+1} = \\
= \; & (a+b)^n(a+b) \\
= \; & \Big(\sum_{i=0}^{n} \binom{n}{i}_q a^{n-i}b^i\Big)(a+b) \quad \text{(induction hypothesis)} \\
= \; & \binom{n}{0}_q a^{n+1} + \binom{n}{n}_q b^{n+1} + \sum_{i=0}^{n}\Big(\binom{n}{i-1}_q a^{n+1-i}b^i + \binom{n}{i}_q a^{n-i}b^i a\Big) \\
= \; & \binom{n+1}{0}_q a^{n+1} + \binom{n+1}{n+1}_q b^{n+1} + \sum_{i=0}^{n}\Big(\binom{n}{i-1}_q a^{n+1-i}b^i + \\
& + q^i\binom{n}{i}_q a^{n-i+1}b^i\Big) \\
= \; & \binom{n+1}{0}_q a^{n+1} + \binom{n+1}{n+1}_q b^{n+1} + \sum_{i=0}^{n} \binom{n+1}{i}_q a^{n+1-i}b^i \\
= \; & \sum_{i=0}^{n+1} \binom{n+1}{i}_q a^{n+1-i}b^i
\end{aligned}
$$

which gives the desired formula for $n+1$.
(ii) Since q is a primitive n-th root of unity we have that $(n)_q = 0$, and $(i)_q \neq 0$ for any $i < n$. The result follows now from the quantum binomial formula. ∎

Remark 5.6.3 *We have seen in the proof of (ii) of Lemma 5.6.2 that if q is a primitive n-th root of unity, then*

$$\binom{n}{1}_q = \binom{n}{2}_q = \ldots = \binom{n}{n-1}_q = 0$$

The converse also holds, i.e. if

$$\binom{n}{1}_q = \binom{n}{2}_q = \ldots = \binom{n}{n-1}_q = 0$$

then q is a primitive n-th root of 1. Indeed, by $\binom{n}{1}_q = 0$ we see that q is a n-th root of 1. If q is not a primitive n-th root, then q is a primitive d-th root of 1 for some divisor d of n with $d < n$. Then $\binom{n}{d}_q \neq 0$, since

$$P_{n,d} = \frac{[n] \cdot [n-1] \cdot \ldots \cdot [n-d+1]}{[d] \cdot [d-1] \cdot \ldots \cdot [1]}$$

and q is not a root of any of the polynomials $[n-1], \ldots, [n-d+1], [d-1], \ldots, [1]$, and also q is a simple root of both $[n]$ and $[d]$. Thus we obtain a contradiction, and conclude that q must be a primitive n-th root of 1. ∎

Recall that for a k-algebra A, an algebra endomorphism φ of A, and a φ-derivation δ of A (i.e. a linear map $\delta : A \to A$ such that $\delta(ab) = \delta(a)b + \varphi(a)\delta(b)$ for all $a, b \in A$), the Ore extension $A[X, \varphi, \delta]$ is $A[X]$ as an abelian group, with multiplication induced by $Xa = \delta(a) + \varphi(a)X$ for all $a \in A$. The following is an obvious extension of the universal property for polynomial rings.

Lemma 5.6.4 *Let $A[X, \varphi, \delta]$ be an Ore extension of A and*

$$i : A \to A[X, \varphi, \delta]$$

the inclusion morphism. Then for any algebra B, any algebra morphism $f : A \to B$ and every element $b \in B$ such that $bf(a) = f(\delta(a)) + f(\varphi(a))b$ for all $a \in A$, there exists a unique algebra morphism $\overline{f} : A[X, \varphi, \delta] \to B$ such that $f(X) = b$ and the following diagram is commutative:

$$\begin{tikzcd}
A \arrow[r, "i"] \arrow[dr, "f"'] & A[X, \phi, \delta] \arrow[d, "\overline{f}"] \\
& B
\end{tikzcd}$$

∎

We construct pointed Hopf algebras by starting with the coradical, forming Ore extensions, and then factoring out a Hopf ideal.

Let $A = kC$ be the group algebra of an abelian group C with the usual Hopf algebra structure, and let C^* be the character group of C, i.e. C^* consists of all group morphisms from C to the multiplicative group $k^* = k - \{0\}$, and the multiplication of C^* is given by $(uv)(g) = u(g)v(g)$ for any $u, v \in C^*$ and $g \in C$.
Let $c_1 \in C$ and $c_1^* \in C^*$ and take the algebra automorphism φ_1 of A

defined by $\varphi_1(g) = c_1^*(g)g$ for all $g \in C$. Consider the Ore extension $A_1 = A[X_1, \varphi_1, \delta_1]$, where $\delta_1 = 0$. Apply Lemma 5.6.4 first with $B = A_1 \otimes A_1, f = (i \otimes i) \cdot \Delta_A, b = c_1 \otimes X_1 + X_1 \otimes 1$ and then with $B = k$, $f = \epsilon_A, b = 0$, to define algebra homomorphisms $\Delta : A_1 \to A_1 \otimes A_1$ and $\epsilon : A_1 \to k$ by

$$\Delta(X_1) = c_1 \otimes X_1 + X_1 \otimes 1 \text{ and } \epsilon(X_1) = 0. \tag{5.5}$$

It is easily checked that Δ and ϵ define a bialgebra structure on A_1. The antipode S of A extends to an antipode on A_1 by $S(X_1) = -c_1^{-1}X_1$.
Next, let $c_2^* \in C^*, \gamma_{12} \in k^*$, and let $\varphi_2 \in Aut(A_1)$ be defined by,

$$\varphi_2(g) = c_2^*(g)g \text{ for } g \in C, \quad \varphi_2(X_1) = \gamma_{12}X_1.$$

We seek a φ_2-derivation δ_2 of A_1, such that δ_2 is zero on kC and $\delta_2(X_1) \in kC$. We want the Ore extension $A_2 = A_1[X_2, \varphi_2, \delta_2]$ to have a Hopf algebra structure with X_2 a $(1, c_2)$-primitive for some $c_2 \in C$, i.e. $\Delta(X_2) = c_2 \otimes X_2 + X_2 \otimes 1$. Then

$$X_2X_1 = \delta_2(X_1) + \gamma_{12}X_1X_2. \tag{5.6}$$

Applying Δ to both sides of (5.6), we see that

$$\gamma_{12} = c_1^*(c_2)^{-1} = c_2^*(c_1) \text{ and } \Delta(\delta_2(X_1)) = c_1c_2 \otimes \delta_2(X_1) + \delta_2(X_1) \otimes 1.$$

Thus $\delta_2(X_1)$ is a $(1, c_1c_2)$-primitive in kC and so we must have

$$\delta_2(X_1) = b_{12}(c_1c_2 - 1)$$

for some scalar b_{12}. If $c_1c_2 - 1 = 0$, then we define b_{12} to be 0. If $b_{12} = 0$, then δ_2 is clearly a φ_2-derivation. Suppose that $\delta_2 \neq 0$. In this case it remains to check that δ_2 is a φ_2-derivation of A_1. In order that δ_2 be well defined we must have, for all $g \in C$,

$$\begin{aligned} \delta_2(gX_1) &= \varphi_2(g)\delta_2(X_1) \\ &= \delta_2(c_1^*(g)^{-1}X_1g) \\ &= c_1^*(g)^{-1}\delta_2(X_1)g \end{aligned}$$

Thus $\varphi_2(g) = c_2^*(g)g = c_1^*(g)^{-1}g$ and therefore $c_1^*c_2^* = 1$ and

$$\gamma_{12} = c_1^*(c_2)^{-1} = c_2^*(c_2) = c_2^*(c_1) = c_1^*(c_1)^{-1}$$

Now we compute

$$\begin{aligned} \delta_2(X_1^2) &= \delta_2(X_1)X_1 + \varphi_2(X_1)\delta_2(X_1) \\ &= b_{12}(1 + c_1^*(c_1))c_1c_2X_1 - b_{12}(1 + c_1^*(c_1)^{-1})X_1 \end{aligned}$$

and, by induction, we see that for every positive integer r, we have

$$\delta_2(X_1^r) = b_{12}(\sum_{i=0}^{r-1} c_1^*(c_1)^i)c_1c_2X_1^{r-1} - b_{12}(\sum_{i=0}^{r-1} c_1^*(c_1)^{-i})X_1^{r-1} \tag{5.7}$$

A straightforward but tedious computation now ensures that for $g, g' \in C$,

$$\delta_2(gX_1^r g' X_1^p) = \delta_2(gX_1^r)g'X_1^p + \varphi_2(gX_1^r)\delta_2(g'X_1^p)$$

and our definition of $A_2 = A_1[X_2, \varphi_2, \delta_2]$ is complete.
Summarizing, A_2 is a Hopf algebra with generators $g \in C$, X_1, X_2, such that the elements of C are commuting grouplikes, X_j is a $(1, c_j)$-primitive and the following relations hold:

$$gX_j = c_j^*(g)^{-1}X_jg \text{ and } X_2X_1 - \gamma_{12}X_1X_2 = b_{12}(c_1c_2 - 1),$$

$$\text{where } \gamma_{12} = c_1^*(c_2)^{-1} = c_2^*(c_1),$$

and, if $\delta_2(X_1) \neq 0$,

$$c_1^*c_2^* = 1 \text{ and } \gamma_{12} = c_1^*(c_1)^{-1} = c_1^*(c_2)^{-1} = c_2^*(c_1) = c_2^*(c_2).$$

We continue forming Ore extensions. Define an automorphism φ_j of A_{j-1} by $\varphi_j(g) = c_j^*(g)g$ where $c_j^* \in C^*$, and $\varphi_j(X_i) = c_j^*(c_i)X_i$ where $c_i \in C$, and X_i is a $(1, c_i)$-primitive. The derivation δ_j of A_{j-1} is 0 on kC and $\delta_j(X_i) = b_{ij}(c_ic_j - 1)$. If $c_ic_j = 1$, we define $b_{ij} = 0$. We write X^p for $X_1^{p_1} \dots X_t^{p_t}$ where $p \in \mathbf{N}^t$. After t steps, we have a Hopf algebra A_t.

Definition 5.6.8 *A_t is the Hopf algebra generated by the elements $g \in C$ and $X_j, j = 1, \dots, t$ where*
i) the elements of C are commuting grouplikes;
ii) the X_j are $(1, c_j)$-primitives;
iii) $X_jg = c_j^*(g)gX_j$;
iv) $X_jX_i = c_j^*(c_i)X_iX_j + b_{ij}(c_ic_j - 1)$ for $1 \leq i < j \leq t$;
v) $c_i^*(c_j)c_j^*(c_i) = 1$ for $j \neq i$;
vi) If $b_{ij} \neq 0$ then $c_i^*c_j^* = 1$.
vii) If $c_ic_j = 1$, then $b_{ij} = 0$.
The antipode of A_t is given by $S(g) = g^{-1}$ for $g \in G$ and $S(X_j) = -c_j^{-1}X_j$. ∎

The relations show that A_t has basis $\{gX^p | g \in C, \ p \in \mathbf{N}^t\}$. Since for $q_j = c_j^*(c_j)$,

$$(X_j \otimes 1)(c_j \otimes X_j) = q_j(c_j \otimes X_j)(X_j \otimes 1),$$

then, for $n \in \mathbf{Z}^+$, $\Delta(X_j^n) = \Delta(X_j)^n = (c_j \otimes X_j + X_j \otimes 1)^n$, and expansion of this power follows the rules in Lemma 5.6.2. For $g \in C$, $p = (p_1, \ldots, p_t) \in \mathbf{N}^t$,

$$\Delta(gX_1^{p_1} \ldots X_t^{p_t}) = \Delta(gX^p) = \sum_d \alpha_d g c_1^{d_1} c_2^{d_2} \ldots c_t^{d_t} X^{p-d} \otimes gX^d, \qquad (5.9)$$

where $d = (d_1, \ldots, d_t) \in \mathbf{Z}^t$, the j-th entry d_j in the t-tuple d ranges from 0 to p_j, and the α_d are scalars resulting from the q-binomial expansion described in Lemma 5.6.2 and the commutation relations. In particular, for $1 \leq j \leq t$, $n \in \mathbf{Z}^+$,

$$\Delta(X_j^n) = \sum_{i=0}^{n} \binom{n}{i}_{q_j} c_j^i X_j^{n-i} \otimes X_j^i. \qquad (5.10)$$

Proposition 5.6.11 *The Hopf algebra A_t has the following properties:*

(i) The term, $(A_t)_n$, in the coradical filtration of A_t is spanned by gX^p, $g \in C$, $p \in \mathbf{N}^t$, $p_1 + \ldots + p_t \leq n$. In particular, A_t is pointed with coradical kC.

(ii) The Hopf algebra A_t does not have nonzero integrals.

Proof: (i) An induction argument using Equation (5.9) shows that for all n,

$$< gX^p | g \in C,\ p \in \mathbf{N}^t,\ p_1 + \ldots + p_t \leq n > \subseteq \wedge^{(n+1)} kC.$$

Thus, $\wedge^{(\infty)} kC = A_t$ and by Exercise 3.1.12 $Corad(A_t) \subseteq kC$. Since kC is a cosemisimple coalgebra, it is exactly the coradical of A_t.

(ii) This follows from Theorem 5.5.8, since $(A_t)_0 = kC$ is a Hopf subalgebra and the coradical filtration is infinite. ∎

Exercise 5.6.12 *Give a different proof for the fact that A_t does not have nonzero integrals, by showing that the injective envelope of the simple right A_t-comodule kg, $g \in C$, is infinite dimensional.*

In order to obtain a Hopf algebra with nonzero integral, we factor A_t by a Hopf ideal.

Lemma 5.6.13 *Let $n_1, n_2, \ldots, n_t \geq 2$ and $a = (a_1, \ldots, a_t) \in \{0, 1\}^t$. The ideal $J(a)$ of A_t generated by*

$$(X_1^{n_1} - a_1(c_1^{n_1} - 1), \ldots, X_t^{n_t} - a_t(c_t^{n_t} - 1))$$

is a Hopf ideal if and only if $q_j = c_j^*(c_j)$ is a primitive n_j-th root of unity for any $1 \leq j \leq t$.

Proof: Since $c_j^{n_j}-1$ is a $(1, c_j^{n_j})$-primitive, it follows that $X_j^{n_j}-a_j(c_j^{n_j}-1)$ is a $(1, c_j^{n_j})$-primitive if and only if so is $X_j^{n_j}$. By (5.10) and Remark 5.6.3, this occurs if and only if $\binom{n_j}{k}_{q_j}=0$ for every $0<k<n_j$, i.e. if and only if q_j is a primitive n_j-th root of unity. Moreover, since $S(X_j)=-c_j^{-1}X_j$, induction on n shows that

$$S(X_j^n)=(-1)^n q_j^{-n(n-1)/2} c_j^{-n} X_j^n.$$

Now, since $q_j^{n_j}=1$, checking the cases n_j even and n_j odd, we see that $(-1)^{n_j} q_j^{-n_j(n_j-1)/2}=-1$ and hence

$$S(X_j^{n_j}-a_j(c_j^{n_j}-1))=-c_j^{-n_j}(X_j^{n_j}-a_j(c_j^{n_j}-1))$$

for $1\le j\le t$, so that the ideal $J(a)$ is invariant under the antipode S, and is thus a Hopf ideal. ∎

By Lemma 5.6.13, $H=A_t/J(a)$ is a Hopf algebra. However the coradical may be affected by taking this quotient. Since we want H to be a pointed Hopf algebra with coradical kC, some additional restrictions are required. We denote by x_i the image of X_i in H and write x^p for $x_1^{p_1}\dots x_t^{p_t}, p=(p_1,\dots,p_t)\in \mathbf{N}^t$.

Proposition 5.6.14 *Assume $J(a)$ as in Lemma 5.6.13 is a Hopf ideal. Then $J(a)\cap kC=0$ if and only if for each i either $a_i=0$ or $(c_i^*)^{n_i}=1$. If this is the case then $\{gx^p|g\in C, p\in \mathbf{N}^t, 0\le p_j\le n_j-1\}$ is a basis of $A_t/J(a)$.*

Proof: By Lemma 5.6.13, we know that $J(a)$ is a Hopf ideal if and only if $q_i=c_i^*(c_i)$ is a primitive n_i-th root of unity for $1\le i\le t$. Now suppose that $J(a)\cap kC=0$. Since

$$(X_i^{n_i}-a_i(c_i^{n_i}-1))g=c_i^*(g)^{n_i}g(X_i^{n_i}-c_i^*(g)^{-n_i}a_i(c_i^{n_i}-1))$$

is in $J(a)$ for every $g\in C$, it follows that

$$X_i^{n_i}-c_i^*(g)^{-n_i}a_i(c_i^{n_i}-1)\in J(a)$$

But then for every $g\in C$, both $a_i(1-c_i^*(g)^{-n_i})(c_i^{n_i}-1)$ and $(1-c_i^*(g)^{-n_i})X_i^{n_i}$ are in $J(a)$. If $a_i\ne 0$, which by our convention implies that $c_i^{n_i}-1\ne 0$, then we must have $c_i^*(g)^{n_i}=1$ for all g, and thus $c_i^{*n_i}=1$.

Conversely, assume that $c_i^{*n_i}=1$ whenever $a_i\ne 0$. By Definition 5.6.8 (iii), $X_i^{n_i}g=c_i^*(g)^{n_i}gX_i^{n_i}$. In particular, $X_i^{n_i}g=gX_i^{n_i}$ if $a_i\ne 0$. Also, if

$i < j$ then by (5.7),

$$\begin{aligned} X_j X_i^{n_i} &= \varphi_j(X_i^{n_i})X_j + \delta_j(X_i^{n_i}) \\ &= c_j^*(c_i)^{n_i} X_i^{n_i} X_j + b_{ij}(\sum_{t=0}^{n_i-1} c_i^*(c_i)^t) c_i c_j X_i^{n_i-1} \\ &\quad -b_{ij}(\sum_{t=0}^{n_i-1} c_i^*(c_i)^{-t}) X_i^{n_i-1} \end{aligned}$$

So, if $b_{ij} = 0$, then $X_j X_i^{n_i} = c_j^*(c_i)^{n_i} X_i^{n_i} X_j$, where $c_j^*(c_i)^{n_i} = c_i^*(c_j)^{-n_i} = 1$ if $a_i \neq 0$. If $b_{ij} \neq 0$ then $c_i^* c_j^* = 1$, hence $c_i^*(c_i)$ is a primitive n_i-th root of unity, so that $X_j X_i^{n_i} = X_i^{n_i} X_j$. A similar argument works for $i > j$. Thus, $X_i^{n_i}$ is a central element of A_t if $a_i \neq 0$. It follows that

$$X_j(X_i^{n_i} - a_i(c_i^{n_i} - 1)) = c_j^*(c_i)^{n_i}(X_i^{n_i} - a_i(c_i^{n_i} - 1))X_j,$$

so that $J(a)$ is equal to the left ideal generated by $\{X_j^{n_j} - a_j(c_i^{n_j} - 1) | 1 \leq j \leq t\}$, and A_t is a free left module with basis $\{X^p | 0 \leq p_j \leq n_j - 1\}$ over the subalgebra B generated by C and $X_1^{n_1}, \ldots, X_t^{n_t}$. We now show that no nonzero linear combination of elements of the form gX^p, $p \in \mathbf{N}^t$, $0 \leq p_j \leq n_j - 1$ lies in $J(a)$. Otherwise there exist $f_j \in A_t$, $1 \leq j \leq t$, not all zero, such that

$$\sum_{1 \leq j \leq t} (X_j^{n_j} - a_j(c_j^{n_j} - 1))f_j = \sum \alpha_{g,p} g X^p,$$

where in the second sum $g \in C$, $p \in \mathbf{N}^t$, $0 \leq p_j \leq n_j - 1$. Since A_t is a free left B-module with basis $\{X^p | 0 \leq p_j \leq n_j - 1\}$, each f_j can be expressed in terms of this basis, and we find that

$$\sum_{1 \leq j \leq t} (X_j^{n_j} - a_j(c_j^{n_j} - 1))F_j \in kC - \{0\}$$

for some $F_j \in B$. Now, B is isomorphic to the algebra R obtained from kC by a sequence of Ore extensions with zero derivations in the indeterminates $Y_i = X_i^{n_i}$, so that $Y_i g = c_i^{*n_i}(g) g Y_i$ and $Y_j Y_i = c_j^{*n_j}(c_i^{n_i}) Y_i Y_j$. Thus, we have

$$\sum_{1 \leq j \leq t} (Y_j - a_j(c_j^{n_j} - 1))G_j \in kC - \{0\}$$

for some $G_j \in R$. It follows from Lemma 5.6.4 by induction on the number of indeterminates that there exists a kC-algebra homomorphism $\theta : R \to kC$ such that $\theta(Y_j) = c_j^{n_j} - 1$ if $a_j \neq 0$ and $\theta(Y_j) = 0$ otherwise. Then $\theta(\sum_{1 \leq j \leq t}(Y_j - a_j(c_j^{n_j} - 1))G_j) = 0$, a contradiction. ∎

From now on, we assume that $n_j \geq 2$, $q_j = c_j^*(c_j)$ is a primitive n_j-th root of 1, and $c_j^{*n_j} = 1$ whenever $a_j \neq 0$, and we study the new Hopf algebra $H = A_t/J(a)$. We have shown that the following defines a Hopf algebra structure on H.

Definition 5.6.15 *Let $t \geq 1$, C an abelian group, $n = (n_1, \dots, n_t) \in \mathbf{N}^t, c = (c_j) \in C^t, c^* = (c_j^*) \in C^{*t}$, $a \in \{0,1\}^t$, $b = (b_{ij})_{1 \leq i < j \leq t} \subseteq k$ such that the following conditions are satisfied.*
- $c_i^*(c_i)$ is a primitive n_i-th root of unity for any i.
- $c_i^*(c_j) = c_j^*(c_i)^{-1}$ for any $i \neq j$.
- If $a_i = 1$, then $(c_i^*)^{n_i} = 1$.
- If $c_i^{n_i} = 1$, then $a_i = 0$.
- $b_{ij} = -c_i^*(c_j)b_{ji}$ for any i, j.
- If $b_{ij} \neq 0$, then $c_i^* c_j^* = 1$.
- If $c_i c_j = 1$ then $b_{ij} = 0$.
Define $H = A_t/J(a) = H(C, n, c, c^*, a, b)$ to be the Hopf algebra generated by the commuting grouplike elements $g \in C$, and the $(1, c_j)$-primitives $x_j, 1 \leq j \leq t$, subject to the relations

$$x_j g = c_j^*(g) g x_j, \; x_j^{n_j} = a_j(c_j^{n_j} - 1)$$

$$x_i x_j = c_i^*(c_j) x_j x_i + b_{ji}(c_j c_i - 1)$$

for $1 \leq j < i \leq t$ The coalgebra structure is given by

$$\Delta(g) = g \otimes g, \; \varepsilon(g) = 1 \;\; \text{for } g \in C$$

$$\Delta(x_i) = c_i \otimes x_i + x_i \otimes 1, \;\; \text{for } 1 \leq i \leq t$$

∎

Remark 5.6.16 *i) If $a_i = 0$ for all i, we write $a = 0$. Similarly if $b_{ij} = 0$ for all $i < j$, we write $b = 0$. If $t = 1$ so that no nonzero derivation occurs, we also write $b = 0$.*

ii) If $a = 0$ and $b = 0$, then we write $H = H(C, n, c, c^*)$ instead of $H(C, n, c, c^*, 0, 0)$.

iii) If in Definition 5.6.15, the a_i's were arbitrary elements of k, then a simple change of variables would reduce to the case where the a_i's are 0 or 1.
iv) Since the elements b_{ii} do not appear in the defining relations for

$$H(C, n, c, c^*, a, b),$$

we always take them to be zero. ∎

Remark 5.6.17 *In order to construct $H(C,n,c,c^*,a,b)$, it suffices to have c^* and c such that $c_i^*(c_i)$ is a root of unity not equal to 1, and $c_i^*(c_j)c_j^*(c_i) = 1$ for $i \neq j$. Then n_i is the order of $c_i^*(c_i)$, and we choose a and b such that $a_i = 0$ whenever $c_i^{n_i} = 1$, $a_i = 0$ whenever $c_i^{*n_i} \neq 1$, $b_{ij} = 0$ whenever $c_i c_j = 1$, and $b_{ij} = 0$ whenever $c_j^* c_i^* \neq 1$. The remaining a_i's and b_{ij}'s are arbitrary.* ∎

By Proposition 5.6.14, $\{gx^p | g \in C,\ p \in \mathbf{N}^t,\ 0 \leq p_j \leq n_j - 1\}$ is a basis for H. As in Equation (5.9), comultiplication on a general basis element is given by

$$\Delta(gx^p) = \sum_d \alpha_d g c_1^{d_1} c_2^{d_2} \dots c_t^{d_t} x^{p-d} \otimes gx^d, \tag{5.18}$$

where $d = (d_1, \dots, d_t) \in \mathbf{Z}^t$ with $0 \leq d_j \leq p_j$. Here the scalars α_d are nonzero products of q_j-binomial coefficients and powers of $c_j^*(c_i)$.

In particular, for $n \in \mathbf{Z}^+$,

$$\Delta(x_j^n) = \sum_{0 \leq d \leq n} \binom{n}{d}_{q_j} c_j^d x_j^{n-d} \otimes x_j^d. \tag{5.19}$$

Proposition 5.6.20 *Let $H = H(C,n,c,c^*,a,b)$. Then H is pointed and the $(r+1)$st term in the coradical filtration of H is $H_r = < gx^p | g \in C,\ p \in \mathbf{N}^t,\ p_1 + \ldots + p_t \leq r >$. In particular $H = H_n$ where $n = n_1 + \ldots + n_t - t$ so that the coradical filtration has $n_1 + \ldots + n_t - t + 1$ terms.*

Proof. The proof is similar to the proof of Proposition 5.6.11. The second part follows from the fact that the α_d are nonzero. ∎

Unlike A_t, the Hopf algebra H has nonzero integrals. We compute the left and right integrals in H^* explicitely. For $g \in C$, and $w = (w_1, \dots, w_t) \in \mathbf{Z}^t$, let $E_{g,w} \in H^*$ be the map taking gx^w to 1 and all other basis elements to 0.

Proposition 5.6.21 *The Hopf algebra $H = H(C,n,c,c^*,a,b)$ has nonzero integrals. The space of left integrals in H^* is $kE_{l,n-1}$, where $l = c_1^{1-n_1} c_2^{1-n_2} \dots c_t^{1-n_t} = \prod_{j=1}^t c_j^{-(n_j-1)}$, and where $n-1$ is the t-tuple $(n_1 - 1, \dots, n_t - 1)$. The space of right integrals for H is $kE_{1,n-1}$ where 1 denotes the identity in C.*

Proof. We show that $E_{l,n-1}$ is a left integral by evaluating $h^* E_{l,n-1}$ for $h^* \in H^*$. This is nonzero only on elements $z \otimes lx^{n-1}$ and such an element can only occur as a summand in

$$\Delta(\prod_{j=1}^{t}(c_j^{-1}x_j)^{n_j-1}) = \Delta(\gamma l x^{n-1})$$

where $\gamma \in k^*$. Now $h^* E_{l,n-1}(lx^{n-1}) = h^*(1)E_{l,n-1}(lx^{n-1})$.

Similarly $x^{n-1} \otimes z$ only occurs in $\Delta(x^{n-1})$. Since $\Delta(x^{n-1}) = x^{n-1} \otimes 1 + \dots$, thus $E_{1,n-1}h^* = E_{1,n-1}h^*(1)$. ∎

Corollary 5.6.22 *H is unimodular if and only if $l = 1$.* ∎

If G is a group and $g = (g_1, \dots, g_t) \in G^t$, we write g^{-1} for the t-tuple $(g_1^{-1}, \dots, g_t^{-1})$.

Example 5.6.23 (i) If $H = H(C, n, c, c^*, a, b)$ then H^{op} and H^{cop} are also of this type. Indeed, $H^{op} \cong H(C, n, c, c^{*-1}, a, b')$, where $b'_{ij} = -c_j^*(c_i)b_{ij}$ for $i < j$.

Also $H^{cop} \cong H(C, n, c^{-1}, c^*, a, b'')$; the isomorphism is given by the map f taking g to g and x_j to $z_j = -c_j^{-1}x_j$. Then z_j is a $(1, c_j^{-1})$-primitive and, using the fact that $(-1)^{n_j} q_j^{-n_j(n_j-1)/2} = -1$ where q_j is a primitive n_j-th root of 1, we see that its n_j-th power is either 0 or $c_j^{-n_j} - 1$. The last parameter, b'', is given by $b''_{ij} = -c_j^*(c_i)b_{ij}$ for $i < j$.

(ii) In particular if $H = H(C, n, c, c^*)$ then

$$H^{op} \cong H(C, n, c, c^{*-1}) \text{ and } H^{cop} \cong H(C, n, c^{-1}, c^*).$$

(iii) The Taft Hopf algebras, in particular Sweedler's 4-dimensional Hopf algebra, are of this form. ∎

Exercise 5.6.24 *Let A be the algebra generated by an invertible element a and an element b such that $b^n = 0$ and $ab = \lambda ba$, where λ is a primitive $2n$-th root of unity. Show that A is a Hopf algebra with the comultiplication and counit defined by*

$$\Delta(a) = a \otimes a,\ \Delta(b) = a \otimes b + b \otimes a^{-1}, \varepsilon(a) = 1, \varepsilon(b) = 0$$

Also show that A has nonzero integrals and it is not unimodular.

Exercise 5.6.25 *Let H be the Hopf algebra with generators $c, x_1, \dots, x_t$ subject to relations*

$$c^2 = 1, \quad x_i^2 = 0, \quad x_i c = -c x_i, \quad x_j x_i = -x_i x_j,$$

$$\Delta(c) = c \otimes c, \quad \Delta(x_i) = c \otimes x_i + x_i \otimes 1.$$

Show that H is a pointed Hopf algebra of dimension 2^{t+1} with coradical of dimension 2.

The following exercise shows that our assumption that the derivations are zero on kC is not unreasonable.

Exercise 5.6.26 *Let ϕ be an automorphism of kC of the form $\phi(g) = c^*(g)g$ for $g \in C$, and assume that $c^*(g) \neq 1$ for any $g \in C$ of infinite order. Show that if δ is a ϕ-derivation of kC such that the Ore extension $(kC)[Y, \phi, \delta]$ has a Hopf algebra structure extending that of kC with Y a $(1, c)$-primitive, then there is a Hopf algebra isomorphism $(kC)[Y, \phi, \delta] \simeq (kC)[X, \phi]$.*

We now classify Hopf algebras of the form $H(C, n, c, c^*, a, 0)$, i.e. they are constructed by using Ore extensions with zero derivations. Suppose $H = H(C, n, c, c^*, a, 0) \simeq H' = H(C', n', c', c^{*'}, a', 0)$ and write g, x_i (g', x_i') for the generators of H (H' respectively). Let f be a Hopf algebra isomorphism from H to H'. Since the coradicals must be isomorphic, we may assume that $C = C'$, and the Hopf algebra isomorphism induces an automorphism of C. Also by Proposition 5.6.20, $t = t'$. If π is a permutation of $\{1, \ldots, t\}$ and $v \in \mathbf{Z}^t$, we write $\pi(v)$ for $(v_{\pi(1)}, \ldots, v_{\pi(t)})$.

Theorem 5.6.27 *Let*

$$H = H(C, n, c, c^*, a, 0)$$

and

$$H' = H(C', n', c', c^{*'}, a', 0)$$

be Hopf algebras as described above. Then $H \cong H'$ if and only if $C = C'$ (in fact we should write $C \simeq C'$, but we take for simplicity $C = C'$), $t = t'$ and there is an automorphism f of C and a permutation π of $\{1, \ldots, t\}$ such that for $1 \leq i \leq t$

$$n_i = n'_{\pi(i)}, f(c_i) = c'_{\pi(i)}, c_i^* = c^{*'}_{\pi(i)} \circ f, \text{ and } a_i = a'_{\pi(i)}.$$

Proof. We have seen that $C \simeq C'$ as the group of grouplike elements in the two Hopf algebras. Assume that $C = C'$.
Let $I = \{i | 1 \leq i \leq t,\ c_i = c_1, c_i^* = c_1^*\}$ and let

$$\tilde{J} = \{j | 1 \leq j \leq t,\ c_j' = f(c_1)\} \supseteq J = \{j | 1 \leq j \leq t,\ j \in \tilde{J}, c_j^{*'} \circ f = c_1^*\}.$$

Note that since $c_i^*(c_i)$ is a primitive n_i-th root of 1 and for $i \in I$, $c_i^*(c_i) = c_1^*(c_1)$, then $n_i = n_1$ for $i \in I$. Similarly, since for $j \in J$, $c_j^{*'}(c_j') = c_j^{*'}(f(c_1)) = c_1^*(c_1)$, $n_j' = n_1$ for $j \in J$. Let L be the Hopf subalgebra of H generated by C and $\{x_i | i \in I\}$ and L' the Hopf subalgebra of H' generated by C and $\{x_j' | j \in J\}$.

Since x_1 is a $(1, c_1)$-primitive, $f(x_1)$ is a $(1, f(c_1)$-primitive and so

$$f(x_1) = \alpha_0(f(c_1) - 1) + \sum_{i=1}^{r} \alpha_i x'_{j_i} \text{ with } \alpha_i \in k, j_i \in \tilde{J}.$$

Then, since $gx_1 = c_1^*(g)^{-1}x_1 g$ for all $g \in C$, we see that $\alpha_0 = 0$, and

$$\begin{aligned}\sum_{i=1}^{r} f(g)\alpha_i x'_{j_i} &= \sum_{i=1}^{r} \alpha_i c_1^*(g)^{-1} x'_{j_i} f(g) \\ &= \sum_{i=1}^{r} \alpha_i c_1^*(g)^{-1} c_{j_i}^{*'}(f(g)) f(g) x'_{j_i}\end{aligned}$$

and thus $\alpha_i = 0$ for any i for which $c_1^* \neq c_{j_i}^{*'} \circ f$. Thus $f(L) \subseteq L'$. The same argument using f^{-1} shows that $f^{-1}(L') \subseteq L$ and so $f(L) = L'$.

If $L \neq H$, we repeat the argument for M, the Hopf subalgebra of H generated by C and the set $\{x_i | c_i = c_p, c_i^* = c_p^*\}$ where x_p is the first element in the list $x_2, \ldots, x_t$ which is not in L. Continuing in this way, we see that there exists a permutation σ such that

$$n_i = n'_{\sigma(i)}, f(c_i) = c_{\sigma(i)}, c_i^* = c_{\sigma(i)}^{*'} \circ f.$$

It remains to find π such that $a_i = a'_{\pi(i)}$. First suppose $n_1 > 2$. Then $I = \{1\}$. For if $p \in I$, $p \neq 1$, then

$$c_1^*(c_1) = c_p^*(c_1) = c_1^*(c_p)^{-1} = c_1^*(c_1)^{-1}$$

and $c_1^*(c_1)^2 = 1$, a contradiction. Similarly $J = \{\sigma(1)\}$. Hence $f(x_1) = \alpha x'_{\sigma(1)}$ for some nonzero scalar α, and the relation $x_1^{n_1} = a_1(c_1^{n_1} - 1)$ implies $\alpha^{n_1} {x'}_{\sigma(1)}^{n'_{\sigma(1)}} = a_1({c'}_{\sigma(1)}^{n_1} - 1)$, so that $a'_{\sigma(1)} = a_1$.

Next suppose $n_1 = 2$. Let $I_1 = \{i \in I | a_i = 1\}$ and $J_1 = \{j \in J | a_{j'} = 1\}$. For any $i \in I$, there exist $\alpha_{ij} \in k$ such that $f(x_i) = \sum_{j \in J} \alpha_{ij} x'_j$. As above, for all $i \in I$, $c_i^*(c_i) = -1$ (for all $j \in J$, $c_j^{*'}(c'_j) = -1$) and thus the x_i (respectively the x'_j) anticommute. If $i \in I_1$, f applied to $x_i^2 = c_1^2 - 1$ yields $\sum_{j \in J_1} \alpha_{ij}^2 = 1$. On the other hand, comparing $f(x_i x_k)$ and $f(x_k x_i)$ for $i, k \in I_1$, $i \neq k$, we see that

$$\sum_{j \in J_1} \alpha_{ij}\alpha_{kj} = -\sum_{j \in J_1} \alpha_{kj}\alpha_{ij}$$

and thus $\sum_{j \in J_1} \alpha_{ij}\alpha_{kj} = 0$.

This implies that the vectors $B_i \in k^{J_1}$, defined by $B_i = (\alpha_{ij})_{j \in J_1}$ for $i \in I_1$, form an orthonormal set in k^{J_1} under the ordinary dot product. Thus the space k^{J_1} contains at least $|I_1|$ independent vectors and so $|J_1| \geq |I_1|$. The reverse inequality is proved similarly. Now define π to be a refinement of the permutation σ such that for $i \in I_1, \pi(i) \in J_1$ and then $a_i = a'_{\pi(i)}$ for all $i \in I$.

Conversely, let f be an automorphism of C and let π be a permutation of $\{1, 2, \ldots, t\}$ such that for all $1 \leq i \leq t$,

$$n_i = n'_{\pi(i)}, f(c_i) = c'_{\pi(i)}, c_i^* = c^{*'}_{\pi(i)} \circ f, \text{ and } a_i = a'_{\pi(i)}.$$

Extend f to a Hopf algebra isomorphism from H to H' by $f(x_i) = x'_{\pi(i)}$. If we note that

$$c^{*'}_{\pi(i)}(c'_{\pi(j)}) = c^{*'}_{\pi(i)}(f(c_j)) = c_i^*(c_j)$$

the rest of the verification that f induces a Hopf algebra isomorphism is straightforward. ∎

Note that in the proof above, it was shown that if $n_k > 2$, then $|I| = |J| = 1$ where $I = \{i | 1 \leq i \leq t,\ c_i = c_k, c_i^* = c_k^*\}$ and $J = \{j | 1 \leq j \leq t,\ c'_j = f(c_k), c^{*'}_j \circ f = c_k^*\}$. Thus we can also classify Hopf algebras of the form $H(C, n, c, c^*, a, b)$ if all $n_i > 2$. We revisit later the case where some $n_i = 2$.

Theorem 5.6.28 *Let*

$$H = H(C, n, c, c^*, a, b)$$

and

$$H' = H(C', n', c', c^{*'}, a', b')$$

be such that all n_i and $n'_i > 2$. Then $H \cong H'$ if and only if $C = C'$ (in fact we should write again $C \simeq C'$, but we identify C and C'), $t = t'$ and there is an automorphism f of C, nonzero scalars $(\alpha_i)_{1 \leq i \leq t}$, and a permutation π of $\{1, \ldots, t\}$ such that

$$n_i = n'_{\pi(i)}, f(c_i) = c'_{\pi(i)}, c_i^* = c^{*'}_{\pi(i)} \circ f, \text{ and } a_i = a'_{\pi(i)},$$

$\alpha_i^{n_i} = 1$ *for any i such that $a_i = 1$, and for any $1 \leq i < j \leq t$,*

$$b_{ij} = \alpha_i \alpha_j b'_{\pi(i)\pi(j)} \text{ if } \pi(i) < \pi(j) \text{ and}$$

$$c_i^*(c_j) b_{ij} = -\alpha_i \alpha_j b'_{\pi(j)\pi(i)} \text{ if } \pi(j) < \pi(i).$$

Proof: The argument is similar to that in Theorem 5.6.27. An application of the isomorphism f to the equation $x_j x_i = c_j^*(c_i) x_i x_j + b_{ij}(c_i c_j - 1),\ i < j$, yields the relationship between b and b'. ∎

In [107], I. Kaplansky conjectured that there exist only finitely many isomorphism types of Hopf algebras of a fixed finite dimension over an algebraically closed field of characteristic zero. The following corollary answers in the negative this conjecture.

Corollary 5.6.29 *Suppose that $C, c \in C^t, c^* \in C^{*t}$, are such that $c_j^*(c_l) = c_l^*(c_j)^{-1}$ if $l \neq j$, $c_i^*(c_i)$ is a primitive root of unity of order $n_i > 2$, and there exist $i < j$ such that $c_i^{*n_i} = c_j^{*n_j} = 1$, $c_i^{n_i} \neq 1, c_j^{n_j} \neq 1$, $c_i c_j \neq 1$, and $c_i^* c_j^* = 1$. Then for any a with $a_i = a_j = 1$ and satisfying the conditions of Remark 5.6.17, there exist infinitely many non-isomorphic Hopf algebras of the form $H(C, n, c, c^*, a, b)$.*

Proof: Let b and b' be such that $H = H(C, n, c, c^*, a, b)$ and $H' = H(C, n, c, c^*, a, b')$ are well defined. By Remark 5.6.17, infinitely many such b and b' exist. If $f : H \to H'$ is a Hopf algebra isomorphism, then the permutation π in Theorem 5.6.28 is the identity and thus $b_{ij} = \alpha_i \alpha_j b'_{ij}$ for some n_ith and n_jth roots of unity α_i and α_j. Since there exist only finitely many such roots, and k is infinite, the result follows. ∎

Example 5.6.30 To find a concrete example of a class consisting of infinitely many types of Hopf algebras of the same finite dimension, we need some data (C, c, c^*) as in Corollary 5.6.29, with C finite. The simplest such data are the following.

(i) Let p be an odd prime, and ρ a primitive p-th root of 1. Take $C = C_{p^2} =< g >$, the cyclic group of order p^2, $t = 2$, $c = (g, g), c^* = (g^*, g^{*-1})$ where $g^*(g) = \rho$ and $a = (1, 1)$. Then $n_1 = n_2 = p$ and by Corollary 5.6.29, $H(C, n, c, c^*, a, b) \cong H(C, n, c, c^*, a, b')$ if and only if $b_{12} = \gamma b'_{12}$ for γ a primitive p-th root of 1. Thus there are infinitely many types of Hopf algebras of dimension p^4.

(ii) Let $C = C_{pq} =< g >$, the cyclic group of order pq where p is an odd prime, $q > 1$, and $t = 2$, $c = (g, g), c^* = (g^*, g^{*-1})$ where $g^*(g) = \rho$, ρ a primitive p-th root of 1. Let $a_1 = a_2 = 1$. Then again $n_1 = n_2 = p$, and as in (i), there are infinitely many types of Hopf algebras $H(C, n, c, c^*, a, b)$ of dimension $p^3 q$. ∎

Exercise 5.6.31 *(i) Let $C = C_4 =< g >, t = 2, n = (2, 2), c = (g, g), c^* = (g^*, g^*)$ where $g^*(g) = -1, b_{12} = 1, a = (1, 1), a' = (0, 1)$. Show that there exists a Hopf algebra isomorphism $H(C, n, c, c^*, a, b) \simeq H(C, n, c, c^*, a', b)$. (ii) Let $C = C_4 =< g >, t = 2, n = (2, 2), c = (g, g), c^* = (g^*, g^*)$ where $g^*(g) = -1, a = (1, 1)$ and $b_{12} = 2, a' = (0, 1), b'_{12} = 0$. Show that the Hopf algebras $H(C, n, c, c^*, a', b')$ and $H(C, n, c, c^*, a, b)$ are isomorphic.*

Exercise 5.6.32 *Let C be a finite abelian group, $c \in C^t$ and $c^* \in C^{*t}$ such that we can define $H(C, n, c, c^*)$. Show that $H(C, n, c, c^*)^* \cong H(C^*, n, c^*, c)$, where in considering $H(C^*, n, c^*, c)$ we regard $c \in C^{**}$ by identifying C and C^{**}.*

Remark 5.6.33 *The previous exercise shows that if $H = H(C, n, c, c^*)$ where C is a finite abelian group, then $H \cong H^*$ if and only if there is* *an isomorphism $f : C \to C^*$ and a permutation $\pi \in S_t$ such that for all $1 \le j \le t$,*

$$n_{\pi(j)} = n_j,\ f(c_j) = c^*_{\pi(j)},\ < f(c_j), g > = < f(g), c_{\pi^2(j)} > \text{ for all } g \in C.$$

∎

Let us consider now the case where $C = < g >$ will be a cyclic group, either of order m, or infinite cyclic. We first determine for which values of the parameters t and m, finite dimensional Hopf algebras $H = H(C_m, n, c, c^*, a, b)$ exist. By Remark 5.6.17, for a given t, in order to construct H, we need $c \in C^t_m$, $c^* \in (C^*_m)^t$ such that $c^*_i(c_i)$ is a root of unity different from 1, and $c^*_i(c_j)c^*_j(c_i) = 1$ for $i \ne j$. Let ζ be a primitive mth root of unity, and then $g^* \in C^*_m$ defined by $g^*(g) = \zeta$ generates C^*_m. Thus we may write $c_i = g^{u_i}$ and $c^*_i = g^{*d_i}$. To find suitable c and c^*, we require $u, d \in \mathbf{Z}^t$ with $u_i, d_i \in \mathbf{Z}$ mod m such that,

$$(d_iu_j + d_ju_i) \equiv 0 \text{ if } i \ne j \text{ and } d_iu_i \not\equiv 0. \tag{5.34}$$

Then H will be the Hopf algebra with basis g^ix^p, $p \in \mathbf{Z}^t$, $0 \le p_i \le n_i$ and $0 \le i \le m-1$, and such that

$$x_i^{n_i} = a_i(g^{n_iu_i} - 1)\ ,\ x_ig^j = \zeta^{d_ij}g^jx_i,\ \Delta(x_i) = g^{u_i} \otimes x_i + x_i \otimes 1$$

$$x_jx_i = \zeta^{d_ju_i}x_ix_j + b_{ij}(g^{u_i+u_j} - 1) \text{ for } 1 \le i < j \le t.$$

Proposition 5.6.35 *Let m be a positive integer.*
i) If m is even, then the system (5.34) has solutions for any t.
ii) If m is odd, then the system (5.34) has solutions if and only if $t \le 2s$, where s is the number of distinct primes dividing m.

Proof: i) If $m = 2r$ then $d_i = r, u_i = 1$, $1 \le i \le t$, is a solution of (5.34).
ii) We first prove by induction on s that the system has solutions for $t = 2s$ and thus for any $t \le 2s$. If $s = 1$ then $d_1 = u_1 = 1 = u_2, d_2 = -1$ is a solution of (5.34). Now suppose the assertion holds for $s-1$ and let $m = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ with the p_i prime. Then $m' = m/p_s^{\alpha_s}$ has $s-1$ distinct prime divisors, so by the induction hypothesis there exist d'_i, u'_i for $1 \le i \le 2s-2$, such that $(d'_iu'_j + d'_ju'_i) \equiv 0$ mod m' for $1 \le i \ne j \le 2s-2$ and $d'_iu'_i \not\equiv 0$ mod m' for $1 \le i \le 2s-2$. Now a solution of the system for $t = 2s$ is given by $d_i = p_s^{\alpha_s}d'_i, u_i = p_s^{\alpha_s}u'_i$ for $1 \le i \le 2s-2$ and $d_{2s} = d_{2s-1} = u_{2s-1} = m', u_{2s} = -m'$.

Next we show that for $m = p^\alpha$ and $t = 3$ the system has no solutions. Suppose $d, u \in \mathbf{Z}^3$ is a solution, and suppose $d_i = d'_ip^{\alpha_i}, u_i = u'_ip^{\beta_i}$ where $(d'_i, p) = (u'_i, p) = 1$ for $1 \le i \le 3$. For $i \ne j$, p^α divides $d_iu_j + d_ju_i =$

$p^{\alpha_i+\beta_j} d'_i u'_j + p^{\alpha_j+\beta_i} d'_j u'_i$, and so $\alpha_i+\beta_j = \alpha_j+\beta_i$. Since p^α does not divide $d_i u_i$ for any i, then $\alpha_i+\beta_i < \alpha$, so $\alpha_i+\beta_j+\alpha_j+\beta_i < 2\alpha$ for all i,j. Thus $d'_i u'_j \equiv -d'_j u'_i \bmod p$ for all $i \neq j$. Multiplying these three congruences, we obtain $d'_1 d'_2 d'_3 u'_1 u'_2 u'_3 \equiv 0 \bmod p$, a contradiction.

Now suppose that $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ and $2s+1 \leq t$. If the system had a solution d, u, then for every i there would exist j_i, $1 \leq j_i \leq s$, such that $p_{j_i}^{\alpha_{j_i}}$ does not divide $d_i u_i$. By the Pigeon Hole Principle we find i_1, i_2, i_3 such that $j_{i_1} = j_{i_2} = j_{i_3}$; denote this integer by j. Then $p_j^{\alpha_j}$ does not divide any $d_k u_k$, but divides $d_k u_r + d_r u_k$ for all distinct $r,k \in \{i_1, i_2, i_3\}$, and this contradicts what we proved in the case $m = p^\alpha$. ∎

Corollary 5.6.36 *i) If m is even, then Hopf algebras of the form*

$$H(C_m, n, c, c^*, a, b)$$

exist for every t.
ii) If m is odd, then $H(C_m, n, c, c^*, a, b)$ exist for any $t \leq 2s$, where s is the number of distinct prime factors of m. ∎

Corollary 5.6.37 *If $C =< g >$ is an infinite cyclic group, then Hopf algebras $H(C, n, c, c^*, a, b)$ exist for all t.*

Proof: Let t be a positive integer and choose m such that $t \leq 2s$ where s is the number of distinct prime divisors of m. Then by Proposition 5.6.35, there exist $d_i, u_i, 1 \leq i \leq t$ solutions for the system (5.34). Now let $c_i = g^{u_i}$ and $c_i^* = g^{*d_i}$ for $g^*(g) = \zeta$, a primitive m-th root of 1, as before. ∎

The classification results presented in Theorem 5.6.27 and Theorem 5.6.28 depend upon knowledge of the automorphism group of C. In case C is cyclic, $Aut(C)$ is well known, and Theorem 5.6.27 specializes to the following.

Proposition 5.6.38 *If $C =< g >$ is cyclic, then $H(C, n, c, c^*, a, 0) \cong H(C', n', c', c^{*'}, a', 0)$ if and only if $C = C', t = t'$ and there is an automorphism f of C mapping g to g^h and a permutation π of $\{1, \dots, t\}$ such that $n_i = n'_{\pi(i)}$, $c_i^h = c'_{\pi(i)}$ (i.e. $hu_i \equiv u_{\pi(i)}$), $c_i^* = (c^{*'}_{\pi(i)})^h$ (i.e. $d_i = hd_{\pi(i)}$), and $a_i = a'_{\pi(i)}$.*
If C is cyclic of order m, then $(h, m) = 1$; if C is infinite cyclic, then $h = 1$ or $h = -1$. ∎

If C is cyclic, then it is easy to see when $H(C_m, n, c, c^*)$ is isomorphic to its dual, its opposite or co-opposite Hopf algebra.

Corollary 5.6.39 *Let $C = C_m =< g >$, finite, and $H = H(C_m, n, c, c^*)$ where $c_i = g^{u_i}$, $c_i^* = (g^*)^{d_i}$ and $< g^*, g >= \zeta$, a fixed primitive mth root of 1.*

(i) $H \cong H^*$ if and only if there exist h, π as in Proposition 5.6.38 such that for all $1 \le j \le t$,

$$n_{\pi(j)} = n_j,\ hu_j \equiv d_{\pi(j)} \ mod\ m,\ u_{\pi^2(j)} \equiv u_j \ mod\ m.$$

In particular a Taft Hopf algebra is selfdual.

(ii) $H \cong H^{cop}$ if and only if there exist h, π such that for all $1 \le j \le t$,

$$n_{\pi(j)} = n_j,\ hu_j \equiv -u_{\pi(j)} \ mod\ m,\ d_j \equiv hd_{\pi(j)} \ mod\ m.$$

(iii) $H \cong H^{op}$ if and only if there exist h, π such that for all $1 \le j \le t$,

$$n_{\pi(j)} = n_j,\ hu_j \equiv u_{\pi(j)} \ mod\ m,\ d_j \equiv -hd_{\pi(j)} \ mod\ m.$$

∎

We study now Hopf algebras of the form $H(C, n, c^*, c, 0, 1)$, where $b = 1$ means that $b_{ij} = 1$ for all $i < j$. Thus, the skew-primitives x_i are all nilpotent and for $i \neq j$, $x_i x_j - c_i^*(c_j) x_j x_i$ is a nonzero element of kC. It is easy to see that if $a = 0$ and all b_{ij} are nonzero, then a change of variables ensures that all b_{ij} equal 1. This class produces many interesting examples.

The following two definitions are particular cases of Definition 5.6.15.

Definition 5.6.40 *For $t = 2$, let $n \ge 2, c = (c_1, c_2) \in C^2, g^* \in C^*$ with $g^*(c_1) = g^*(c_2)$ a primitive n-th root of unity, and $c_1 c_2 \neq 1$. Denote the pair (n, n) by (n), and, if $c_1 = c_2 = g$, denote (c_1, c_2) by (g). Then $H(C, (n), (c_1, c_2), (g^*, g^{*-1}), 0, 1)$ denotes the Hopf algebra generated by the commuting grouplike elements $g \in C$, and the $(1, c_j)$-primitives x_j, $j = 1, 2$, with multiplication relations*

$$x_j^n = 0,\ x_1 g =< g^*, g > gx_1, \quad x_2 g =< g^{*-1}, g > gx_2$$

$$x_2 x_1 - < g^{*-1}, c_1 > x_1 x_2 = c_1 c_2 - 1$$

∎

Definition 5.6.41 *Let $t > 2$ and let $c \in C^t, g^* \in C^*$ such that $g^*(c_i) = -1$ for all i and $c_i c_j \neq 1$ if $i \neq j$. We denote the t-tuple $(2, \ldots, 2)$ by (2), and the t-tuple $(g^*, \ldots, g^*)$ by (g^*). Then $H(C, (2), (c_1, \ldots, c_t), (g^*), 0, 1)$ is the Hopf algebra generated by the commuting grouplike elements $g \in C$, and the $(1, c_j)$-primitives x_j, with relations*

$$x_i^2 = 0, \quad x_i g = g^*(g) g x_i, \quad x_i x_j + x_j x_i = c_i c_j - 1 \text{ for } i \neq j.$$

∎

Example 5.6.42 (i) Let $C_m =< g >$ be cyclic of finite order $m \geq 2$, let n be an integer ≥ 2, and let $c_1 = g^{u_1}, c_2 = g^{u_2}, g^* \in C^*$ be such that $g^*(g) = \lambda$ where $\lambda^m = 1$, $u_1 + u_2 \not\equiv 0 \mod m$, and $\lambda^{u_1} = \lambda^{u_2}$, a primitive nth root of 1. Then $H = H(C_m, (n), c, (g^*, g^{*-1}), 0, 1)$ is a Hopf algebra of dimension mn^2, with coradical kC_m and generators g, x_1, x_2 such that g is grouplike of order m, x_i is a $(1, g^{u_i})$-primitive, and

$$x_1^n = x_2^n = 0, \quad x_1 g = \lambda g x_1, \quad x_2 g = \lambda^{-1} g x_2$$

$$x_2 x_1 - \lambda^{-u_1} x_1 x_2 = g^{u_1+u_2} - 1$$

(ii) Let $m \geq 2, t > 2$ be integers, m even, and let $C = C_m =< g >$. Let $u_1, \ldots, u_t$ be odd integers such that $u_i + u_j \not\equiv 0 \mod m$ if $i \neq j$ and let $c_i = g^{u_i}, c_i^* = g^*$ where $g^*(g) = -1$. Then the Hopf algebra $H(C_m, (2), c, (g^*), 0, 1)$ has dimension $2^t m$ and has generators $g, x_1, \ldots, x_t$ such that g is grouplike, x_i is a $(1, g^{u_i})$-primitive, and

$$g^m = 1, \quad x_i^2 = 0, \quad x_i g = -g x_i, \quad x_j x_i + x_i x_j = g^{u_i+u_j} - 1.$$

(iii) Suppose $C =< g >$ is infinite cyclic, and $n \geq 2$. Let u_1, u_2 be integers such that $u_1 + u_2 \neq 0$, and let $\lambda \in k$ such that $\lambda^{u_1} = \lambda^{u_2}$ is a primitive nth root of 1. Let $g^* \in C^*$ with $g^*(g) = \lambda$. Then there is an infinite dimensional pointed Hopf algebra with nonzero integral

$$H(C, (n), (g^{u_1}, g^{u_2}), (g^*, g^{*-1}), 0, 1)$$

with generators g, x_1, x_2 such that g is grouplike of infinite order, x_i is a $(1, g^{u_i})$-primitive, and

$$x_1^n = x_2^n = 0, \quad x_1 g = \lambda g x_1, \quad x_2 g = \lambda^{-1} g x_2$$

$$x_2 x_1 - \lambda^{-u_1} x_1 x_2 = g^{u_1+u_2} - 1$$

(iv) Let $C =< g >$ be infinite cyclic, $t > 2$ and let $u_1, \ldots, u_t$ be odd integers such that $u_i + u_j \neq 0$ for $i \neq j$. Then there is an infinite dimensional pointed Hopf algebra with nonzero integral $H(C, (2), c, (g^*), 0, 1)$, where $c_i = g^{u_i}$ and $g^*(g) = -1$. The generators are $g, x_1, \ldots, x_t$ such that g is grouplike of infinite order, x_i is a $(1, g^{u_i})$-primitive, and

$$x_i^2 = 0, \quad x_i g = -g x_i, \quad x_j x_i + x_i x_j = g^{u_i+u_j} - 1.$$

∎

By an argument similar to the proof of Theorem 5.6.27, we can classify the Hopf algebras from Definition 5.6.40.

Theorem 5.6.43 *There is a Hopf algebra isomorphism from*

$$H = H(C, (n), c, (g^*, g^{*-1}), 0, 1)$$

to

$$H' = H(C', (n'), c', (g^{*'}, (g^{*'})^{-1}), 0, 1)$$

if and only if $C = C', n = n'$ *and there is an automorphism* f *of* C *such that*

(i) $f(c_1) = c_1', f(c_2) = c_2'$ *and* $g^* = g^{*'} \circ f$*; or*

(ii) $f(c_1) = c_2', f(c_2) = c_1'$ *and* $g^* = (g^{*'})^{-1} \circ f$.

Proof: If $H \cong H'$, then exactly as in the proof of Theorem 5.6.27, there exists an automorphism f of C and a bijection π of $\{1, 2\}$ such that $f(c_i) = c'_{\pi(i)}$ and $c_i^* = c^{*'}_{\pi(i)} \circ f$. The conditions (i) and (ii) in the statement correspond to π the identity and π the nonidentity permutation.

Conversely, if (i) holds, define an isomorphism from H to H' by mapping g to $f(g)$ and x_i to x_i'. If (ii) holds, define an isomorphism from H to H' by mapping g to $f(g)$, x_1 to x_2' and x_2 to $-g^*(c_1)x_1'$. ∎

Corollary 5.6.44 *If* $C =< g >$ *is cyclic, then the Hopf algebras* H *and* H' *above are isomorphic if and only if* $C = C'$,$n = n'$, *and there is an integer* h *such that the map taking* g *to* g^h *is an automorphism of* C *and either*

(i) $c_i^* = c_i^{*'h}$ *and* $c_i^h = g^{u_i h} = g^{u_i'} = c_i'$ *for* $i = 1, 2$*; or*

(ii) $c_i^* = (c_i^{*'})^{-h}$ *and* $g^{u_1 h} = g^{u_2'}, g^{u_2 h} = g^{u_1'}$. ∎

For the Hopf algebras of Definition 5.6.41 there is a similar classification result.

Theorem 5.6.45 *There is a Hopf algebra isomorphism from*

$$H = H(C, (2), c, (g^*), 0, 1)$$

to

$$H' = H(C', (2), c', (g^{*'}), 0, 1)$$

if and only if $C = C', t = t'$ *and there is a permutation* $\pi \in S_t$ *and an automorphism* f *of* C *such that* $f(c_i) = c'_{\pi(i)}$ *and* $g^* = g^{*'} \circ f$. ∎

Corollary 5.6.46 *Suppose* $C =< g >$ *is cyclic. Then* H *and* H' *as above are isomorphic if and only if* $C = C'$, $t = t'$ *and there exists a permutation* $\pi \in S_t$ *and an automorphism of* C *taking* g *to* g^h, *such that* $c_i^h = g^{u_i h} = c'_{\pi(i)}$ *for all* i. ∎

In Exercise 5.6.31 we saw that if $a \neq 0$, Ore extension Hopf algebras with nonzero derivations may be isomorphic to Ore extension Hopf algebras with zero derivations. The following theorem shows that if $a = 0$, this is impossible.

Theorem 5.6.47 *Hopf algebras of the form*

$$H(C, n, c, c^*) = H(C, n, c, c^*, 0, 0)$$

cannot be isomorphic to either the Hopf algebras of Definition 5.6.40 or Definition 5.6.41.

Proof: Suppose that

$$f : H(C', (n'), c', (g^{*'}, g^{*'-1}), 0, 1) \to H(C, n, c, c^*)$$

is an isomorphism of Hopf algebras. Then, as in the proof of Theorem 5.6.27, we see that $C = C'$, $f(x_1') = \sum_i \alpha_i x_i$ and $f(x_2') = \sum_i \beta_i x_i$ for scalars α_i, β_i. But f applied to the relation

$$x_2'x_1' = (g^{*'})^{-1}(c_1')x_1'x_2' + c_1'c_2' - 1$$

yields $\sum_{i,j} \alpha_i\beta_j(x_jx_i - (g^{*'})^{-1}(c_1')x_ix_j) = l - 1$ in $H(C, n, c, c^*)$, where $l \neq 1$ is a grouplike element. The relations of an Ore extension with zero derivations show that this is impossible. Similarly, $H(C, n, c, c^*)$ cannot be isomorphic to a Hopf algebra as in Definition 5.6.41. ∎

5.7 Solutions to exercises

Exercise 5.1.6 *Let H be a Hopf algebra over the field k, K a field extension of k, and $\overline{H} = K \otimes_k H$ the Hopf algebra over K defined in Exercise 4.2.17. If $T \in H^*$ is a left integral of H, show that the map $\overline{T} \in \overline{H}^*$ defined by $\overline{T}(\delta \otimes_k h) = \delta T(h)$ is a left integral of $\overline{H}$.*
Solution: Let $\delta \otimes_k h \in \overline{H}$. Then

$$\begin{aligned} \sum(\delta \otimes_k h_1)\overline{T}(1 \otimes_k h_2) &= \sum(\delta \otimes_k h_1)T(h_2) \\ &= \delta \otimes_k \sum h_1T(h_2) \\ &= \delta \otimes_k \sum T(h)1_H \\ &= \delta T(h)1_k \otimes_k 1_H \\ &= \overline{T}(\delta \otimes_k h)1_k \otimes_k 1_H \end{aligned}$$

showing that $\overline{T}$ is a left integral of $\overline{H}$.

Exercise 5.1.7 *Let H and H' be two Hopf algebras with nonzero integrals. Then the tensor product Hopf algebra $H \otimes H'$ has a nonzero integral.*
Solution: Assume that H and H' have nonzero integrals. Then we show that $t \otimes t'$ is a left integral for $H \otimes H'$, and this is obviously nonzero. Note that we regard $H^* \otimes H'^*$ as a subspace of $(H \otimes H')^*$, in particulat $t \otimes t' \in (H \otimes H')^*$ is the element working by $(t \otimes t')(h \otimes h') = t(h)t'(h')$ for any $h \in H, h' \in H'$. If $h \in H, h' \in H'$ we have that

$$\begin{aligned}
\sum (h \otimes h')_1 (t \otimes t')((h \otimes h')_2) &= \sum (h_1 \otimes h'_1)(t \otimes t')(h_2 \otimes h'_2) \\
&= \sum (h_1 \otimes h'_1) t(h_2) t'(h'_2) \\
&= \sum h_1 t(h_2) \otimes h'_1 t'(h'_2) \\
&= t(h)1 \otimes t'(h')1 \\
&= (t \otimes t')(h \otimes h') 1 \otimes 1
\end{aligned}$$

showing that indeed $t \otimes t'$ is a left integral.

Exercise 5.2.5 *Let H be a Hopf algebra. Then the following assertions are equivalent:*
i) H has a nonzero left integral.
ii) There exists a finite dimensional left ideal in H^*.
iii) There exists $h^* \in H^*$ such that $Ker(h^*)$ contains a left coideal of finite codimension in H.
Solution: It follows from Corollary 5.2.4 and the characterization of $H^{*\, rat}$ given in Corollary 2.2.16.

Exercise 5.2.12 *A semisimple Hopf algebra is separable.*
Solution: Let $t \in H$ be a left integral with $\varepsilon(t) = 1$. We show that

$$\sum t_1 \otimes S(t_2)$$

is a separability idempotent. Since $\sum t_1 S(t_2) = \varepsilon(t)1 = 1$, let $x \in H$ and compute

$$\begin{aligned}
&\sum x t_1 \otimes S(t_2) = \\
&= \sum x_1 t_1 \otimes S(t_2) S(x_2) x_3 \\
&= \sum x_1 t_1 \otimes S(x_2 t_2) x_3 \\
&= \sum (I \otimes S) \Delta(x_1 t)(1 \otimes x_2) \\
&= \sum (I \otimes S) \Delta(\varepsilon(x_1) t)(1 \otimes x_2)
\end{aligned}$$

$$\begin{aligned} &= \sum (I \otimes S)\Delta(t)(1 \otimes x) \\ &= \sum t_1 \otimes S(t_2)x. \end{aligned}$$

Exercise 5.2.13 *Let H be a finite dimensional Hopf algebra over the field k, K a field extension of k, and $\overline{H} = K \otimes_k H$ the Hopf algebra over K defined in Exercise 4.2.17. If $t \in H$ is a left integral in H, show that $\overline{t} = 1_K \otimes_k t \in \overline{H}$ is a left integral in $\overline{H}$. As a consequence show that H is semisimple over k if and only if $\overline{H}$ is semisimple over K.*

Solution: For any $\delta \otimes_k h \in \overline{H}$ we have that

$$\begin{aligned} (\delta \otimes_k h)\overline{t} &= \delta \otimes_k ht \\ &= \delta \otimes_k \varepsilon(h)t \\ &= \overline{\varepsilon}(\delta \otimes_k h)\overline{t} \end{aligned}$$

which means that $\overline{t}$ is a left integral in $\overline{H}$. The second part follows immediately from Theorem 5.2.10.

Exercise 5.3.5 *Let H be a finite dimensional Hopf algebra. Show that H is injective as a left (or right) H-module.*

Solution: Since H^* has nonzero integrals, we have that H^* is a projective left H^*-comodule. By Corollary 2.4.20 we see that H is injective as a right H^*-comodule. Since the categories $\mathcal{M}^{H^*}$ and ${}_H\mathcal{M}$ are isomorphic, we obtain that H is an injective left H-module.

Exercise 5.4.8 *Let $\chi \in \int_l$ and $h \in H$ be such that $\chi \circ S(h) = 1$. Then χ spans $\int_l$.*

Solution: The existence of χ and h as in the statement was proved in 5.4.4, only in that proof we have used the uniqueness. So we show first that this can be done directly.

Let J be the injective envelope of $k1$, considered as a left H-comodule. Then J is finite dimensional and $H = J \oplus K$ for a left coideal K of H. Let $f : H \to k$ be a nonzero linear map such that $f(K) = 0$ and $f(1_H) = 1$. Since $K \subseteq Ker(f)$ we have that $f \in Rat(H^*_{H^*}) = Rat({}_{H^*}H^*)$. By Theorem 5.2.3 there exist $h_i \in H$ and $t_i \in \int_l$ such that $f = \sum t_i \leftharpoonup h_i$, so $(\sum t_i \leftharpoonup h_i)(1) \neq 0$. Therefore, one of the $(t_i \leftharpoonup h_i)(1)$ is not zero, and we can take this element of H as our h and a suitable multiple of the corresponding left integral for χ.

We will denote the right integral $\chi \circ S$ by χS. We show first that for any $t \in \int_l$ and $g \in H$ there exists an $l \in H$ such that

$$g \rightharpoonup t = l \rightharpoonup \chi \tag{5.35}$$

where $(g \rightharpoonup t)(x) = t(xg)$. Let $x \in H$ and compute

$$
\begin{aligned}
& (g \rightharpoonup t)(x) = \\
= \ & \chi S(h)t(xg) \ \ \text{(by Lemma 5.4.4 ii))} \\
= \ & \sum \chi S(x_1 g_1 h)t(x_2 g_2) \ \ (t \text{ left integral}) \\
= \ & \sum \chi S(x_1 g_1 h_1)t(x_2 g_2 h_2 S(h_3)) \\
= \ & \sum \chi S(x g h_1)t(S(h_2)) \ \ (\chi S \text{ right integral}) \\
= \ & \chi S(x \sum g h_1 t(S(h_2)) \\
= \ & \chi S(xu) \ \ (\text{where } u = \textstyle\sum g h_1 t(S(h_2))) \\
= \ & \chi S(xu)\chi S(h) \\
= \ & \sum \chi S(x_1 u_1)\chi(x_2 u_2 S(h)) \ \ (\chi S \text{ right integral}) \\
= \ & \sum \chi S(x_1 u_1 S(h_2)h_3)\chi(x_2 u_2 S(h_1)) \\
= \ & \sum \chi S(h_2)\chi(xuS(h_1)) \ \ (\chi \text{ left integral}) \\
= \ & \chi(xl) \ \ (\text{where } l = \textstyle\sum uS(h_1)\chi(S(h_2))) \\
= \ & (l \rightharpoonup \chi)(x)
\end{aligned}
$$

so (5.35) is proved, and we can choose $r \in H$ such that

$$h \rightharpoonup t = r \rightharpoonup \chi \tag{5.36}$$

Now

$$
\begin{aligned}
t(x) &= \chi S(h)t(x) \\
&= \chi S(h_1)t(xh_2) \ \ (\chi S \text{ right integral}) \\
&= \chi S(S(x_1)x_2 h_1)t(x_3 h_2) \\
&= \chi S^2(x_1)t(x_2 h) \ \ (t \text{ left integral}) \\
&= \chi S^2(x_1)\chi(x_2 r) \ \ (\text{by } (5.36)) \\
&= \chi S(r)\chi(x),
\end{aligned}
$$

where the last equality follows by reversing the previous five equalities. It follows that $t = \chi S(r)\chi$, i.e. χ spans $\int_l$ and the proof is complete.

Exercise 5.5.6 *Prove Corollary 5.5.5 directly.*
Solution: We know that $\phi : H^* \longrightarrow H$, $\phi(h^*) = \sum t'_1 h^*(t'_2)$ is a bijection. Hence there exists a $T \in H^*$ such that $\sum t'_1 T(t'_2) = 1$. Applying ε to this equality we get $T(t') = 1$. For $h \in H$ we have

$$\sum t'_1 T(ht'_2) \ = \ \sum t'_1 T(\varepsilon(h_1)h_2 t'_2)$$

$$\begin{aligned}
&= \sum \varepsilon(h_1)t'_1T(h_2t'_2) \\
&= \sum S(h_1)h_2t'_1T(h_3t'_2) \\
&= \sum S(h_1)\varepsilon(h_2)t'_1T(t'_2) = S(h).
\end{aligned}$$

In particular, we have $S(t) = \sum t'_1T(t't'_2) = \sum t'_1T(t'\lambda'(t'_2)) = (t' \rightharpoonup \lambda')T(t') = t' \rightharpoonup \lambda'$.

Exercise 5.5.2 *Let $f : C \to D$ be a surjective morphism of coalgebras. Show that if C is pointed, then D is pointed and $Corad(D) = f(Corad(C))$.*
Solution: It follows from Exercise 3.1.13 and from the fact that for any grouplike element $g \in G(C)$, the element $f(g)$ is a grouplike element of D.

Exercise 5.5.7 *Let H be a Hopf algebra such that the coradical H_0 is a Hopf subalgebra. Show that the coradical filtration $H_0 \subseteq H_1 \subseteq \dots H_n \subseteq \dots$ is an algebra filtration, i.e. for any positive integers m, n we have that $H_mH_n \subseteq H_{m+n}$.*
Solution: We remind from Exercise 3.1.11 that the coradical filtration is a coalgebra filtration, i.e. $\Delta(H_n) \subseteq \sum_{i=0,n} H_i \otimes H_{n-i}$ for any n. In particular this shows that $\Delta(H_n) \subseteq H_n \otimes H_{n-1} + H_0 \otimes H_n$.
We first show by induction on m that $H_mH_0 = H_m$ for any m. For $m = 0$ this is clear since H_0 is a subalgebra of H. Assume that $H_{m-1}H_0 = H_{m-1}$. Then

$$\begin{aligned}
\Delta(H_mH_0) &\subseteq (H_m \otimes H_{m-1} + H_0 \otimes H_m) \cdot (H_0 \otimes H_0) \\
&\subseteq H_mH_0 \otimes H_{m-1} + H_0 \otimes H_mH_0 \\
&\subseteq H \otimes H_{m-1} + H_0 \otimes H
\end{aligned}$$

where for the second inclusion we used the induction hypothesis. Thus $H_mH_0 \subseteq H_0 \wedge H_{m-1} = H_m$. Clearly, $H_m \subseteq H_mH_0$ since H_0 contains 1. Similarly $H_0H_m = H_m$ for any m.
Now we prove by induction on p that for any m, n with $m + n = p$ we have that $H_mH_n \subseteq H_p$. It is clear for $p = 0$. Assume this is true for $p - 1$, where $p \geq 1$, and let m, n with $m + n = p$. If $m = 0$ or $n = 0$, we already proved the desired relation. Assume that $m, n > 0$. Then we have that

$$\begin{aligned}
\Delta(H_mH_n) &\subseteq (H_m \otimes H_{m-1} + H_0 \otimes H_m)(H_n \otimes H_{n-1} + H_0 \otimes H_n) \\
&\subseteq H \otimes H_{p-2} + H_m \otimes H_{p-1} + H_n \otimes H_{p-1} + H_0 \otimes H \\
&\subseteq H \otimes H_{p-1} + H_0 \otimes H
\end{aligned}$$

which shows that $H_mH_n \subseteq H_0 \wedge H_{p-1} = H_p = H_{m+n}$.

Exercise 5.5.9 *Let H be a Hopf algebra. Show that the following are equivalent.*

(1) H is cosemisimple.
(2) k is an injective right (or left) H-comodule.
(3) There exists a right (or left) integral $t \in H^*$ such that $t(1) = 1$.
Solution: (1) and (2) are clearly equivalent from Theorem 3.1.5 and Exercise 4.4.7. To see that (2) and (3) are equivalent, we consider the unit map $u : k \longrightarrow H$, which is an injective morphism of right H-comodules. Then k is injective if and only if there exists a morphism $t : H \longrightarrow k$ of right H-comodules with $tu = Id_k$. But such a t is precisely a right integral with $t(1) = 1$.

Exercise 5.5.10 *Show that in a cosemisimple Hopf algebra H the spaces of left and right integrals are equal, and if t is a left integral with $t(1) = 1$, we have that $t \circ S = t$.*
Solution: By Exercise 5.5.9 we know that there exist a left integral t and a right integral T such that $t(1) = T(1) = 1$. Then $t = T(1)t = Tt = t(1)T = T$, so $\int_l = \int_r$. We know that $t \circ S$ is a right integral. Since $(t \circ S)(1) = 1$, we see that $t \circ S = t$.

Exercise 5.5.12 *Let H be a Hopf algebra over the field k, K a field extension of k, and $\overline{H} = K \otimes_k H$ the Hopf algebra over K defined in Exercise 4.2.17. Show that if H is cosemisimple over k, then $\overline{H}$ is cosemisimple over K. Moreover, in the case where H has a nonzero integral, show that if $\overline{H}$ is cosemisimple over K, then H is cosemisimple over k.*
Solution: We know from Exercise 5.1.6 that if T is a left integral of H, then $\overline{T} \in \overline{H}^*$ defined by $\overline{T}(\delta \otimes_k h) = \delta T(h)$ is a left integral of $\overline{H}$. Everything follows now from the characterization of cosemisimplicity given in Exercise 5.5.9.

Exercise 5.5.13 *Let H be a finite dimensional Hopf algebra. Show that the following are equivalent.*
(1) H is semisimple.
(2) k is a projective left (or right) H-module (with the left H-action on k defined by $h \cdot \alpha = \varepsilon(h)\alpha$).
(3) There exists a left (or right) integral $t \in H$ such that $\varepsilon(t) \neq 0$.
Solution: It is clear that (1) and (2) are equivalent from Exercise 4.4.8. If the left H-module k is projective, since $\varepsilon : H \longrightarrow k$ is a surjective morphism of left H-modules, then there exists a morphism of left H-modules $\phi : k \longrightarrow H$ such that $\varepsilon \circ \phi = Id_k$. Denote $t = \phi(1_k) \in H$. We have that

$$ht = h\phi(1_k) = \phi(h \cdot 1_k) = \phi(\varepsilon(h)1_k) = \varepsilon(h)\phi(1_k) = \varepsilon(h)t$$

for any $h \in H$, showing that t is a left integral in H. Clearly $\varepsilon(t) = \varepsilon(\phi(1)) = 1$. Conversely, if there exists a left (or right) integral $t \in H$ such that $\varepsilon(t) \neq 0$, we can obviously assume that $\varepsilon(t) = 1$ by multiplying with a scalar. Then the map $\phi : k \longrightarrow H$, $\phi(\alpha) = \alpha t$ is a morphism of left H-modules and $\varepsilon \circ \phi = Id$, so k is isomorphic to a direct summand in the left H-module H. This shows that k is projective.

Exercise 5.6.12 *Give a different proof for the fact that A_t does not have nonzero integrals, by showing that the injective envelope of the simple right A_t-comodule kg, $g \in C$, is infinite dimensional.*
Solution: Let $\mathcal{E}_g$ be the subspace of A_t spanned by all

$$gc_1^{-p_1}c_2^{-p_2}\dots c_t^{-p_t}X_1^{p_1}\dots X_t^{p_t} = gc_1^{-p_1}\dots c_t^{-p_t}X^p, p = (p_1, \dots, p_t) \in \mathbf{N}^t.$$

Then by Equation (5.9), $\mathcal{E}_g$ is a right A_t-subcomodule of A_t and kg is essential in $\mathcal{E}_g$. On the other hand, $A_t = \oplus_{g\in C}\mathcal{E}_g$. Thus the $\mathcal{E}_g$'s are injective, and we obtain that $\mathcal{E}_g$ is the injective envelope of kg.

Exercise 5.6.24 *Let A be the algebra generated by an invertible element a and an element b such that $b^n = 0$ and $ab = \lambda ba$, where λ is a primitive $2n$-th root of unity. Show that A is a Hopf algebra with the comultiplication and counit defined by*

$$\Delta(a) = a\otimes a,\ \Delta(b) = a\otimes b + b\otimes a^{-1}, \varepsilon(a) = 1, \varepsilon(b) = 0$$

Also show that A has nonzero integrals and it is not unimodular.
Solution: Let $C =< a >$ be an infinite cyclic group and $a^* \in C^*$ such that $a^*(a) = \sqrt{\lambda}$. It is easy to see that $A \simeq H(C, n, a^2, a^*)$. Everything else follows from the properties of Hopf algebras of the form $H(C, n, c, c^*, a, b)$.

Exercise 5.6.25 *Let H be the Hopf algebra with generators $c, x_1, \dots, x_t$ subject to relations*

$$c^2 = 1, \quad x_i^2 = 0, \quad x_i c = -cx_i, \quad x_j x_i = -x_i x_j,$$

$$\Delta(c) = c\otimes c, \quad \Delta(x_i) = c\otimes x_i + x_i\otimes 1.$$

Show that H is a pointed Hopf algebra of dimension 2^{t+1} with coradical of dimension 2.
Solution: Let $C = C_2 =< c >$, the cyclic group of order 2, $c_1^*, \dots, c_t^* \in C^*$ defined by $c_j^*(c) = -1$, and $c_j = c$ for all $1 \le j \le t$. Then $H = H(C, n, c, c^*)$ and all the requirements follow from the general facts about Hopf algebras defined by Ore extensions.

Exercise 5.6.26 *Let ϕ be an automorphism of kC of the form $\phi(g) = c^*(g)g$ for $g \in C$, and assume that $c^*(g) \neq 1$ for any $g \in C$ of infinite order. Show that if δ is a ϕ-derivation of kC such that the Ore extension $(kC)[Y, \phi, \delta]$ has a Hopf algebra structure extending that of kC with Y a $(1, c)$-primitive,*

then there is a Hopf algebra isomorphism $(kC)[Y,\phi,\delta] \simeq (kC)[X,\phi]$.
Solution: Let $U = \{g \in C | c^*(g) \neq 1\}$ and $V = \{g \in C | c^*(g) = 1\}$. Thus, if $g \in V$ then by our assumption g has finite order. In this case, $\phi(g^n) = g^n$ for all n, and induction on $n \geq 1$ shows that $\delta(g^n) = ng^{n-1}\delta(g)$. Then $\delta(1) = mg^{-1}\delta(g)$, where m is the order of g, and $\delta(1) = 0$ imply that $\delta(g) = 0$.
Now let $g \in U$. Applying Δ to the relation $Yg = c^*(g)gY + \delta(g)$, we find that $\Delta(\delta(g)) = cg \otimes \delta(g) + \delta(g) \otimes g$. Thus $\delta(g)$ is a (g, cg)-primitive, and so $\delta(g) = \alpha_g g(c-1)$ for some scalar α_g.
Therefore, for any two elements g and h of U

$$\begin{aligned}\delta(gh) &= \delta(g)h + \phi(g)\delta(h)\\ &= \alpha_g g(c-1)h + c^*(g)g\alpha_h h(c-1)\\ &= (\alpha_g + \alpha_h c^*(g))(c-1)gh\end{aligned}$$

and similarly

$$\delta(hg) = (\alpha_h + \alpha_g c^*(h))(c-1)gh$$

Since C is abelian $\alpha_g + \alpha_h < c^*, g >= \alpha_h + \alpha_g < c^*, h >$, or

$$\alpha_g/(1 - c^*(g)) = \alpha_h/(1 - c^*(h))$$

Denote by γ the common value of the $\alpha_g/(1 - c^*(g))$ for $g \in U$. We have $\alpha_g - \gamma + c^*(g)\gamma = 0$.
Let $Z = Y - \gamma(c-1)$. For any $g \in U$ we have that

$$\begin{aligned}Zg &= Yg - \gamma(c-1)g\\ &= c^*(g)gY + \alpha_g g(c-1) - \gamma(c-1)g\\ &= c^*(g)gZ + c^*(g)\gamma g(c-1) + \alpha_g g(c-1) - \gamma g(c-1)\\ &= c^*(g)gZ + (\alpha_g - \gamma + c^*(g)\gamma)g(c-1)\\ &= c^*(g)gZ\end{aligned}$$

Obviously, $Zg = gZ$ if $g \in V$, so $(kC)[Y,\phi,\delta] \simeq (kC)[Z,\phi]$ as algebras. Since Z is clearly a $(1,c)$-primitive, this is also a coalgebra morphism, which completes the solution.

Exercise 5.6.31 *(i) Let $C = C_4 =< g >, t = 2, n = (2,2), c = (g,g), c^* = (g^*, g^*)$ where $g^*(g) = -1, b_{12} = 1, a = (1,1), a' = (0,1)$. Show that there exists a Hopf algebra isomorphism $H(C,n,c,c^*,a,b) \simeq H(C,n,c,c^*,a',b)$.*
(ii) Let $C = C_4 =< g >, t = 2, n = (2,2), c = (g,g), c^* = (g^*, g^*)$ where $g^*(g) = -1, a = (1,1)$ and $b_{12} = 2, a' = (0,1), b'_{12} = 0$. Show that the Hopf algebras $H(C,n,c,c^*,a',b')$ and $H(C,n,c,c^*,a,b)$ are isomorphic.
Solution: (i) The map $f : H(C,n,c,c^*,a,b) \to H(C,n,c,c^*,a',b)$ defined

by $f(g) = g, f(x_1) = -(\beta^2+\beta)x_1' + \beta x_2', f(x_2) = x_2'$, where $\beta \in k$ is a primitive cube root of -1 is a Hopf algebra isomorphism.
(ii) The map f from $H(C,n,c,c^*,a',b')$ to $H(C,n,c,c^*,a,b)$ defined by $f(g) = g, f(x_1) = x_2, f(x_2) = x_1 - x_2$, is a Hopf algebra isomorphism. Note that one of the Hopf algebras is an Ore extension with nontrivial derivation while the other is an Ore extension with trivial derivation.

Exercise 5.6.32 *Let C be a finite abelian group, $c \in C^t$ and $c^* \in C^{*t}$ such that we can define $H(C,n,c,c^*)$. Show that $H(C,n,c,c^*)^* \cong H(C^*,n,c^*,c)$, where in considering $H(C^*,n,c^*,c)$ we regard $c \in C^{**}$ by identifying C and C^{**}.*
Solution: Suppose $C = C_1 \times C_2 \times \cdots \times C_s =< g_1 > \times \cdots \times < g_s >$ where C_i is cyclic of order m_i. For $i = 1,\ldots,s$, let $\zeta_i \in k^*$ be a primitive m_i-th root of 1. The dual $C^* =< g_1^* > \times \cdots \times < g_s^* >$, where $g_i^*(g_i) = \zeta_i$ and $g_i^*(g_j) = 1$ for $i \neq j$, is then isomorphic to C. We identify C and C^{**} using the natural isomorphism $C \cong C^{**}$ where $g^{**}(g^*) = g^*(g)$.
First we determine the grouplikes in H^*. Let $h_i^* \in H^*$ be the algebra map defined by $h_i^*(g_j) = g_i^*(g_j)$ and $h_i^*(x_j) = 0$ for all i,j. Since the h_i^* are algebra maps from H to k, H^* contains a group of grouplikes generated by the g_i^*, and so isomorphic to C^*.
Now, let $y_j \in H^*$ be defined by $y_j(gx_j) = c_j^{*-1}(g)$, and $y_j(gx^w) = 0$ for $x^w \neq x_j$.
We determine the nilpotency degree of y_j. Clearly y_j^r is nonzero only on basis elements gx_j^r. Note that by (5.19) and the fact that $q_j = c_j^*(c_j)$,

$$\begin{aligned}
y_j^2(gx_j^2) &= (y_j \otimes y_j)[\binom{2}{1}_{q_j} gc_jx_j \otimes gx_j] \\
&= \binom{2}{1}_{q_j} c_j^*(g^2c_j)^{-1} \\
&= (1+q_j)q_j^{-1}c_j^*(g^2)^{-1} \\
&= (1+q_j^{-1})c_j^*(g^2)^{-1}
\end{aligned}$$

By induction, using the fact that $\binom{r}{1}_{q_j} = (1+q_j+\ldots+q_j^{r-1})$, we see that for $\eta_j = q_j^{-1}$,

$$y_j^r(gx_j^r) = (1+\eta_j)\ldots(1+\eta_j+\ldots+\eta_j^{r-1})c_j^*(g^r)^{-1}.$$

Since q_j, and thus η_j, is a primitive n_j-th root of 1, this expression is 0 if and only if $r = n_j$. Thus the nilpotency degree of y_j is n_j.
Let $g^* \in H^*$ be an element of the group of grouplikes generated by the g_i^* above. We check how the y_j multiply with g^* and with each other. Clearly,

both y_jg^* and g^*y_j are nonzero only on basis elements gx_j. We compute

$$g^*y_j(gx_j) = g^*(gc_j)y_j(gx_j) = g^*(g)g^*(c_j)c_j^*(g)^{-1}$$

and

$$y_jg^*(gx_j) = y_j(gx_j)g^*(g) = c_j^*(g)^{-1}g^*(g)$$

so that

$$g^*y_j = g^*(c_j)y_jg^*, \text{ or } y_jg^* = c_j^{**-1}(g^*)g^*y_j.$$

Let $j < i$. Then y_jy_i and y_iy_j are both nonzero only on basis elements $gx_ix_j = c_i^*(c_j)gx_jx_i$. We compute

$$y_iy_j(gx_ix_j) = y_i(gx_i)y_j(gx_j) = c_i^{*-1}(g)c_j^{*-1}(g)$$

and

$$y_jy_i(c_i^*(c_j)gx_jx_i) = c_i^*(c_j)y_j(gx_j)y_i(gx_i) = c_i^*(c_j)c_j^{*-1}(g)c_i^{*-1}(g)$$

Therefore for $j < i$,

$$y_iy_j = c_i^{*-1}(c_j)y_jy_i = c_j^{*-1}(c_i^{-1})y_jy_i = c_i^{**-1}(c_j^{*-1})y_jy_i$$

Finally, we confirm that the elements y_j are (ϵ_H, c_j^{*-1})-primitives and then we will be done. The maps $c_j^{*-1} \otimes y_j + y_j \otimes \epsilon_H$ and $m^*(y_j)$ are both only nonzero on elements of $H \otimes H$ which are sums of elements of the form $g \otimes lx_j$ or $gx_j \otimes l$, where $m : H \otimes H \to H$ is the multiplication of H and $m^* : H^* \to (H \otimes H)^*$ is regarded as the comultiplication of H^*. We check

$$(c_j^{*-1} \otimes y_j + y_j \otimes \epsilon_H)(g \otimes lx_j) = (c_j^{*-1} \otimes y_j)(g \otimes lx_j) = c_j^{*-1}(g)c_j^{*-1}(l)$$

and

$$m^*(y_j)(g \otimes lx_j) = y_j(glx_j) = c_j^{*-1}(gl)$$

Similarly,

$$(c_j^{*-1} \otimes y_j + y_j \otimes \epsilon_H)(gx_j \otimes l) = y_j(gx_j) = c_j^{*-1}(g)$$

and

$$y_j(gx_jl) = y_j(c_j^*(l)glx_j) = c_j^*(l)c_j^{*-1}(gl) = c_j^{*-1}(g)$$

Thus the Hopf subalgebra of H^* generated by the h_i^*, y_j is isomorphic to $H(C^*, n, c^{*-1}, c^{-1})$ and by a dimension argument it is all of H^*. Now we only need note that for any $H = H(C, n, c, c^*)$, the group automorphism of C which maps every element to its inverse induces a Hopf algebra isomorphism from H to $H(C, n, c^{-1}, c^{*-1})$, and the solution is complete.

Bibliographical notes

Again we used the books of M. Sweedler [218], E. Abe [1], and S. Montgomery [149]. Integrals were introduced by M. Sweedler and R. Larson in [120]. The connection with H^{*rat} was given by M. Sweedler in [219]. Lemma 5.1.4 is also in this paper. In the solution of Exercise 5.2.12 (which we believe was first remarked by Kreimer), we have used a trick shown to us by D. Radford. In [218], M. Sweedler asked whether the dimension of the space of integrals is either 0 or 1 (the uniqueness of integrals). Uniqueness was proved by Sullivan in [217]. The study of integrals from a coalgebraic point of view has proved to be relevant, as shown in the papers by B. Lin [123], Y. Doi [72], or D. Radford [189]. The coalgebraic approach produced short proofs for the uniqueness of integrals, given in D. Ştefan [211], M. Beattie, S. Dăscălescu, L. Grünenfelder, C. Năstăsescu, [28], C. Menini, B. Torrecillas, R. Wisbauer [145], S. Dăscălescu, C. Năstăsescu, B. Torrecillas, [68]. The proof given here is a short version of the one in the last cited paper. The idea of the proof in Exercise 5.4.8 belongs to A. Van Daele [236] (this is actually the method used in the case of Haar measures), and we took it from [198]. The bijectivity of the antipode for co-Frobenius Hopf algebras was proved by D.E. Radford [189], where the structure of the 1-dimensional ideals of H^* was also given. The proof given here uses a simplification due to C. Călinescu [52].
The method for constructing pointed Hopf algebras by Ore extensions from Section 5.6 was initiated by M. Beattie, S. Dăscălescu, L. Grünenfelder and C. Năstăsescu in [28], and continued by M. Beattie, S. Dăscălescu and L. Grünenfelder in [27]. A different approach for constructing these Hopf algebras is due to N. Andruskiewitsch and H.-J. Schneider [13], using a process of bosonization of a quantum linear space, followed by lifting. This class of Hopf algebras is large enough for answering in the negative Kaplansky's conjecture on the finiteness of the isomorphism types of Hopf algebras of a given finite dimension over an algebraically closed field of characteristic zero, as showed by N. Andruskiewitsch and H.-J. Schneider in [13], M. Beattie, S. Dăscălescu and L. Grünenfelder in [25, 27]. The conjecture was also answered by S. Gelaki [86] and E. Müller [154]. A more general isomorphism theorem for Hopf algebras constructed by Ore extensions was proved by M. Beattie in [24]

Chapter 6

Actions and coactions of Hopf algebras

6.1 Actions of Hopf algebras on algebras

In this chapter k is a field, and H a Hopf k-algebra with comultiplication Δ and counit ε. The antipode of H will be denoted by S.

Definition 6.1.1 *We say that H* acts on *the k-algebra A (or that A is a (left) H-*module algebra *if the following conditions hold:*
(MA1) A is a left H-module (with action of $h \in H$ on $a \in A$ denoted by $h \cdot a$).
(MA2) $h \cdot (ab) = \sum (h_1 \cdot a)(h_2 \cdot b), \quad \forall h \in H, \quad a, b \in A$.
(MA3) $h \cdot 1_A = \varepsilon(h) 1_A, \quad \forall h \in H$.
Right H-module algebras are defined in a similar way. ∎

Let A be a k-algebra which is also a left H-module with structure given by

$$\nu : H \otimes A \longrightarrow A, \quad \nu(h \otimes a) = h \cdot a.$$

By the adjunction property of the tensor product, we have the bijective natural correspondence

$$Hom(H \otimes A, A) \xrightarrow{\sim} Hom(A, Hom(H, A)).$$

If we denote by $\psi : A \longrightarrow Hom(H, A)$ the map corresponding to ν by the above bijection, we have the following

Proposition 6.1.2 *A is an H-module algebra if and only if ψ is a morphism of algebras ($Hom(H, A)$ is an algebra with convolution: $(f * g)(h) = \sum f(h_1) g(h_2)$).*

Proof: Since ψ corresponds to ν, we have that $\nu(h \otimes a) = \psi(a)(h)$, $\forall h \in H$, $a \in A$. Hence $(MA2)$ holds
$\Leftrightarrow \nu(h \otimes ab) = \sum \nu(h_1 \otimes a)\nu(h_2 \otimes b)$, $\forall h \in H$, $a, b \in A$
$\Leftrightarrow \psi(ab)(h) = \sum \psi(a)(h_1)\psi(b)(h_2) = (\psi(a) * \psi(b))(h)$ $\forall h \in H$, $a, b \in A$
$\Leftrightarrow \psi(ab) = \psi(a) * \psi(b)$, $\forall a, b \in A \Leftrightarrow \psi$ is multiplicative.
Moreover, $(MA3)$ holds
$\Leftrightarrow \nu(h \otimes 1_A) = \psi(1_A)(h) = \varepsilon(h)1_A \Leftrightarrow \psi(1_A) = 1_{Hom(H,A)}$. ∎

Lemma 6.1.3 *Let A be a k-algebra which is a left H-module such that $(MA2)$ holds. Then*
i) $(h \cdot a)b = \sum h_1 \cdot (a(S(h_2) \cdot b))$, $\forall a, b \in A, h \in H$.
ii) If S is bijective, then
$a(h \cdot b) = \sum h_2 \cdot ((S^{-1}(h_1) \cdot a)b)$, $\forall a, b \in A, h \in H$.

Proof: By $(MA2)$ we have:

$$\begin{aligned}\sum h_1 \cdot (a(S(h_2) \cdot b) &= \sum (h_1 \cdot a)(h_2 \cdot (S(h_3) \cdot b)) \\ &= \sum (h_1 \cdot a)((h_2 S(h_3)) \cdot b) \\ &= ((\sum h_1 \varepsilon(h_2)) \cdot a)b = (h \cdot a)b.\end{aligned}$$

ii) is proved similarly. ∎

Proposition 6.1.4 *Let A be a k-algebra which is also a left H-module. Then A is an H-module algebra if and only if $\mu : A \otimes A \longrightarrow A$, $\mu(a \otimes b) = ab$, is a morphism of H-modules ($A \otimes A$ is a left H-module with $h \cdot (a \otimes b) = \sum h_1 \cdot a \otimes h_2 \cdot b$).*

Proof: The assertion is clearly equivalent to $(MA2)$. To finish the proof it is enough to show that $(MA3)$ may be deduced from $(MA2)$. We do this using Lemma 6.1.3. Indeed, taking in Lemma 6.1.3 $a = b = 1_A$, we have

$$\begin{aligned}h \cdot 1_A &= (h \cdot 1_A)1_A \\ &= \sum h_1 \cdot (1_A(S(h_2) \cdot 1_A)) \\ &= \sum h_1 \cdot (S(h_2) \cdot 1_A) \\ &= (\sum h_1 S(h_2)) \cdot 1_A = \varepsilon(h)1_A\end{aligned}$$

so $(MA3)$ holds and the proof is complete. ∎

Definition 6.1.5 *Let A be an H-module algebra. We will call the* algebra of invariants

$$A^H = \{a \in A \mid h \cdot a = \varepsilon(h)a, \ \forall h \in H\}.$$

∎

A^H is indeed a k-subalgebra of A: if $a, b \in A^H$, then for any $h \in H$ we have

$$\begin{aligned} h \cdot (ab) &= \sum (h_1 \cdot a)(h_2 \cdot b) \\ &= \sum \varepsilon(h_1) a \varepsilon(h_2) b \\ &= \sum \varepsilon(h_1)\varepsilon(h_2) ab \\ &= \sum \varepsilon(h_1 \varepsilon(h_2)) ab = \varepsilon(h) ab. \end{aligned}$$

Another algebra associated to an action of the Hopf algebra H on the algebra A is given by the following

Definition 6.1.6 *If A is an H-module algebra, the* smash product *of A and H, denoted $A\#H$, is, as a vector space, $A\#H = A \otimes H$, together with the following operation (we will denote the element $a \otimes h$ by $a\#h$):*

$$(a\#h)(b\#g) = \sum a(h_1 \cdot b)\#h_2 g.$$

∎

Proposition 6.1.7 *i) $A\#H$, together with the multiplication defined above, is a k-algebra.*
ii) The maps $a \longmapsto a\#1_H$ and $h \longmapsto 1_A\#h$ are injective k-algebra maps from A, respectively H, to $A\#H$.
iii) $A\#H$ is free as a left A-module, and if $\{h_i\}_{i\in I}$ is a k-basis of H, then $\{1_A\#h_i\}_{i\in I}$ is an A-basis of $A\#H$ as a left A-module.
iv) If S is bijective (e.g. when H is finite dimensional, see Proposition 5.2.6, or, more general, when H is co-Frobenius see Proposition 5.4.6), then $A\#H$ is free as a right A-module, and for any basis $\{h_i\}_{i\in I}$ of H over k, $\{1_A\#h_i\}_{i\in I}$ is an A-basis of $A\#H$ as a right A-module.

Proof: i) We check associativity:

$$\begin{aligned} ((a\#h)(b\#g))(c\#e) &= \sum (a(h_1 \cdot b)\#h_2 g)(c\#e) \\ &= \sum a(h_1 \cdot b)(h_2 g_1 \cdot c)\#h_3 g_2 e \\ &= \sum a(h_1 \cdot (b(g_1 \cdot c)))\#h_2 g_2 e \\ &= (a\#h)(\sum b(g_1 \cdot c)\#g_2 e \\ &= (a\#h)((b\#g)(c\#e)), \end{aligned}$$

hence the multiplication is associative. The unit element is $1_A\#1_H$:

$$(a\#h)(1_A\#1_H) = \sum (a(h_1 \cdot 1_A)\#h_2)$$

$$\begin{aligned} &= \sum a\#\varepsilon(h_1)h_2 \\ &= a\#h = (1_A\#1_H)(a\#h). \end{aligned}$$

ii) It is clear that $(a\#1_H)(b\#1_H) = ab\#1_H$, $\forall a, b \in A$. We also have $(1_A\#h)(1_A\#g) = \sum h_1 \cdot 1_A\#h_2g = \sum 1_A\#\varepsilon(h_1)h_2 = 1_A\#hg$. The injectivity of the two morphisms follows immediately from the fact that 1_H (resp. 1_A) is linearly independent over k.
iii) The map $a\#h \longmapsto a \otimes h$ is an isomorphism of left A-modules from $A\#H$ to $A \otimes H$, where the left A-module structure on $A \otimes H$ is given by $a(b \otimes h) = ab \otimes h$.
iv) will follow from

Lemma 6.1.8 *If A is an H-module algebra, and S is bijective, we have*

$$a\#h = \sum (1_A\#h_2)(S^{-1}(h_1) \cdot a\#1_H).$$

Proof:

$$\begin{aligned} \sum (1_A\#h_2)(S^{-1}(h_1) \cdot a\#1_H) &= \sum (h_2 S^{-1}(h_1)) \cdot a\#h_3 \\ &= \sum \varepsilon(h_1)a\#h_2 = a\#h. \end{aligned}$$

∎

We return to the proof of *iv)* and define

$$\phi : A\#H \longrightarrow H \otimes A, \quad \phi(a\#h) = \sum h_2 \otimes S^{-1}(h_1) \cdot a,$$

and

$$\theta : H \otimes A \longrightarrow A\#H, \quad \theta(h \otimes a) = (1_A\#h)(a\#1_H).$$

By Lemma 6.1.8 it follows that $\theta \circ \phi = 1_{A\#H}$. Conversely,

$$\begin{aligned} (\phi \circ \theta)(h \otimes a) &= \phi((1_A\#h)(a\#1_H)) \\ &= \phi(\sum h_1 \cdot a\#h_2) \\ &= \sum h_3 \otimes S^{-1}(h_2)h_1 \cdot a \\ &= \sum h_2 \otimes \varepsilon(h_1)a = h \otimes a, \end{aligned}$$

hence also $\phi \circ \theta = 1_{H\otimes A}$. Since θ is a morphism of right A-modules, we deduce that $A\#H$ is isomorphic to $H \otimes A$ as right A-modules. ∎

We define now a new algebra, generalizing the smash product.

Definition 6.1.9 *Let H be a Hopf algebra which* acts weakly *on the algebra A (this means that A and H satisfy all conditions from Definition 6.1.1 with the exception of the associativity of multiplication with scalars from H: hence we do* **not** *necessarily have $h \cdot (l \cdot a) = (hl) \cdot a$ for $\forall h, l \in H$, $a \in A$. As it will soon be seen, this condition will be replaced by a weaker one). Let $\sigma : H \times H \longrightarrow A$ be a k-bilinear map. We denote by $A\#_\sigma H$ the k-vector space $A \otimes H$, together with a bilinear operation $(A \otimes H) \otimes (A \otimes H) \to (A \otimes H)$, $(a\#h) \otimes (b\#l) \mapsto (a\#h)(b\#l)$, given by the formula*

$$(a\#h)(b\#l) = \sum a(h_1 \cdot b)\sigma(h_2, l_1)\#h_3 l_2 \tag{6.1}$$

where we denoted $a \otimes h \in A \otimes H$ by $a\#h$. The object $A\#_\sigma H$, introduced above, is called a crossed product *if the operation is associative and $1_A\#1_H$ is the unit element (i.e. if it is an algebra).* ∎

Proposition 6.1.10 *The following assertions hold:*
i) $A\#_\sigma H$ is a crossed product if and only if the following conditions hold:
The normality condition for σ:

$$\sigma(1, h) = \sigma(h, 1) = \varepsilon(h)1_A, \ \ \forall h \in H \tag{6.2}$$

The cocycle condition:

$$\sum (h_1 \cdot \sigma(l_1, m_1))\sigma(h_2, l_2 m_2) = \sum \sigma(h_1, l_1)\sigma(h_2 l_2, m), \ \ \forall h, l, m \in H \tag{6.3}$$

The twisted module condition:

$$\sum (h_1 \cdot (l_1 \cdot a))\sigma(h_2, l_2) = \sum \sigma(h_1, l_1)((h_2 l_2) \cdot a), \ \ \forall h, l \in H, \ a \in A \tag{6.4}$$

For the rest of the assertions we assume that $A\#_\sigma H$ is a crossed product.
(ii) The map $a \longmapsto a\#1_H$, from A to $A\#_\sigma H$, is an injective morphism of k-algebras.
iii) $A\#_\sigma H \simeq A \otimes H$ as left A-modules.
iv) If σ is invertible (with respect to convolution), and S is bijective, then $A\#_\sigma H \simeq H \otimes A$ as right A-modules. In particular, in this case we deduce that $A\#_\sigma H$ is free as a left and right A-module.

Proof: i) We show that $1_A\#1_H$ is the unit element if and only if (6.2) holds. We compute:

$$(1_A\#1_H)(a\#h) = \sum 1_A(1_H \cdot a)\sigma(1, h_1)\#h_2 = \sum a\sigma(1, h_1)\#h_2.$$

Hence, if $\sigma(1, h) = \varepsilon(h)1_A$, $\forall h \in H$, it follows that $1_A\#1_H$ is a left unit element. Conversely, if $1_A\#1_H$ is a left unit element, applying $I \otimes \varepsilon$ to the equality

$$1_A\#h = \sum \sigma(1, h_1)\#h_2$$

we obtain $\varepsilon(h)1_A = \sigma(1,h)$. Similarly, one can show that $1_A\#1_H$ is a right unit element if and only if $\sigma(h,1) = \varepsilon(h)1_A$.
We assume now that (6.2) holds, and that the multiplication defined in 6.1 is associative, and we prove (6.3) and (6.4). Let $h,l,m \in H$ and $a \in A$.
From $(1\#h)((1\#l)(1\#m)) = ((1\#h)(1\#l))(1\#m)$ we deduce (6.3) after writing both sides and applying $I \otimes \varepsilon$.
From $(1\#h)((1\#l)(a\#m)) = ((1\#h)(1\#l))(a\#m)$ we deduce (6.4) after writing both sides, using (6.2) and applying $I \otimes \varepsilon$.
Conversely, we assume that (6.3) and (6.4) hold. Let $a,b,c \in A$ and $h,l,m \in H$. We have:

$$\begin{aligned}
&(a\#h)((b\#l)(c\#m)) = \\
&= \sum a(h_1 \cdot (b(l_1 \cdot c)\sigma(l_2,m_1)))\sigma(h_2,l_3m_2)\#h_3l_4m_3 \\
&= \sum a(h_1 \cdot b)(h_2 \cdot (l_1 \cdot c))(h_3 \cdot \sigma(l_2,m_1))\sigma(h_4,l_3m_2)\#h_5l_4m_3 \\
&= \sum a(h_1 \cdot b)(h_2 \cdot (l_1 \cdot c))\sigma(h_3,l_2)\sigma(h_4l_3,m_1)\#h_5l_4m_2 \\
&= \sum a(h_1 \cdot b)\sigma(h_2,l_1)(h_3l_2 \cdot c))\sigma(h_4l_3,m_1)\#h_5l_4m_2,
\end{aligned}$$

where we used, $(MA2)$ for the second equality, (6.3) for h_3,l_2,m_1 for the third one, and (6.4) for h_2,l_1,c for the fourth.
On the other hand,
$((a\#h)(b\#l))(c\#m) = \sum a(h_1 \cdot b)\sigma(h_2,l_1)((h_3l_2) \cdot c))\sigma(h_4l_3,m_1)\#h_5l_4m_2$, hence the multiplication of $A\#_\sigma H$ is associative.
ii) and iii) are clear.
iv) We define

$$\alpha : H \otimes A \longrightarrow A\#_\sigma H,$$
$$\alpha(h \otimes a) = \sum \sigma^{-1}(h_2, S^{-1}(h_1))(h_3 \cdot a)\#h_4,$$

where σ^{-1} is the convolution inverse of σ, and S^{-1} is the composition inverse of S. We also define

$$\beta : A\#_\sigma H \longrightarrow H \otimes A,$$
$$\beta(a\#h) = \sum h_4 \otimes (S^{-1}(h_3) \cdot a)\sigma(S^{-1}(h_2), h_1).$$

We show that α and β are isomorphisms of right A-modules, inverse one to each other. We prove first the following

Lemma 6.1.11 *If σ is invertible, the following assertions hold for any $h,l,m \in H$:*
a) $h \cdot \sigma(l,m) = \sum \sigma(h_1,l_1)\sigma(h_2l_2,m_1)\sigma^{-1}(h_3,l_3m_2)$.
b) $h \cdot \sigma^{-1}(l,m) = \sum \sigma(h_1,l_1m_1)\sigma^{-1}(h_2l_2,m_2)\sigma^{-1}(h_3,l_3)$.
c) $\sum(h_1 \cdot \sigma^{-1}(S(h_4),h_5))\sigma(h_2,S(h_3)) = \varepsilon(h)1_A$.

Proof: First, if σ^{-1} is the convolution inverse of σ, we have

$$\sum \sigma^{-1}(l_1, m_1)\sigma(l_2, m_2) = \sum \sigma(l_1, m_1)\sigma^{-1}(l_2, m_2) =$$

$$= \varepsilon(l)\varepsilon(m)1_A, \quad \forall l, m \in H.$$

a) We have

$$\begin{aligned} h \cdot \sigma(l, m) &= \sum (h_1 \cdot \sigma(l_1, m_1))\varepsilon(h_2)\varepsilon(l_2)\varepsilon(m_2)1_A \\ &= \sum (h_1 \cdot \sigma(l_1, m_1))\varepsilon(h_2)\varepsilon(l_2 m_2)1_A \\ &= \sum (h_1 \cdot \sigma(l_1, m_1))\sigma(h_2, l_2 m_2)\sigma^{-1}(h_3, l_3 m_3) \\ &= \sum \sigma(h_1, l_1)\sigma(h_2 l_2, m_1)\sigma^{-1}(h_3, l_3 m_2), \end{aligned}$$

where we used (6.3) for the last equality.
b) Multiplying by $h \in H$ both sides of the equality

$$\sum \sigma^{-1}(l_1, m_1)\sigma(l_2, m_2) = \varepsilon(l)\varepsilon(m)1_A,$$

we get

$$\sum (h_1 \cdot \sigma^{-1}(l_1, m_1))(h_2 \cdot \sigma(l_2, m_2)) = \varepsilon(h)\varepsilon(l)\varepsilon(m)1_A.$$

We deduce that the map $h \otimes l \otimes m \longmapsto h \cdot \sigma^{-1}(l, m)$, from $H \otimes H \otimes H$ to A, is the convolution inverse of the map $h \otimes l \otimes m \longmapsto h \cdot \sigma(l, m)$. To finish the proof of b), we show that the right hand sides of the equalities in a) and b) are each other's convolution inverse. Indeed,

$$\sum \sigma(h_1, l_1)\sigma(h_2 l_2, m_1)\sigma^{-1}(h_3, l_3 m_2)$$

$$\sigma(h_4, l_4 m_3)\sigma^{-1}(h_5 l_5, m_4)\sigma^{-1}(h_6, l_6) =$$

$$= \sum \sigma(h_1, l_1)\sigma(h_2 l_2, m_1)\varepsilon(h_3)\varepsilon(l_3)\varepsilon(m_2)\sigma^{-1}(h_4 l_4, m_3)\sigma^{-1}(h_5, l_5) =$$

$$= \sum \sigma(h_1, l_1)\sigma(h_2 l_2, m_1)\sigma^{-1}(h_3 l_3, m_2)\sigma^{-1}(h_4, l_4) = \varepsilon(h)\varepsilon(l)\varepsilon(m)1_A.$$

c) The left hand side of the equality becomes, after applying b) for $h_1, S(h_4), h_5$:

$$\sum \sigma(h_1, S(h_8)h_9)\sigma^{-1}(h_2 S(h_7), h_{10})\sigma^{-1}(h_3, S(h_6))\sigma(h_4, S(h_5)) =$$

$$= \sum \sigma(h_1, S(h_6)h_7)\sigma^{-1}(h_2 S(h_5), h_8)\varepsilon(h_3)\varepsilon(h_4) =$$

$$= \sum \sigma(h_1, S(h_4)h_5)\sigma^{-1}(h_2 S(h_5), h_6) =$$

$$= \sum \sigma(h_1, \varepsilon(h_3)1_H)\sigma^{-1}(\varepsilon(h_2)1_H, h_4) =$$

$$= \sum \varepsilon(h_1)\varepsilon(h_2)\varepsilon(h_3)\varepsilon(h_4)1_A = \varepsilon(h)1_A,$$

and the proof of the lemma is complete. ∎

We go back to the proof of the proposition and show that α and β are each other's inverse. We compute

$$(\beta \circ \alpha)(h \otimes a) =$$

$$= \sum h_7 \otimes (S^{-1}(h_6) \cdot (\sigma^{-1}(h_2, S^{-1}(h_1))(h_3 \cdot a)))\sigma(S^{-1}(h_5), h_4)$$

$$= \sum h_8 \otimes (S^{-1}(h_7) \cdot \sigma^{-1}(h_2, S^{-1}(h_1)))$$

$$(S^{-1}(h_6) \cdot (h_3 \cdot a))\sigma(S^{-1}(h_5), h_4) \text{ (by } (MA2))$$

$$= \sum h_8 \otimes (S^{-1}(h_7) \cdot \sigma^{-1}(h_2, S^{-1}(h_1)))$$

$$\sigma(S^{-1}(h_6), h_3)((S^{-1}(h_5)h_4) \cdot a) \text{ (by (6.4))}$$

$$= \sum h_7 \otimes (S^{-1}(h_6) \cdot \sigma^{-1}(h_2, S^{-1}(h_1)))\sigma(S^{-1}(h_5), h_3)\varepsilon(h_4)a$$

$$= \sum h_6 \otimes (S^{-1}(h_6) \cdot \sigma^{-1}(h_2, S^{-1}(h_1)))\sigma(S^{-1}(h_4), h_3)a$$

$$= \sum h_2 \otimes \varepsilon(S^{-1}(h_1))a \text{ (by Lemma 6.1.11, c) for } S^{-1}(h_1))$$

$$= \sum h_2 \otimes \varepsilon(h_1)a = h \otimes a,$$

hence $\beta \circ \alpha = 1_{H \otimes A}$. Conversely,

$$(\alpha \circ \beta)(a\#h) =$$

$$= \sum \sigma^{-1}(h_5, S^{-1}(h_4))(h_6 \cdot ((S^{-1}(h_3) \cdot a)\sigma(S^{-1}(h_2), h_1))\#h_7$$

$$= \sum \sigma^{-1}(h_5, S^{-1}(h_4))(h_6 \cdot (S^{-1}(h_3) \cdot a))$$

$$(h_7 \cdot \sigma(S^{-1}(h_2), h_1))\#h_8 \text{ (by } (MA2))$$

$$= \sum \sigma^{-1}(h_8, S^{-1}(h_7))(h_9 \cdot (S^{-1}(h_6) \cdot a))\sigma(h_{10}, S^{-1}(h_5))\sigma(h_{11}S^{-1}(h_4), h_1)$$

$$\sigma^{-1}(h_{12}, S^{-1}(h_3)h_2)\#h_{13} \text{ (by Lemma 6.1.11, a))}$$

$$= \sum \sigma^{-1}(h_6, S^{-1}(h_5))(h_7 \cdot (S^{-1}(h_4) \cdot a))$$

$$\sigma(h_8, S^{-1}(h_3))\sigma(h_9S^{-1}(h_2), h_1)\#h_{10}$$

$$= \sum \sigma^{-1}(h_6, S^{-1}(h_5))\sigma(h_7, S^{-1}(h_4))((h_8S^{-1}(h_3)) \cdot a)$$

$$\sigma(h_9S^{-1}(h_2),h_1)\#h_{10} \text{ (din (6.4))}$$
$$=\sum \varepsilon(h_5)\varepsilon(h_4)((h_6S^{-1}(h_3))\cdot a)\sigma(h_7S^{-1}(h_2),h_1)\#h_8$$
$$=\sum((h_4S^{-1}(h_3))\cdot a)\sigma(h_5S^{-1}(h_2),h_1)\#h_6$$
$$=\sum \varepsilon(h_3)a\sigma(h_4S^{-1}(h_2),h_1)\#h_5$$
$$=\sum a\sigma(h_3S^{-1}(h_2),h_1)\#h_5=\sum a\varepsilon(h_2)\sigma(1,h_1)\#h_3$$
$$=\sum a\varepsilon(h_1)\#h_2=a\#h,$$

hence also $\alpha\circ\beta=1_{A\#_\sigma H}$. Finally, we note that

$$\begin{aligned}\alpha(h\otimes a)b &= \alpha(h\otimes a)(b\#1)\\ &= \sum(\sigma^{-1}(h_2,S^{-1}(h_1))(h_3\cdot a)\#h_4)(b\#1)\\ &= \sum\sigma^{-1}(h_2,S^{-1}(h_1))(h_3\cdot a)(h_4\cdot b)\sigma(h_5,1)\#h_6\\ &= \sum\sigma^{-1}(h_2,S^{-1}(h_1))(h_3\cdot(ab))\#h_4\\ &= \alpha(h\otimes ab)=\alpha((h\otimes a)b),\end{aligned}$$

hence α is a morphism of right A-modules. It follows that α is an isomorphism of right A-modules, and the proof is complete. ∎

Remark 6.1.12 *In case $\sigma: H\otimes H \longrightarrow A$ is trivial, i.e. $\sigma(h,l)=\varepsilon(h)\varepsilon(l)1_A$, A is even an H-module algebra, and the crossed product $A\#_\sigma H$ is the smash product $A\#H$.* ∎

We look now at some examples of actions:

Example 6.1.13 *(Examples of Hopf algebras acting on algebras)*

1) Let G be a finite group acting as automorphisms on the k-algebra A. If we put $H=kG$, with $\Delta(g)=g\otimes g$, $\varepsilon(g)=1$, $S(g)=g^{-1}$, $\forall g\in G$, and $g\cdot a=g(a)=a^g$, $a\in A$, $g\in G$, then A is an H-module algebra, as it may be easily seen. The smash product $A\#H$ is in this case the skew group ring $A*G$ (we recall that this is the group ring, in which multiplication is altered as follows:

$$(ag)(bh)=(ab^g)(gh),$$

$\forall a,b\in A,\ g,h\in G$), and $A^H=A^G$ is the subalgebra of the elements fixed by G (which explains the name of algebra of the invariants, given to A^H in general).
The smash product $A\#H$ is sometimes called the semidirect product. Here is why. Let K be a group acting as automorphisms on the group H (i.e.

there exists a morphism of groups $\phi : K \longrightarrow Aut(H)$). Then K acts as automorphisms on the group ring kH, which becomes in this way a kK-module algebra. Since in $kH\#kK$ we have, by the definition of the multiplication,

$$(h\#k)(h'\#k') = h(k \cdot h')\#kk' = h\phi(k)(h')\#kk',$$

we obtain that $kH\#kK \simeq k(H \times_\phi K)$, where $H \times_\phi K$ is the semidirect product of the groups H and K.

2) Let G be a finite group, and A a graded k-algebra of type G. This means that $A = \bigoplus_{g\in G} A_g$ (direct sum of k-vector spaces), such that $A_gA_h \subseteq A_{gh}$. If $1 \in G$ is the unit element, A_1 is a subalgebra of A. Each element $a \in A$ writes uniquely as $a = \sum_{g\in G} a_g$. The elements $a_g \in A_g$ are called the homogeneous components of a. Let $H = kG^* = Hom_k(kG, k)$, with dual basis $\{p_g \mid g \in G,\ p_g(h) = \delta_{g,h}\}$. The elements p_g are a family of orthogonal idempotents, whose sum is 1_H. We recall that H is a Hopf algebra with $\Delta(p_g) = \sum_{h\in G} p_{gh^{-1}} \otimes p_h$, $\varepsilon(p_g) = \delta_{g,1}$, $S(p_g) = p_{g^{-1}}$. For $a \in A$ we put $p_g \cdot a = a_g$, the homogeneous component of degree g of a. In this way, A becomes an H-module algebra, since $p_g \cdot (ab) = (ab)_g = \sum_{h\in G} a_{gh^{-1}}b_h = \sum_{h\in G} (p_{gh^{-1}} \cdot a)(p_h \cdot b)$. The smash product $A\#kG^*$ is the free left A-module with basis $\{p_g \mid g \in G\}$, in which multiplication is given by

$$(ap_g)(bp_h) = ab_{gh^{-1}}p_h, \quad \forall a, b \in A,\ g, h \in G.$$

The subalgebra of the invariants is in this case A_1, the homogeneous component of degree 1 of A.

3) Let L be a Lie algebra over k, and A a k-algebra such that L acts on A as derivations (this means that there exists $\alpha : L \longrightarrow Der_k(A)$ a morphism of Lie algebras). For $x \in L$ and $a \in A$, we denote by $x \cdot a = \alpha(x)(a)$. Let $H = U(L)$, be the universal enveloping algebra of L (for $x \in L$ $\Delta(x) = x \otimes 1 + 1 \otimes x$, $\varepsilon(x) = 0$, $S(x) = -x$). Since H is generated by monomials of the form $x_1 \ldots x_n$, $x_i \in L$, we put

$$x_1 \ldots x_n \cdot a = x_1 \cdot (x_2 \cdot (\ldots (x_n \cdot a) \ldots)), \quad a \in A.$$

In this way, A becomes an H-module algebra, and $A^H = \{a \in A \mid x \cdot a = 0,\ \forall x \in L\}$.

4) Any Hopf algebra H acts on itself by the *adjoint action*, defined by

$$h \cdot l = (ad\, h)l = \sum h_1 l S(h_2).$$

This action extends the usual ones from the case $H = kG$, where $(ad\ x)y = xyx^{-1}$, $x, y \in G$, or from the case $H = U(L)$, where $(ad\ x)h = xh - hx$, $x \in L$, $h \in H$ (the second case shows the origin of the name of this action). We have then $H^H = Z(H)$ (center of H). Indeed, if $g \in H^H$, then $\forall h \in H$

$$\begin{aligned} hg &= \sum h_1\varepsilon(h_2)g = \sum h_1 g\varepsilon(h_2) \\ &= \sum h_1 g S(h_2)h_3 = \sum \varepsilon(h_1)gh_2 = gh \end{aligned}$$

The reverse inclusion is obvious.
5) If H is a Hopf algebra, then H^* is a left (and right) H-module algebra with actions defined by $(h \rightharpoonup h^*)(g) = h^*(gh)$ (and $(h^* \leftharpoonup h)(g) = h^*(hg)$) for all $h, g \in H$, $h^* \in H^*$. ∎

6.2 Coactions of Hopf algebras on algebras

We have seen in Example 6.1.13 2) that a grading by an finite group G on an algebra is an example of an action of a Hopf algebra. To study the case when G is infinite requires the notion of a coaction of a Hopf algebra on an algebra.

Definition 6.2.1 *Let H be a Hopf algebra, and A a k-algebra. We say that H* coacts *to the right on A (or that A is a right H-*comodule algebra*) if the following coditions are fulfilled:*
(CA1) A is a right H-comodule, with structure map

$$\rho : A \longrightarrow A \otimes H, \quad \rho(a) = \sum a_0 \otimes a_1,$$

(CA2) $\sum (ab)_0 \otimes (ab)_1 = \sum a_0 b_0 \otimes a_1 b_1, \quad \forall a, b \in A.$
(CA3) $\rho(1) = 1_A \otimes 1_H$.
The notion of a left H-comodule algebra is defined similarly. If no mention of the contrary is made, we will understand by an H-comodule algebra a right H-comodule algebra. ∎

The following result shows that, unlike condition $(MA2)$ from the definition of H-module algebras, conditions $(CA2)$ and $(CA3)$ may be interpreted in both possibile ways.

Proposition 6.2.2 *Let H be a Hopf algebra, and A a k-algebra which is a right H-comodule with structural morphism $\rho : A \longrightarrow A \otimes H$. The following assertions are equivalent:*
i) A is an H-comodule algebra.

ii) ρ *is a morphism of algebras.*
iii) The multiplication of A *is a morphism of comodules (the right comodule structure on* $A \otimes A$ *is given by* $a \otimes b \longmapsto \sum a_0 \otimes b_0 \otimes a_1 b_1$*), and the unit of* A, $u : k \longrightarrow A$ *is a morphism of comodules.*

Proof: Obvious. ∎

As in the case of actions, we can define a subalgebra of an H-comodule algebra using the coaction.

Definition 6.2.3 *Let* A *be an* H*-comodule algebra. The following subalgebra of* A

$$A^{coH} = \{a \in A \mid \rho(a) = a \otimes 1\}.$$

is called the algebra of the coinvariants *of* A. ∎

In case H is finite dimensional, we have the following natural connection between actions and coactions.

Proposition 6.2.4 *Let* H *be a finite dimensional Hopf algebra, and* A *a* k*-algebra. Then* A *is a (right)* H*-comodule algebra if and only if* A *is a (left)* H^**-module algebra. Moreover, in this case we also have that* $A^{H^*} = A^{coH}$.

Proof: Let $n = dim_k(H)$, and $\{e_1, \ldots, e_n\} \subset H$, $\{e_1^*, \ldots, e_n^*\} \subset H^*$ be dual bases, i.e. $e^*(e_j) = \delta_{ij}$.
Assume that A is an H-comodule algebra. Then A becomes an H^*-module algebra with

$$f \cdot a = \sum a_0 f(a_1), \quad \forall f \in H^*, \ a \in A.$$

Indeed, we know already that A is a left H^*-module, and

$$\begin{aligned} f \cdot (ab) &= \sum (ab)_0 f((ab)_1) \\ &= \sum a_0 b_0 f(a_1 b_1) \\ &= \sum a_0 b_0 f_1(a_1) f_2(b_1) \\ &= \sum a_0 f_1(a_1) b_0 f_2(b_1) \\ &= \sum (f_1 \cdot a)(f_2 \cdot b). \end{aligned}$$

Conversely, if A is a left H^*-module algebra, A is a right H-comodule with

$$\rho : A \longrightarrow A \otimes H, \quad \rho(a) = \sum_{i=1}^{n} e_i^* \cdot a \otimes e_i.$$

We have, for any $f \in H^*$

$$
\begin{aligned}
(I \otimes f)(\rho(ab)) &= \sum_{i=1}^{n} e_i^* \cdot (ab) \otimes f(e_i) \\
&= \sum_{i=1}^{n} (e_i^* f(e_i)) \cdot (ab) \otimes 1 \\
&= f \cdot (ab) \otimes 1 \\
&= \sum (f_1 \cdot a)(f_2 \cdot b) \otimes 1 \\
&= \sum_{i,j=1}^{n} ((e_i^* f_1(e_i)) \cdot a)((e_j^* f_2(e_j)) \cdot b) \otimes 1 \\
&= \sum_{i,j=1}^{n} (e_i^* \cdot a)(e_j^* \cdot b) \otimes f_1(e_i) f_2(e_j) \\
&= \sum_{i,j=1}^{n} (e_i^* \cdot a)(e_j^* \cdot b) \otimes f(e_i e_j) \\
&= (I \otimes f)(\sum_{i,j=1}^{n} (e_i^* \cdot a)(e_j^* \cdot b) \otimes e_i e_j) \\
&= (I \otimes f)(\rho(a)\rho(b)),
\end{aligned}
$$

and so $\rho(ab) = \rho(a)\rho(b)$. Finally,

$$
\begin{aligned}
\rho(1) &= \sum_{i=1}^{n} e_i^* \cdot 1 \otimes e_i = \sum_{i=1}^{n} e_i^*(1) 1 \otimes e_i \\
&= \sum_{i=1}^{n} 1 \otimes e_i^*(1) e_i = 1_A \otimes 1_H.
\end{aligned}
$$

We now have

$$
\begin{aligned}
A^{H^*} &= \{a \in A \mid f \cdot a = f(1)a, \ \forall f \in H^*\} \\
&= \{a \in A \mid \sum a_0 f(a_1) = f(1)a, \ \forall f \in H^*\} \\
&= \{a \in A \mid (Id \otimes f)(\rho(a)) = (Id \otimes f)(a \otimes 1), \ \forall f \in H^*\} \\
&= \{a \in A \mid \rho(a) = a \otimes 1\} = A^{coH}.
\end{aligned}
$$

∎

Example 6.2.5 *(Examples of coactions of Hopf algebras on algebras)*

1) Any Hopf algebra H is an H-comodule algebra (left and right) with comodule structure given by Δ. Let us compute H^{coH}. If $h \in H^{coH}$, we have $\Delta(h) = \sum h_1 \otimes h_2 = h \otimes 1$. Applying $I \otimes \varepsilon$ to both sides, we obtain $h = \varepsilon(h)1$, hence $H^{coH} \subseteq k1$. Since the reverse inclusion is clear, we have $H^{coH} = k1$.

2) Let G be an arbitrary group, and A a graded k-algebra of type G (see Example 6.1.13, 2)). Then A is a kG-comodule algebra with comodule structure given by

$$\rho : A \longrightarrow A \otimes kG, \ \ \rho(a) = \sum_{g \in G} a_g \otimes g,$$

where $a = \sum_{g \in G} a_g$, $a_g \in A_g$ almost all of them zero. We also have $A^{co\ kG} = A_1$.

3) Let $A \#_\sigma H$ be a crossed product. This becomes an H-comodule algebra with

$$\rho : A\#_\sigma H \longrightarrow A\#_\sigma H \otimes H, \ \ \rho(a\#h) = \sum (a\#h_1) \otimes h_2.$$

We have $(A\#_\sigma H)^{coH} = A\#_\sigma 1 \simeq A$. Indeed, if $a\#h \in (A\#_\sigma H)^{coH}$, then applying $I \otimes I \otimes \varepsilon$ to the equality $\rho(a\#h) = (a\#h) \otimes 1$ we obtain $a\#h \in A\#_\sigma 1$, and the reverse inclusion is clear. Since the smash product is a particular case of a crossed product, the assertion also hold for a smash product $A\#H$. ∎

It is possible to associate different smash products to a right H-comodule algebra A. First, the smash product $\#(H, A)$ is the k-vector space $Hom(H, A)$ with multiplication given by

$$(f \cdot g)(h) = \sum f(g(h_2)_1 h_1) g(h_2)_0, \ \ f, g \in \#(H, A), \ h \in H. \qquad (6.5)$$

Exercise 6.2.6 *With the multiplication defined in (6.5), $\#(H, A)$ is an associative ring with multiplicative identity $u_H \varepsilon_H$. Moreover, A is isomorphic to a subalgebra of $\#(H, A)$ by identifying $a \in A$ with the map $h \longmapsto \varepsilon(h)a$. Also $H^* = Hom(H, k)$ is a subalgebra of $\#(H, A)$.*

Remark 6.2.7 *If we take k with the H-comodule algebra structure given by u_H, then the multiplication from (6.5) is just the convolution product.* ∎

We can also construct the (right) smash product of A with U, where U is any right H-module subring of H^*, (i.e. possibly without a 1). This smash product, written $A\#U$, is the tensor product $A \otimes U$ over k but with multiplication given by

$$(a\#h^*)(b\#g^*) = \sum ab_0 \#(h^* \leftharpoonup b_1) g^*.$$

If H is co-Frobenius, H^{*rat} is a right H-module subring of H^*, $A\#H^{*rat}$ makes sense and is an ideal (a proper ideal if H is infinite dimensional) of $A\#H^*$. In fact, $A\#H^{*rat}$ is the largest rational submodule of $A\#H^*$ where $A\#H^*$ has the usual left H^*-action given by multiplication by $1\#H^*$. To see this, note that $A\#H^*$ is isomorphic as a left H^*-module to $H^* \otimes A$, where the left H^*-action on $H^* \otimes A$ is given by multiplication by $H^* \otimes 1$. The isomorphism is given by the H^*-module map

$$\phi : H^* \otimes A \longrightarrow A\#H^*, \quad \phi(h^* \otimes a) = \sum a_0 \# h^* \leftharpoonup a_1. \tag{6.6}$$

with inverse ψ defined by $\psi(a\#h^*) = \sum h^* \leftharpoonup S^{-1}(a_1) \otimes a_0$.

Since $(H^* \otimes A)^{rat} = H^{*rat} \otimes A, (A\#H^*)^{rat} = \phi(H^{*rat} \otimes A) = A\#H^{*rat}$. Thus we have

$$A\#H^{*rat} = (A\#H^*)^{rat} \subseteq A\#H^* \subseteq \#(H, A)$$

If H is finite-dimensional, then H is a left H^*-module algebra, and these smash products are all equal (this is the usual smash product from the previous section). Note that the idea for the definition of (6.5) comes naturally by transporting the smash product structure from $A\#H^*$ to $Hom(H, A)$ via the isomorphism of vector spaces from Lemma 1.3.2.

Exercise 6.2.8 *In general, $A\#H^{*rat}$ is properly contained in $\#(H, A)^{rat}$.*

Remark 6.2.9 *Let us remark that for graded rings A over an infinite group G, $A\#(kG)^{*rat}$ is just Beattie's smash product [21].*
We can adjoin a 1 to $A\#H^{*rat}$ in the standard way. Let $(A\#H^{*rat})^1 = A\#H^{*rat} \times A$ with componentwise addition and multiplication given by

$$(a\#h^*, c)(b\#g^*, d) = ((a\#h^*)(b\#g^*) + (\sum ad_0\#h^* \leftharpoonup d_1) + cb\#g^*, cd).$$

Then $(A\#H^{*rat})^1$ is an associative ring with multiplicative identity (0,1) and with $A\#H^{*rat}$ isomorphic to an ideal in $(A\#H^{*rat})^1$ via $i(x) = (x, 0)$. Again, for graded rings A over an infinite group G, $(A\#(kG)^{*rat})^1$ is just Quinn's smash product [184]. ∎

We define now the categories of relative Hopf modules (left and right).

Definition 6.2.10 *Let H be a Hopf algebra, A an H-comodule algebra. We say that M is a* left (A, H)-Hopf module *if M is a left A-module and a right H-comodule (with $m \mapsto \sum m_0 \otimes m_1$), such that the following relation holds.*

$$\sum (am)_0 \otimes (am)_1 = \sum a_0 m_0 \otimes a_1 m_1, \quad a \in A, \; m \in M. \tag{6.7}$$

We denote by ${}_A\mathcal{M}^H$ the category whose objects are the left (A,H)-Hopf modules, and in which the morphisms are the maps which are A-linear and H-colinear.
We say that M is a right (A,H)-Hopf module *if M is a right A-module and a right H-comodule (with $m \mapsto \sum m_0 \otimes m_1$), such that the following relation holds.*

$$\sum (ma)_0 \otimes (ma)_1 = \sum m_0 a_0 \otimes m_1 a_1, \quad a \in A,\ m \in M. \tag{6.8}$$

We denote by $\mathcal{M}_A^H$ the category with objects the right (A,H)-Hopf modules, and morphisms linear maps which are A-linear and H-colinear.
Similar definitions may be given for left H-comodule algebras. If A is such an algebra, the objects of the category ${}_A^H\mathcal{M}$ are left A-modules and left H-comodules M satisfying the relation

$$\sum (am)_{-1} \otimes (am)_0 = \sum a_{-1}m_{-1} \otimes a_0 m_0,$$

for all $a \in A$, $m \in M$, and the objects of the category ${}^H\mathcal{M}_A$ are right A-modules and left H-comodules M satisfying the relation

$$\sum (ma)_{-1} \otimes (ma)_0 = \sum m_{-1}a_{-1} \otimes a_0 m_0,$$

for all $a \in A$, $m \in M$.

If M is a left H-module, we denote by

$$M^H = \{m \in M \mid h \cdot m = \varepsilon(h)m, \ \ \forall h \in H\}.$$

If A is a left H-module algebra, and M is also a left $A\#H$-module, it may be easily checked that M^H is an A^H-submodule of M. If M is a right H-comodule with $m \mapsto \sum m_0 \otimes m_1$, we denote by

$$M^{coH} = \{m \in M \mid \sum m_0 \otimes m_1 = m \otimes 1\}.$$

If A is a right H-comodule algebra, and M is also a right (A,H)-module, it may be checked that M^{coH} is an A^{coH}-submodule of M.
The following result characterizes the categories of relative Hopf modules in case H is co-Frobenius.

Proposition 6.2.11 *Let H be a co-Frobenius Hopf algebra, and A a right H-comodule algebra. Then:*
i) The category ${}_A\mathcal{M}^H$ is isomorphic to the category of left unital $A\#H^{*rat}$-modules (i.e. modules M such that $M = (A\#H^{*rat}) \cdot M$), denoted by ${}_{A\#H^{*rat}}\mathcal{M}^u$.
ii) The category $\mathcal{M}_A^H$ is isomorphic to the category of right unital $A\#H^{*rat}$-modules, denoted by $\mathcal{M}^u_{A\#H^{*rat}}$.

Proof: i) The reader is first invited to solve the following

Exercise 6.2.12 *Let H be co-Frobenius Hopf algebra and M a unital left $A\#H^{*rat}$-module. Then for any $m \in M$ there exists an $u^* \in H^{*rat}$ such that $m = u^* \cdot m = (1\#u^*) \cdot m$, so M is a unital left H^{*rat}-module, and therefore a rational left H^*-module.*

Let $M \in {}_{A\#H^{*rat}}\mathcal{M}^u$. The Exercise shows that M is a rational left H^*-module, and therefore a right H-comodule. M also becomes a left $A\#H^*$-module via

$$(a\#h^*) \cdot m = (a\#h^*u^*) \cdot m$$

for $a \in A$, $h^* \in H^*$, $m \in M$, $u^* \in H^{*rat}$, and $m = u^* \cdot m$. The definition is correct, because we can find a common left unit for finitely many elements in H^{*rat}. Now we turn M into a left A-module by putting $a \cdot m = (a\#\varepsilon) \cdot m$. We have

$$\begin{aligned} h^* \cdot (a \cdot m) &= (1\#h^*)(a\#\varepsilon) \cdot m \\ &= \sum (a_0\#h^* \leftharpoonup a_1) \cdot m \\ &= \sum (a_0\#\varepsilon)(1\#h^* \leftharpoonup a_1) \cdot m \\ &= \sum (a_0\#\varepsilon) \cdot (h^* \leftharpoonup a_1)(m_1)m_0 \\ &= \sum a_0 \cdot m_0 (h^* \leftharpoonup a_1)(m_1), \end{aligned}$$

so $M \in {}_A\mathcal{M}^H$.
Conversely, if $M \in {}_A\mathcal{M}^H$, then M becomes a left H^*-module with $H^{*rat} \cdot M = M$, and a left $A\#H^*$-module via

$$(a\#h^*) \cdot m = \sum a m_0 h^*(m_1).$$

Then

$$(a\#h^*)((b\#g^*) \cdot m) = \sum ab_0 m_0 g^*(a_1 m_1) h^*(m_2) = ((a\#h^*)(b\#g^*)) \cdot m,$$

so M becomes a unital left $A\#H^{*rat}$-module. It is clear that the above correspondences define functors (which are the identity on morphisms) establishing the desired category isomorphism.
ii) The proof is along the same lines as the one above. It should be noted that H^{*rat} is stabilized by the antipode, which is an automorphism of H considered as a k-vector space, and so if $h^* \in H^*$ with $Ker(h^*) \supseteq I$, I a finite codimensional coideal, then $Ker(h^*S) \supseteq S^{-1}(I)$, which is also a

coideal of finite codimension. We also note that if $M \in \mathcal{M}_A^H$, then the right $A\#H^*$-module structure on M is given by

$$m \cdot (a\#h^*) = \sum m_0 a_0 h^*(S^{-1}(m_1 a_1)).$$

∎

Exercise 6.2.13 *Consider the right H-comodule algebra A with the left and right $A\#H^*$-module structures given by the fact that $A \in \mathcal{M}_A^H$ and $A \in {}_A\mathcal{M}^H$:*

$$a \cdot (b\#h^*) = \sum a_0 b_0 h^*(S^{-1}(a_1 b_1)), \quad (b\#h^*) \cdot a = \sum b a_0 h^*(a_1).$$

Then A is a left $A\#H^*$ and right A^{coH}-bimodule, and a left A^{coH} and right $A\#H^*$-bimodule. Consequently, the map

$$\pi : A\#H^{*rat} \longrightarrow End(A_{A^{coH}}), \quad \pi(a\#l)(b) = (a\#l) \cdot b,$$

is a ring morphism.

Exercise 6.2.14 *Let A be a right H-comodule algebra and consider A as a left or right $A\#H^{*rat}$-module as in Exercise 6.2.13. Then:*
i) $A^{coH} \simeq End({}_{A\#H^{*rat}}A)$
ii) $A^{coH} \simeq End(A_{A\#H^{*rat}})$.

Example 6.2.15 *1) If H is a Hopf algebra, H is a right comodule algebra as in Example 6.2.5, 1), then the categories ${}_H\mathcal{M}^H$ and $\mathcal{M}_H^H$ are the usual categories of Hopf modules.*
2) If G is a group, $H = kG$, and A is a graded k-algebra of type G (see Example 6.2.5, 2)), then the category ${}_A\mathcal{M}^H$ (respectively $\mathcal{M}_A^H$) is the category of left (resp. right) A-modules graded over G. ∎

Proposition 6.2.16 *If H is a co-Frobenius Hopf algebra, and $0 \neq t \in \int_l$, let $M \in {}_A\mathcal{M}^H$ (resp. $M \in \mathcal{M}_A^H$). Then:*
i) $t \cdot M \subseteq M^{coH}$
ii) If $m \in M^{coH}$ and $c \in A$, then $t \cdot (cm) = (t \cdot c)m$
(resp. $t \cdot (mc) = m(t \cdot c)$).
In particular, the map $M \longrightarrow M^{coH}$, $m \mapsto t \cdot m$ is a morphism of A^{coH}-bimodules.

Proof: We prove only one of the cases.
i) If $h^* \in H^*$, then $h^* \cdot (t \cdot m) = (h^* t) \cdot m = h^*(1)t \cdot m$.
ii) $t \cdot (cm) = \sum t(c_1 m_1) c_0 m_0 = \sum t(c_1) c_0 m = (t \cdot c)m$. ∎

Corollary 6.2.17 *If H is a finite dimensional Hopf algebra, $0 \neq t \in H$ is a left integral, and A is a left H-module algebra, the map*

$$tr : A \longrightarrow A^H, \ \ tr(a) = t \cdot a$$

is a morphism of A^H-bimodules. ∎

Definition 6.2.18 *The map tr from Corollary 6.2.17 is called the* trace function. *We say that the the H-module algebra A has an element of trace 1 if tr is surjective, i.e. there exists an $a \in A$ with $t \cdot a = 1$.* ∎

Example 6.2.19 *1) Let G be a finite group acting on the k-algebra A as automorphisms (see Example 6.1.13, 1)). Then $t = \sum_{g\in G} g$ is a left integral in $H = kG$, and the trace function is in this case*

$$tr : A \longrightarrow A^G, \ \ tr(a) = \sum_{g\in G} a^g.$$

In case A is a field, a Galois extension with Galois group G, the trace function is then exactly the trace function defined e.g. in N. Jacobson [99, p.284], which justifies the choice for the name. The connection with the trace of a matrix is the following: in the Galois case, the trace of an element is the trace of the image of this element in the matrix ring via the regular representation (cf. [99, p.403]).
2) If H is semisimple, then any H-module algebra has an element of trace 1. Indeed, if t is an integral with $\varepsilon(t) = 1$, then $t \cdot 1 = 1$. ∎

Exercise 6.2.20 *(Maschke's Theorem for smash products) Let H be a semisimple Hopf algebra, and A a left H-module algebra. Let V be a left $A\#H$-module, and W an $A\#H$-submodule of V. If W is a direct summand in V as A-modules, then it is a direct summand in V as $A\#H$-modules.*

6.3 The Morita context

Let H be a co-Frobenius Hopf algebra, t a nonzero left integral on H, and A a right H-comodule algebra. In this section, we construct a Morita context connecting $A\#H^{*rat}$ and A^{coH}. Then we will use the Morita context to study the situation when A/A^{coH} is Galois.

Recall from Exercise 6.2.13 that A is an $A\#H^{*rat} - A^{coH}$-bimodule and an $A^{coH} - A\#H^{*rat}$-bimodule with the usual A^{coH}-module structure on A, and for $a, b \in A$, $h^* \in H^{*rat}$, the left and right $A\#H^{*rat}$-module structures are given by:

$$(a\#h^*) \cdot b = \sum ab_0 h^*(b_1),$$

and

$$b \cdot (a\#h^*) = (h^*S^{-1}) \rightharpoonup (ba) = \sum b_0 a_0 h^*(S^{-1}(b_1 a_1)).$$

If g is the grouplike element of H from Proposition 5.5.4 (iii) (which was denoted there by a), we can also define a (unital) right $A\#H^{*rat}$-module structure on A by

$$b \cdot_g (a\#h^*) = b \cdot (a\#g \rightharpoonup h^*) = \sum b_0 a_0 h^*(S^{-1}(b_1 a_1)g).$$

Since g defines an automorphism of $A\#H^{*rat}$, $a\#h^* \mapsto a\#g \rightharpoonup h^*$, it follows that with this structure A is also an $A^{coH} - A\#H^{*rat}$-bimodule.

We define now the Morita context. Let $P =_{A\#H^{*rat}} A_{A^{coH}}$ with the standard bimodule structure given above. Let $Q =_{A^{coH}} A_{A\#H^{*rat}}$ where now the right $A\#H^{*rat}$-module structure on A is defined using the grouplike from Proposition 5.5.4 (iii), which we will now denote by g, as above.

Define bimodule maps $[-,-]$ and $(-,-)$ by

$$[-,-] : P \otimes Q = A \otimes_{A^{coH}} A \longrightarrow A\#H^{*rat},$$

$$[-,-](a \otimes b) = [a,b] = \sum ab_0\#t \leftharpoonup b_1,$$

and

$$(-,-) : Q \otimes P = A \otimes_{A\#H^{*rat}} A \longrightarrow A^{coH},$$

$$(-,-)(a \otimes b) = (a,b) = t \rightharpoonup (ab) = \sum a_0 b_0 t(a_1 b_1).$$

Note that since $t \rightharpoonup A \subseteq A^{coH}$, the image of $(-,-)$ lies in A^{coH}. Then, with the notation above, we have

Proposition 6.3.1 *For H with nonzero left integral t, $A, P, Q, [-,-], (-,-)$ as above, the sextuple*

$$(A\#H^{*rat}, A^{coH}, P, Q, [-,-], (-,-))$$

is a Morita context.

Proof: We have to check that:
1. The bracket [-,-]: $A \otimes_{A^{coH}} A \longrightarrow A\#H^{*rat}$ satisfies $[ab,c] = [a,bc]$ for $b \in A^{coH}$, which is clear, and that it is a bimodule map.

Left $A\#H^{*rat}$-linearity:
$[(a\#l) \cdot b, c] = \sum [ab_0 l(b_1), c] = \sum ab_0 c_0 l(b_1)\#t \leftharpoonup c_1$
and

$$\begin{aligned}
(a\#l)[b,c] &= (a\#l)\sum bc_0\#t \leftharpoonup c_1 \\
&= \sum ab_0c_0\#(l \leftharpoonup b_1c_1)(t \leftharpoonup c_2) \\
&= \sum ab_0c_0\#[(l \leftharpoonup b_1)t] \leftharpoonup c_1 \\
&= \sum ab_0c_0\#l(b_1)t \leftharpoonup c_1 \text{ since } t \text{ is a left integral.}
\end{aligned}$$

Right $A\#H^{*rat}$-linearity:
$[a, b\cdot_g(c\#l)] = \sum[a, b_0c_0l(S^{-1}(b_1c_1)g)] = \sum ab_0c_0\#(t \leftharpoonup b_1c_1)l(S^{-1}(b_2c_2)g)$, and,

$$\begin{aligned} [a,b](c\#l) &= \sum(ab_0\#t \leftharpoonup b_1)(c\#l) \\ &= \sum ab_0c_0\#(t \leftharpoonup b_1c_1)l \\ &= \sum ab_0c_0\#(t \leftharpoonup l(S^{-1}(b_2c_2))) \leftharpoonup b_1c_1 \\ &= \sum ab_0c_0\#l(S^{-1}(b_2c_2)g)t \leftharpoonup b_1c_1, \end{aligned}$$

since $\lambda(l \leftharpoonup h) = (l \leftharpoonup h)(g) = l(hg)$.

2. The bracket (-,-) : $A \otimes_{A\#H^{*rat}} A \longrightarrow t \rightharpoonup A \subseteq A^{coH}$ is obviously left and right A^{coH}-linear and the definition is correct by Exercise 6.2.16. Moreover,
$(a, (b\#l)\cdot c) = \sum(a, bc_0l(c_1)) = \sum a_0b_0c_0t(a_1b_1c_1)l(c_2)$
$= \sum a_0b_0c_0((t \leftharpoonup a_1b_1)l)(c_1)$
$= \sum a_0b_0c_0((t(l \leftharpoonup S^{-1}(a_2b_2))) \leftharpoonup a_1b_1)(c_1)$
$= \sum a_0b_0c_0(t \leftharpoonup a_1b_1)(c_1)(l \leftharpoonup S^{-1}(a_2b_2))(g)$ by $\lambda(m) = m(g)$
and
$(a\cdot_g(b\#l), c) = \sum(a_0b_0l(S^{-1}(a_1b_1)g), c) = \sum a_0b_0c_0t(a_1b_1c_1)l(S^{-1}(a_2b_2)g)$.

3. Associativity of the brackets.

First note that we will use $(g \rightharpoonup t)S^{-1} = t$ from Proposition 5.5.4 (iii). Now,

$$\begin{aligned} a\cdot_g [b,c] = \sum a\cdot_g (bc_0\#t \leftharpoonup c_1) &= \sum a_0b_0c_0(t \leftharpoonup c_2)(S^{-1}(a_1b_1c_1)g) \\ &= \sum a_0b_0ct(S^{-1}(a_1b_1)g) \\ &= \sum a_0b_0((g \rightharpoonup t)S^{-1})(a_1b_1)c \\ &= \sum a_0b_0t(a_1b_1)c \text{ by the above} \\ &= (a,b)c. \end{aligned}$$

Also
$[a,b]\cdot c = \sum(ab_0\#t \leftharpoonup b_1)c = \sum ab_0c_0(t \leftharpoonup b_1)(c_1) = \sum ab_0c_0t(b_1c_1) = a(b,c)$. ∎

If any of the maps of the above Morita context is surjective, then it is an isomorphism. While for the map $(-,-)$ this is well known, there is a little problem with the other map, since $A\#H^{*rat}$ has no unit. Although the proof is almost the same as the usual one, we propose the following

Exercise 6.3.2 *If the map $[-,-]$ from the Morita context in Proposition 6.3.1 is surjective, then it is bijective.*

Now we discuss the surjectivity of the Morita map to A^{coH}, leaving the discussion on the other map for the section on Galois extensions.

Definition 6.3.3 *A* total integral *for the H-comodule algebra A is an H-comodule map from H to A taking 1 to 1.*

Since an integral for the Hopf algebra H is a colinear map from H to k, the H-comodule algebra k has a total integral if and only if H is cosemisimple.

Exercise 6.3.4 *Let H be a finite dimensional Hopf algebra. Then a right H-comodule algebra A has a total integral if and only if the corresponding left H^*-module algebra A has an element of trace 1.*

We give now the characterization of the surjectivity of one of the Morita context maps.

Proposition 6.3.5 *The Morita context map to A^{coH} is onto if and only if there exists a total integral $\Phi : H \longrightarrow A$.*

Proof: ($\Leftarrow$) Let Φ be a total integral, i.e. Φ is a morphism of right H-comodules, and $\Phi(1) = 1$. Then Φ is also a morphism of left H^*-modules, so $\Phi(t \rightharpoonup h) = t \rightharpoonup \Phi(h)$ for any $h \in H$.

Suppose $h \in H$ is such that $t \rightharpoonup h = 1$, then for $(-,-)$ the map from Proposition 6.3.1,

$$(1, \Phi(h)) = t \rightharpoonup \Phi(h) = \Phi(t \rightharpoonup h) = \Phi(1) = 1,$$

which shows that $(-,-)$ is onto. Since $t \rightharpoonup H \subseteq H^{coH} = k1_H$, to find an $h \in H$ with $t \rightharpoonup h = 1$, it is enough to prove that $t \rightharpoonup H \neq 0$. But if $t \rightharpoonup H = 0$, then for any $h, g \in H$ we have that:

$$(h \rightharpoonup t) \rightharpoonup g = \sum t(g_2 h) g_1 =$$

$$= \sum t(g_2 h_3) g_1 h_2 S^{-1}(h_1) = \sum (t \rightharpoonup (g h_2)) S^{-1}(h_1) = 0$$

and so $(H \rightharpoonup t) \rightharpoonup H = 0$. But $H \rightharpoonup t = H^{*rat}$, so $H^{*rat} \rightharpoonup H = 0$. Finally, since H^{*rat} is dense in H^*, this implies that $H^* \rightharpoonup H = 0$ which is clearly a contradiction.

($\Rightarrow$) Choose $a \in A$ such that $t \rightharpoonup a = 1$, and define $\Phi : H \longrightarrow A$ by

$$\Phi(h) = (S(h) \rightharpoonup t) \rightharpoonup a = \sum a_0 t(a_1 S(h)).$$

Then $\Phi(1) = 1$ and Φ is a morphism of left H^*-modules since for $h^* \in H^*, h \in H$,

$$\Phi(h^* \rightharpoonup h) \quad = \quad \Phi(\sum h_1 h^*(h_2))$$

$$\begin{aligned}
&= \sum a_0 t(a_1 S(h_1))h^*(h_2) \\
&= \sum a_0 t(a_1 S(h_1))(h_2 \rightharpoonup h^*)(1) \\
&= \sum a_0((h_2 \rightharpoonup h^*)t)(a_1 S(h_1)) \\
&= \sum a_0 h^*(a_1)t(a_2 S(h)) \\
&= h^* \rightharpoonup \Phi(h).
\end{aligned}$$

∎

6.4 Hopf-Galois extensions

Let H be a Hopf algebra over the field k, and A a right H-comodule algebra. We denote by

$$\rho : A \longrightarrow A \otimes H, \ \ \rho(a) = \sum a_0 \otimes a_1$$

the morphism giving the H-comodule structure on A, and by A^{coH} the subalgebra of coinvariants. We define the following canonical map

$$can : A \otimes_{A^{coH}} A \longrightarrow A \otimes H, \ \ can(a \otimes b) = (a \otimes 1)\rho(b) = \sum ab_0 \otimes b_1.$$

Definition 6.4.1 *We say that A is* right H-Galois, *or that the extension A/A^{coH} is Galois, if can is bijective.* ∎

We can also define the map

$$can' : A \otimes_{A^{coH}} A \longrightarrow A \otimes H, \ \ can(a \otimes b) = \rho(a)(b \otimes 1) = \sum a_0 b \otimes a_1.$$

Exercise 6.4.2 *If S is bijective, then can is bijective if and only if can′ is bijective.*

We give two examples showing that this notion covers, on one hand, the classical definition of a Galois extension, and, on the other hand, in the case of gradings (Example 6.2.5, 2)) it comes down to another well known notion. We will give some more examples after proving a theorem containing various characterizations of Galois extensions.

Example 6.4.3 *(Examples of Hopf-Galois extensions)*

1) Let G be a finite group acting as automorphisms on the field $E \supset k$. We know from Example 6.1.13, 2) that E is a left kG-module algebra, hence a right kG^*-comodule algebra. Let $F = E^G$. It is known that E/F is Galois with Galois group G if and only if $[E : F] =\mid G \mid$ (see N. Jacobson

[99, Artin's Lemma, p. 229]). Suppose that E/F is Galois. Let $n = \mid G \mid$, $G = \{\eta_1, \ldots, \eta_n\}$, $\{u_1, \ldots, u_n\}$ a basis of E/F. Let $\{p_1, \ldots, p_n\} \subset kG^*$ be the dual basis for $\{\eta_i\} \subset kG$.
E is a right kG^*-comodule algebra with $\rho : E \longrightarrow E \otimes kG^*$, $\rho(a) = \sum(\eta_i \cdot a) \otimes p_i$. $can : E \otimes_F E \longrightarrow E \otimes kG^*$ is given by $can(a \otimes b) = \sum a(\eta_i \cdot b) \otimes p_i$. If $w = \sum x_j \otimes u_j \in Ker(can)$, it follows that

$$\sum_j x_j(\eta_i \cdot u_j) = 0, \quad \forall i \tag{6.9}$$

(because p_i are linearly independent). As in the proof of Artin's Lemma, it may be shown that if the system (6.9) has a non-zero solution, then all the elements x_j are in F, which contradicts the fact that $\{u_i\}$ is a basis. Hence all x_j are 0, so $w = 0$. It follows that can is injective. But can is F-linear, and both $E \otimes_F E$ and $E \otimes kG^*$ are F-vector spaces of dimension n^2, and therefore can is a bijection.
Conversely, we use $dim_F(E \otimes_F E) = [E : F]^2$ and $dim_F(E \otimes kG^*) = [E : F] \mid G \mid$. If can is an isomorphism, it follows that $[E : F] = \mid G \mid$, so E/F is Galois.
2) Let $A = \bigoplus_{g \in G} A_g$ be a graded k-algebra of type G. We know from Example 6.2.5, 2) that A is a right kG-comodule algebra, and that $A^{co\, kG} = A_1$. We recall that A is said to be strongly graded if $A_g A_h = A_{gh}$, $\forall g, h \in G$, or, equivalently, if $A_g A_{g^{-1}} = A_1$, $\forall g \in G$. We have that A/A_1 is right kG-Galois if and only if A is strongly graded.
Assume first that A is strongly graded. Let

$$\beta : A \otimes kG \longrightarrow A \otimes_{A_1} A, \quad \beta(a \otimes g) = \sum a a_i \otimes b_i,$$

where $a_i \in A_{g^{-1}}$, $b_i \in A_g$, $\sum a_i b_i = 1$. It may be seen immediately that $(can \circ \beta)(a \otimes g) = a \otimes g$. Moreover,

$$\begin{aligned}
(\beta \circ can)(a \otimes b) &= \beta(\sum_g a b_g \otimes g) \\
&= \sum_g \sum_{i_g} a b_g a_{i_g} \otimes b_{i_g} \\
&= \sum_g \sum_{i_g} a \otimes b_g a_{i_g} b_{i_g} \\
&= \sum_g a \otimes b_g = a \otimes b.
\end{aligned}$$

Conversely, if *can* is bijective, it is in particular surjective. For each $g \in G$, let $a_i, b_i \in A$ be such that

$$\sum_{i,h} a_i(b_i)_h \otimes h = 1 \otimes g.$$

It follows that all b_i may be assumed homogeneous of degree g, and $\sum a_i b_i = 1$. Since the sum of homogeneous components is direct, it follows that the a_i may be also assumed homogeneous of degree g^{-1}. ∎

We remark that in the last example it was enough to assume that *can* is surjective to get Galois. As we will see below, in the main result of this section, this is due to the fact that kG is cosemisimple, in particular co-Frobenius.

For any $M \in {}_A\mathcal{M}^H$, consider the left $A\#H^{*rat}$-module map

$$\phi_M : A \otimes_{A^{coH}} M^{coH} \longrightarrow M, \quad \phi_M(a \otimes m) = am$$

where the $A\#H^{*rat}$-module structure of $A \otimes_{A^{coH}} M^{coH}$ is induced by the usual left $A\#H^{*rat}$ action on A. Thus ϕ_M is also a morphism in the category ${}_A\mathcal{M}^H$. If ϕ_M is an isomorphism for all $M \in {}_A\mathcal{M}^H$, we say the Weak Structure Theorem holds for ${}_A\mathcal{M}^H$. Similarly, if for any $M \in \mathcal{M}_A^H$, the map

$$\phi'_M : M^{coH} \otimes_{A^{coH}} A \longrightarrow M, \quad \phi'_M(m \otimes a) = ma$$

is an isomorphism, the Weak Structure Theorem holds for $\mathcal{M}_A^H$.

We prove now the main result of this section.

Theorem 6.4.4 *Let H be a Hopf algebra with non-zero left integral t, A a right H-comodule algebra. Then the following are equivalent:*
i) A/A^{coH} is a right H-Galois extension.
ii) The map can: $A \otimes_{A^{coH}} A \longrightarrow A \otimes H$ is surjective.
iii) The Morita map $[-,-]$ is surjective.
iv) The Weak Structure Theorem holds for ${}_A\mathcal{M}^H$.
v) The map ϕ_M is surjective for all $M \in {}_A\mathcal{M}^H$.
vi) A is a generator for the category ${}_A\mathcal{M}^H \cong {}_{A\#H^{*rat}}\mathcal{M}^u$.

Proof: Since H is co-Frobenius, the map

$$r : H \longrightarrow H^{*rat}, \quad r(h) = t \leftharpoonup h$$

is bijective. Then, since $[-,-] = (I \otimes r) \circ can$, it follows that ii) $\Leftrightarrow$ iii). This also shows that i)$\Leftrightarrow$ ii), using Exercise 6.3.2.

In order to show that v) $\Rightarrow$ iii), we consider $A\#H^{*rat} \in {}_A\mathcal{M}^H$, which is isomorphic to $H^{*rat} \otimes A$ as in (6.6). Therefore, $(A\#H^{*rat})^{coH} = (H^{*rat} \otimes A)^{coH} = t \otimes A$, and so $\phi_{A\#H^{*rat}} = [-,-]$.

iii) $\Rightarrow$ iv). Let $M \in {}_A\mathcal{M}^H$, $m \in M$. We show first that ϕ_M is one to one. Suppose $m = \phi_M(\sum a_i \otimes m_i)$ for $a_i \in A, m_i \in M^{coH}$. Let e^* be an element of H^{*rat} that agrees with ε on the finite set of elements a_{i_1}, m_1 in H. Suppose $\sum [c_k, d_k] = 1\#e^*$. Then

$$\begin{aligned}
\sum a_i \otimes_{A^{coH}} m_i &= \sum [c_k, d_k] a_i \otimes m_i \\
&= \sum c_k (d_k, a_i) \otimes m_i \\
&= \sum c_k \otimes (d_k, a_i) m_i \\
&= \sum c_k \otimes (t \rightharpoonup d_k a_i) m_i \\
&= \sum c_k \otimes t \rightharpoonup (d_k \sum a_i m_i)) \text{ since } m_i \in M^{coH} \\
&= \sum c_k \otimes t \rightharpoonup (d_k m).
\end{aligned}$$

So if $m = 0$ it follows that $\sum a_i \otimes_{A^{coH}} m_i = 0$, and so ϕ_M is injective. To show that ϕ_M is surjective, note that for m and e^* as above

$$m = e^* \cdot m = \phi_M(\sum c_k \otimes t \rightharpoonup (d_k m)).$$

We have thus proved that iii), iv), and v) are equivalent.

iv)$\Rightarrow$ vi). Let $M \in {}_A\mathcal{M}^H$. Since A^{coH} is a generator in ${}_{A^{coH}}\mathcal{M}$, for some set I, there is a surjection from $(A^{coH})^{(I)}$ to M^{coH}. Thus there is a surjection from $A^{(I)} \simeq A \otimes_{A^{coH}} (A^{coH})^{(I)}$ to $A \otimes_{A^{coH}} M^{coH} \simeq M$.

vi) $\Rightarrow$ v). Let $M \in {}_A\mathcal{M}^H$. Since A a generator, given $x \in M$, there is an index set I, $(f_i)_{i \in I}$, $f_i \in Hom_A^H(A, M)$, $a_i \in A$, with $\sum f_i(a_i) = x$. Then $f_i(1) \in M^{coH}$, and $x = \phi_M(\sum a_i \otimes f_i(1))$. ∎

Remark 6.4.5 *A similar statement holds with can′ replacing can, and the category $\mathcal{M}_A^H$ replacing ${}_A\mathcal{M}^H$.*

Corollary 6.4.6 *If H is co-Frobenius and the equivalent conditions of Theorem 6.4.4 hold, then the map π in Exercise 6.2.13 induces a ring isomorphism*

$$A\#H^{*rat} \simeq End(A_{A^{coH}})^{rat},$$

where the rational part is taken with respect with the right H^*-module structure given by $(f \cdot h^*)(b) = \sum h^*(b_1) f(b_0)$.

Proof: We prove first that the map

$$\pi_1 : A\#H^{*rat} \longrightarrow End(A_{A^{coH}}), \quad \pi_1(z)(a) = z \cdot a,$$

is injective. Let $z \in A\#H^{*rat}$ be such that $z \cdot a = 0$, $\forall a \in A$. Let $g^* \in H^{*rat}$ be such that $z(1\#g^*) = z$. Since $[-,-]$ is surjective, there exist $a_i, b_i \in A$

such that $1\#g^* = \sum[a_i, b_i]$. Then we have $z = z(1\#g^*) = \sum[z \cdot a_i, b_i] = 0$. Thus it remains to show that the corestriction of π to $End(A_{A^{coH}})^{rat}$ is surjective. Let $f \in End(A_{A^{coH}})^{rat}$, and let $h^* \in H^{*rat}$ such that $f = f \cdot h^*$. Let t' be a right integral and $\sum_i a_i \otimes b_i \in A \otimes_{A^{coH}} A$ such that

$$1 \otimes (h^* \circ S^{-1}) = \sum_i a_i b_{i_0} \otimes S(b_{i_1}) \rightharpoonup t'.$$

Then, for any $b \in A$ we have

$$\begin{aligned}
f(b) &= (f \cdot h^*)(b) \\
&= \sum h^*(b_1) f(b_0) \\
&= \sum h^*(S^{-1}(S(b_1))) f(b_0) \\
&= \sum f(a_i b_{i_0} b_0) t'(S(b_1) S(b_{i_1})) \\
&= \sum f(a_i) b_{i_0} b_0 (t' \circ S)(b_{i_1} b_1) \\
&= \sum f(a_i) b_{i_0} b_0 ((S(b_{i_1}) \rightharpoonup t') S)(b_1) \\
&= \pi(\sum f(a_i) b_{i_0} \#(S(b_{i_1} \rightharpoonup t') S)(b)
\end{aligned}$$

and the proof is complete. ∎

If H is finite dimensional, then from the Morita theory it follows that A/A^{coH} is an H-Galois extension if and only if A is projective finitely generated as a right A^{coH}-module and the map π is an isomorphism. The behaviour of π in the general co-Frobenius case was exhibited in the previous proposition. The next result investigates the structure of A as a right A^{coH}-module in the Galois case.

Corollary 6.4.7 *If H is co-Frobenius, then any H-Galois H-comodule algebra A is a flat right A^{coH}-module.*

Proof: A well known criterion for flatness ([3, 19.19]) says that A is flat over A^{coH} if and only if for every relation

$$\sum_{j=1}^{n} a_j b_j = 0 \quad (a_j \in A,\ b_j \in A^{coH})$$

there exist elements $c_1, \ldots, c_m \in A$ and $c_{ij} \in A^{coH}$ $(i = 1, \ldots, m, j = 1, \ldots, n)$ such that

$$\sum_{i=1}^{m} c_i c_{ij} = a_j \quad (j = 1, \ldots, n) \tag{6.10}$$

and

$$\sum_{j=1}^{n} c_{ij}b_j = 0 \quad (i = 1, \ldots, m) \tag{6.11}$$

So let $a_1, \ldots, a_n \in A$ and $b_1, \ldots, b_n \in A^{coH}$ such that $\sum\limits_{j=1}^{n} a_j b_j = 0$. Consider the morphism in ${}_A\mathcal{M}^H$

$$\xi : A^n \longrightarrow A, \quad \xi(x_1, \ldots, x_n) = \sum_{j=1}^{n} x_j b_j.$$

Since A is a generator in ${}_A\mathcal{M}^H$, there exist a set X and a surjective morphism $\phi : A^{(X)} \to Ker(\xi)$. Therefore, there exist elements $c_1, \ldots, c_n \in A$ and morphisms $\phi_1, \ldots, \phi_m : A \to Ker(\xi)$ in ${}_A\mathcal{M}^H$ such that

$$(a_1, \ldots, a_n) = \sum_{i=1}^{m} \phi_i(c_i) = \sum_{i=1}^{m} c_i \phi_i(1).$$

Applying the canonical projection π_j to bothe sides we get (6.10) for $c_{ij} = (\pi_j \circ \phi_i)(1) \in A^{coH}$. As for (6.11), we have

$$\sum_{j=1}^{n} (\pi_j \circ \phi_i)(1) b_j = (\xi \circ \phi_i)(1) = 0,$$

and the proof is complete. ∎

Example 6.4.8 *(Other examples of Hopf-Galois extensions)*

1) Let H be a Hopf algebra. Then we know that H is a right H-comodule algebra, $H^{coH} \simeq k$. The extension H/k is clearly Galois, since

$$can : H \otimes H \longrightarrow H \otimes H, \quad can(h \otimes g) = \sum hg_1 \otimes g_2$$

has inverse $h \otimes g \longmapsto \sum hS(g_1) \otimes g_2$.
2) Let A be a left H-module algebra. By Example 6.4.3, 2), $A\#H$ is a right H-comodule algebra, and $(A\#H)^{coH} \simeq A$. It is easy to see that $A\#H/A$ is a Galois extension. Indeed, in this case we have

$$can : A\#H \otimes_A A\#H \longrightarrow (A\#H) \otimes H,$$

and $(a\#h) \otimes (b\#g) = (a\#h)(b\#1) \otimes (1\#g)$, so it is enough to define can on elements of the form $(a\#h) \otimes (1\#g)$. But $can((a\#h) \otimes (1\#g)) = \sum (a\#hg_1) \otimes g_2$. It follows that the inverse of can may be defined as in

1).
3) The assertion in 2) also holds for crossed products with invertible cocycle. This will be proved at the end of this section. Until then, we give a proof in the case H is finite dimensional. Let $A\#_\sigma H$ be a crossed product with invertible σ. By 1) H/k is Galois, so by Theorem 6.4.4, iii), for $0 \neq t \in H^*$ left integral, the map

$$H \otimes H \longrightarrow H\#H^*, \;\; x \otimes y \longmapsto (x\#t)(y\#1)$$

is surjective. Let $x^i, y^i \in H$ such that

$$\sum(x^i\#t)(y^i\#1) = \sum x^i(t_1 \cdot y^i)\#t_2 = 1\#1.$$

We compute

$$\begin{aligned}
& \sum((\sigma^{-1}(x^i_1, y^i_1)\#x^i_2)\#t)((1\#y^i_2)\#1) = \\
= \; & \sum(\sigma^{-1}(x^i_1, y^i_1)\#x^i_2)(t_1 \cdot (1\#y^i_2))\#t_2 \\
= \; & \sum(\sigma^{-1}(x^i_1, y^i_1)\#x^i_2)(1\#t_1(y^i_3)y^i_2)\#t_2 \\
= \; & \sum \sigma^{-1}(x^i_1, y^i_1)(x^i_2 \cdot 1)\sigma(x^i_3, t_1(y^i_4)y^i_2)\#x^i_4y^i_3\#t_2 \\
= \; & \sum \sigma^{-1}(x^i_1, y^i_1)\varepsilon(x^i_2)\sigma(x^i_3, t_1(y^i_4)y^i_2)\#x^i_4y^i_3\#t_2 \\
= \; & \sum \sigma^{-1}(x^i_1, y^i_1)\sigma(x^i_2, y^i_2)\#x^i_3t_1(y^i_4)y^i_3\#t_2 \\
= \; & \sum \varepsilon(x^i_1)\varepsilon(y^i_1)1\#x^i_2t_1(y^i_3)y^i_2\#t_2 \\
= \; & \sum 1\#\varepsilon(x^i_1)x^i_2t_1(y^i_3)\varepsilon(y^i_1)y^i_2\#t_2 \\
= \; & \sum 1\#x^it_1(y^i_2)y^i_1\#t_2 \\
= \; & \sum 1\#x^i(t_1 \cdot y^i)\#t_2 = 1\#1\#1,
\end{aligned}$$

which ends the proof by Theorem 6.4.4, iii).
Note also that $A\#_\sigma H$ has an element of trace 1: if $h \in H$ is such that $t(h) = 1$, then $1\#h$ is such an element. ∎

Remarks 6.4.9 *1) If H is co-Frobenius, A/A^{coH} is H-Galois, and A has a total integral, then A^{coH} is Morita equivalent to $A\#H^{*rat}$. This follows from Theorem 6.4.4 iii), Exercise 6.3.2, and Proposition 6.3.5.*
2) In particular, if H is finite dimensional, A/A^{coH} is H-Galois, and A has an element of trace 1, then 1) above and Exercise 6.3.4 show that A^{coH} is Morita equivalent to $A\#H^*$. An example is provided by a crossed product with invertible cocycle $A\#_\sigma H$, as Example 6.4.8 3) shows.

3) As it will be mentioned in the notes at the end of this chapter, there exist much more general theorems about the equivalence of the categories $\mathcal{M}_A^H$ (or ${}_A\mathcal{M}^H$) and the category of right (or left) A^{coH}-modules. In this context, the fundamental theorem of Hopf modules may be seen as an example of such a situation, due to Example 6.4.8 1).
4) If H is finite dimensional, A is a left H-module algebra, A/A^H is H^*-Galois, and M is a left A-module, we have the isomorphism

$$A \otimes_{A^H} M \simeq (A \otimes_{A^H} A) \otimes_A M \simeq (A\#H) \otimes_A M,$$

(where the last isomorphism is $[-,-] \otimes I$), which is even functorial. ∎

We can now prove a Maschke-type theorem for crossed products.

Proposition 6.4.10 *Let H be a semisimple Hopf algebra, and $A\#_\sigma H$ a crossed product with invertible σ. Let V be a left $A\#_\sigma H$-module, and W an $A\#_\sigma H$-submodule of V. If W is a direct summand in V as A-modules, then it is a direct summand in V as $A\#_\sigma H$-modules.*

Proof: If W is a direct summand in V as A-modules, then we have that $(A\#_\sigma H) \otimes_A W$ is a direct summand in $(A\#_\sigma H) \otimes_A V$ as $A\#_\sigma H$-modules, since the functor $(A\#_\sigma H) \otimes_A -$ is an equivalence. By Remark 6.4.9, 4), it follows that $(A\#_\sigma H)\#H^* \otimes_{A\#_\sigma H} W$ is a direct summand in $(A\#_\sigma H)\#H^* \otimes_{A\#_\sigma H} V$ as $(A\#_\sigma H)\#H^*$-modules. Since H is semisimple, from Exercise 6.2.20 we deduce that $(A\#_\sigma H)\#H^* \otimes_{A\#_\sigma H} W$ is a direct summand in $(A\#_\sigma H)\#H^* \otimes_{A\#_\sigma H} V$ as $((A\#_\sigma H)\#H^*)\#H$-modules. But again the functor $(A\#_\sigma H)\#H^* \otimes_{A\#_\sigma H} -$ is an equivalence, and so W is a direct summand in V as $A\#_\sigma H$-modules. ∎

The following exercise shows again how close co-Frobenius Hopf algebras are to finite dimensional Hopf algebras.

Exercise 6.4.11 *Let H be a co-Frobenius Hopf algebra, and A a right H-comodule algebra with structure map*

$$\rho : A \longrightarrow A \otimes A \otimes H, \ \ \rho(a) = \sum a_0 \otimes a_1.$$

If A/A^{coH} is a separable Galois extension, then H is finite dimensional.

We close this section by a characterization of crossed products which will be used later on.

Theorem 6.4.12 *Let A be a right H-comodule algebra, and $B = A^{coH}$. The following assertions are equivalent:*
a) There exists an invertible cocycle $\sigma : B \otimes B \longrightarrow B$, and a weak action of H on B, such that $A = B\#_\sigma H$.

b) The extension A/B is Galois, and A is isomorphic as left B-modules and right H-comodules to $B \otimes H$, where the B-module and H-comodule structures on $B \otimes H$ are the trivial ones.

Proof: a)$\Rightarrow$b). It is clear that the identity map is the required isomorphism, so all we have to prove is that the extension $B\#_\sigma H/B$ is Galois. We have to show that the map

$$can : B\#_\sigma H \otimes_B B\#_\sigma H \longrightarrow B\#_\sigma H \otimes H,$$

$$can((a\#h) \otimes (b\#l)) = \sum (a\#h)(b\#l_1) \otimes l_2 =$$

$$= \sum a(h_1 \cdot b)\sigma(h_2, l_1)\#h_3 l_2 \otimes l_3$$

is bijective. We define

$$\beta : B\#_\sigma H \otimes H \longrightarrow B\#_\sigma H \otimes_B B\#_\sigma H,$$

$$\beta(a\#h \otimes l) = \sum (a\#h)(\sigma^{-1}(S(l_2), l_3)\#S(l_1)) \otimes 1\#l_4 =$$

$$= \sum a(h_1 \cdot \sigma^{-1}(S(l_3), l_4))\sigma(h_2, S(l_2))\#h_3 S(l_1) \otimes 1\#l_5,$$

and show this is an inverse for can. We compute first

$$\begin{aligned}
& can(\beta(a\#h \otimes l)) = \\
= \;& \sum a(h_1 \cdot \sigma^{-1}(S(l_4), l_5))\sigma(h_2, S(l_3))\sigma(h_3 S(l_2), l_6)\# \\
& \qquad \#h_4 S(l_1) l_7 \otimes l_8 \\
= \;& \sum a(h_1 \cdot \sigma^{-1}(S(l_4), l_5))(h_2 \cdot \sigma(S(l_3), l_6))\sigma(h_3, S(l_2) l_7)\# \\
& \qquad \#h_4 S(l_1) l_8 \otimes l_9 \quad \text{(by (6.3))} \\
= \;& \sum a(h_1 \cdot \sigma^{-1}(S(l_4), l_5)\sigma(S(l_3), l_6))\sigma(h_2, S(l_2) l_7)\# \\
& \qquad \#h_3 S(l_1) l_8 \otimes l_9 \quad \text{(by (MA2))} \\
= \;& \sum a(h_1 \cdot (\varepsilon(l_3)\varepsilon(l_4)1)\sigma(h_2, S(l_2) l_5)\#h_3 S(l_1) l_6 \otimes l_7 \\
= \;& \sum a\sigma(h_1, S(l_2) l_3)\#h_3 S(l_1) l_4 \otimes l_5 \quad \text{(by (MA3))} \\
= \;& \sum a\#h_3 S(l_1) l_2 \otimes l_3 \quad \text{(by (6.2))} \\
= \;& a\#h \otimes g.
\end{aligned}$$

Note that the proof would be finished if H would be co-Frobenius, due to Theorem 6.4.4, so this gives another proof for Example 6.4.8 3). But since

H is arbitrary, we also have to compute

$$\begin{aligned}
& \beta(can((a\#h)\otimes(b\#l))) = \\
= & \sum(a\#h)(b\#l_1)(\sigma^{-1}(S(l_3),l_4)\#S(l_2))\otimes 1\#l_5 \\
= & \sum(a\#h)(b(l_1\cdot\sigma^{-1}(S(l_6),l_7))\sigma(l_2,s(l_5))\#l_3S(l_4))\otimes 1\#l_8 \\
= & \sum(a\#h)(b(l_1\cdot\sigma^{-1}(S(l_4),l_5))\sigma(l_2,s(l_3))\#1)\otimes 1\#l_6 \\
= & \sum(a\#h)\otimes(b(l_1\cdot\sigma^{-1}(S(l_4),l_5))\sigma(l_2,s(l_3))\#1)(1\#l_6) \\
= & \sum(a\#h)\otimes(b\#l_1)(\sigma^{-1}(S(l_3),l_4)\#S(l_2))(1\#l_5) \\
= & \sum(a\#h)\otimes(b\#l_1)(\sigma^{-1}(S(l_4),l_5)\sigma(S(l_3),l_6)\#S(l_2)l_7 \\
= & \sum(a\#h)\otimes(b\#l_1)(\varepsilon(l_3)\varepsilon(l_4)1\#S(l_2)l_5 \\
= & \sum(a\#h)\otimes(b\#l_1)(1\#S(l_2)l_3 \\
= & (a\#h)\otimes(b\#l),
\end{aligned}$$

so β is the inverse of can, and the proof is complete.
b)$\Rightarrow$a). Let $\Phi : B\otimes H \to A$ be an isomorphism of left B-modules and right H-comodules. Much like in the case of group extensions, we define first a sort of a "set-splitting" map $\gamma : H \to A$, $\gamma(h) = \Phi(1\otimes h)$, which is clearly H-colinear. We show first that γ is convolution invertible. Since A/B is Galois, for each $h \in H$ there exists an element $\sum a_i(h)\otimes b_i(h) \in A\otimes_B A$, the preimage of $1\otimes h$ by can. We have

$$\sum a_0 a_i(a_1)\otimes b_i(a_1) = 1\otimes a, \tag{6.12}$$

which may be checked by applying can to both sides. We also have

$$\sum a_i(h)\otimes b_i(h)_0\otimes b_i(h)_1 = \sum a_i(h_1)\otimes b_i(h_1)\otimes h_2, \tag{6.13}$$

which may be seen after applying $can\otimes I$ to both sides. Now we define $\mu : H \to A$, $\mu(h) = \sum a_i(h)(I\otimes\varepsilon)\Phi^{-1}(b_i(h))$, and we compute

$$\begin{aligned}
& (\gamma * \mu)(h) = \\
= & \sum \gamma(h_1)\mu(h_2) \\
= & \sum \gamma(h_1)a_i(h_2)(I\otimes\varepsilon)\Phi^{-1}(b_i(h_2)) \\
= & \sum \gamma(h)_0 a_i(\gamma(h)_1)(I\otimes\varepsilon)\Phi^{-1}(b_i(\gamma(h)_1)) \\
= & (I\otimes\varepsilon)\Phi^{-1}(\gamma(h)) \ \text{(by (6.12))} \\
= & (I\otimes\varepsilon)\Phi^{-1}(\Phi(1\otimes h)) \\
= & \varepsilon(h)1,
\end{aligned}$$

and

$$\begin{aligned}
&(\mu * \gamma)(h) = \\
= \;& \sum \mu(h_1)\gamma(h_2) \\
= \;& \sum a_i(h_1)(I \otimes \varepsilon)\Phi^{-1}(b_i(h_1))\gamma(h_2) \\
= \;& \sum a_i(h_1)\Phi((I \otimes \varepsilon)\Phi^{-1}(b_i(h_1)) \otimes h_2) \\
= \;& \sum a_i(h_1)\Phi((I \otimes \varepsilon \otimes I)(\Phi^{-1}(b_i(h_1)) \otimes h_2)) \\
= \;& \sum a_i(h)\Phi((I \otimes \varepsilon \otimes I)(\Phi^{-1}(b_i(h)_0) \otimes b_i(h)_1)) \text{ (by (6.13))} \\
= \;& \sum a_i(h)\Phi((I \otimes \varepsilon \otimes I)(\Phi^{-1}(b_i(h))_0 \otimes \Phi^{-1}(b_i(h))_1)) \\
= \;& \sum a_i(h)\Phi(\Phi^{-1}(b_i(h))) \\
= \;& \sum a_i(h)b_i(h) = \varepsilon(h)1,
\end{aligned}$$

so γ is a convolution invertible H-comodule map. Since 1 is grouplike, $\gamma(1)$ is invertible with inverse $\gamma^{-1}(1)$, so replacing γ by γ', $\gamma'(h) = \gamma(h)\gamma^{-1}(1)$, we can assume that $\gamma(1) = 1$.
From now on, the proof follows closely the proof of the fact that an extension of groups is a crossed product:
1. We define a weak action of H on B by putting for $h \in H$ and $a \in B$:

$$h \cdot a = \sum \gamma(h_1)a\gamma^{-1}(h_2),$$

and a cocycle $\sigma : H \times H \to B$ by

$$\sigma(h, l) = \sum \gamma(h_1)\gamma(l_1)\gamma^{-1}(h_2 l_2).$$

In order to check that the definitions are correct, we note first that

$$\gamma^{-1}(h)_0 \otimes \gamma^{-1}(h)_1 = \sum \gamma^{-1}(h_2) \otimes S(h_1) \tag{6.14}$$

for all $h \in H$. To see this, note that the left hand side of (6.14) is the convolution inverse of

$$\psi : H \to B \otimes H, \;\; \psi(h) = \sum \gamma(h)_0 \otimes \gamma(h)_1 = \sum \gamma(h_1) \otimes h_2,$$

and if we denote by $\xi(h)$ the right hand side of (6.14), then it is immediate that $(\psi * \xi)(h) = \varepsilon(h)1 \otimes 1$, so (6.14) holds.
Now

$$(h \cdot a)_0 \otimes (h \cdot a)_1 = \sum \gamma(h_1)a\gamma^{-1}(h_4) \otimes h_2 S(h_3) = h \cdot a \otimes 1,$$

so $H \cdot B \subseteq B$. To check $(MA2)$, we compute

$$\sum (h_1 \cdot a)(h_2 \cdot b) = \sum \gamma(h_1) a \gamma^{-1}(h_2)\gamma(h_3) b \gamma^{-1}(h_4) = h \cdot (ab),$$

while $(MA3)$ is obvious.
Now

$$\sigma(h,l)_0 \otimes \sigma(h,l)_1 = \sum \gamma(h_1)\gamma(l_1)\gamma^{-1}(h_4 l_4) \otimes h_2 l_2 S(h_3 l_3) = \sigma(h,l) \otimes 1,$$

so the definition of σ is also correct.
2. It is clear that σ is a normal cocycle (it satisfies (6.2)) and is convolution invertible, with inverse given by:

$$\sigma^{-1}(h,l) = \sum \gamma(h_1, l_1)\gamma^{-1}(l_2)\gamma^{-1}(h_2).$$

We check that σ satisfies the cocycle condition (6.3):

$$\begin{aligned}
& \sum (h_1 \cdot \sigma(l_1, m_1))\sigma(h_2, l_2 m_2) = \\
= & \sum \gamma(h_1)\sigma(l_1, m_1)\gamma^{-1}(h_2)\sigma(h_3, l_2 m_2) \\
= & \sum \gamma(h_1)\gamma(l_1)\gamma(m_1)\gamma^{-1}(l_2 m_2)\gamma^{-1}(h_2)\gamma(h_3)\gamma(l_3 m_3)\gamma^{-1}(h_4 l_4 m_2) \\
= & \sum \gamma(h_1)\gamma(l_1)\gamma^{-1}(h_2 l_2 m_2) \\
= & \sum \gamma(h_1)\gamma(l_1)\gamma(m_1)\gamma^{-1}(h_2 l_2)\gamma(h_3 l_3)\gamma(m_1)\gamma^{-1}(h_2 l_2 m_2) \\
= & \sum \sigma(h_1, l_1)\sigma(h_2 l_2, m).
\end{aligned}$$

To check the twisted module condition (6.4) we compute

$$\begin{aligned}
& \sum (h_1 \cdot (l_1 \cdot a))\sigma(h_2, l_2) = \\
= & \sum \gamma(h_1)\gamma(l_1) a \gamma^{-1}(l_2)\gamma^{-1}(h_2)\gamma(h_3)\gamma(l_3)\gamma^{-1}(h_4 l_4) \\
= & \sum \gamma(h_1)\gamma(l_1) a \gamma^{-1}(h_2 l_2) \\
= & \sum \gamma(h_1)\gamma(l_1)\gamma^{-1}(h_2 l_2)\gamma(h_3 l_3) a \gamma^{-1}(h_4 l_4) \\
= & \sum \sigma(h_1, l_1)(h_2 l_2 \cdot a).
\end{aligned}$$

3. By 1 and 2 we can introduce a crossed product structure (with invertible cocycle) on $B \otimes H$, and we show that transporting this multiplication via Φ', $\Phi'(a \otimes h) = \Phi(a \otimes h)\Phi(1 \otimes 1)^{-1}$, we get the multiplication of A. First recall that the connection between the map γ (from 1 and 2) and Φ is given by:

$$\gamma(h) = \Phi(1 \otimes h)\Phi(1 \otimes 1)^{-1}.$$

Now we compute

$$
\begin{aligned}
&\Phi'((a\otimes h)(b\otimes l)) = \\
= \;& \Phi((a\otimes h)(b\otimes l))\Phi(1\otimes 1)^{-1} \\
= \;& \Phi(\sum a(h_1\cdot b)\sigma(h_2,l_1)\otimes h_3l_2)\Phi(1\otimes 1)^{-1} \\
= \;& \Phi(\sum a\gamma(h_1)b\gamma^{-1}(h_2)\gamma(h_3)\gamma(l_1)\gamma^{-1}(h_4l_2)\otimes h_5l_3)\Phi(1\otimes 1)^{-1} \\
= \;& \Phi(\sum a\gamma(h_1)b\gamma(l_1)\gamma^{-1}(h_2l_2)\otimes h_3l_3)\Phi(1\otimes 1)^{-1} \\
= \;& \sum a\gamma(h_1)b\gamma(l_1)\gamma^{-1}(h_2l_2)\Phi(1\otimes h_3l_3)\Phi(1\otimes 1)^{-1} \\
= \;& \sum a\gamma(h_1)b\gamma(l_1)\gamma^{-1}(h_2l_2)\gamma(h_3l_3) \\
= \;& a\Phi(1\otimes h)\Phi(1\otimes 1)^{-1}b\Phi(1\otimes l)\Phi(1\otimes 1)^{-1} \\
= \;& \Phi'(a\otimes h)\Phi'(b\otimes l),
\end{aligned}
$$

and the proof is complete. ∎

Remark 6.4.13 *A crossed product with trivial weak action is called a* twisted product. *From the above proof we obtain that a Galois extension A/B with $A \simeq B\otimes H$ (as left A-modules and right H-comodules), and with the property that B is contained in the center of A, is isomorphic to a twisted product of B and H.* ∎

6.5 Application to the duality theorems for co-Frobenius Hopf algebras

Throughout this section, H will be a co-Frobenius Hopf algebra over the field k. In this section we show that it is possible to derive the duality theorems for co-Frobenius Hopf algebras from Corollary 6.4.6.

Let $M, N \in \mathcal{M}_A^H$. Then we can consider $HOM_A(M,N)$ consisting of those $f \in Hom_A(M,N)$ for which there exist $f_0 \in Hom_A(M,N)$ and $f_1 \in H$ such that

$$\sum f(m_0)_0 \otimes f(m_0)_1 S(m_1) = \sum f_0(m)\otimes f_1. \tag{6.15}$$

We remark that $HOM_A(M,N)$ is the rational part of $Hom_A(M,N)$ with respect to the left H^*-module structure defined by

$$(h^*\cdot f)(m) = \sum h^*(f(m_0)_1 S(m_1)) f(m_0)_0. \tag{6.16}$$

If $M=N$, we denote

$$END_A(M) = HOM_A(M,M)$$

Definition 6.5.1 *We will denote by ${}_H\mathcal{M}_A^H$ the category whose objects are right A-modules M which are also left H-modules and right H-comodules such that the following conditions hold:*
i) M is a left H, right A-bimodule,
ii) M is a right (A,H)-Hopf module,
iii) M is a left-right H-Hopf module.
The morphisms in this category are the left H-linear, right A-linear and right H-colinear maps.
We will call ${}_H\mathcal{M}_A^H$ the category of two-sided (A,H)-Hopf modules. ∎

Example 6.5.2 *Let $M \in \mathcal{M}_A^H$ and consider $H \otimes M$ with the natural structures of a left H-module and right A-module, and with right H-comodule structure given by*

$$h \otimes m \longmapsto \sum h_1 \otimes m_0 \otimes h_2 m_1.$$

Then $H \otimes M$ is a two-sided (A,H)-Hopf module. In particular, $U = H \otimes A$ is a two-sided (A,H)-Hopf module. ∎

Remark 6.5.3 *Let $N \in \mathcal{M}_A$. Then $N \otimes H \in {}_H\mathcal{M}_A^H$ if we put*

$$(n \otimes h)b = \sum nb_0 \otimes hb_1,$$

and

$$\sum (n \otimes h)_0 \otimes (n \otimes h)_1 = \sum n \otimes h_1 \otimes h_2,$$

the left H-module structure being the natural one.
If $M \in \mathcal{M}_A^H$, then $M \otimes H \simeq H \otimes M$ (as in Example 6.5.2) in ${}_H\mathcal{M}_A^H$, the isomorphism (of right A-modules, left H-modules and right H-comodules) being given by

$$m \otimes h \mapsto \sum hS^{-1}(m_1) \otimes m_0 \text{ and } h \otimes m \mapsto \sum m_0 \otimes hm_1.$$

In particular, $U = H \otimes A \simeq A \otimes H$ in ${}_H\mathcal{M}_A^H$. ∎

Theorem 6.5.4 *Let A be a right H-comodule algebra, and $M \in {}_H\mathcal{M}_A^H$. Then*

$$End_A^H(M)\#H \longrightarrow END_A(M), \quad f \otimes h \longmapsto f \cdot h$$

is an isomorphism of right H-comodule algebras.

Proof: $END_A(M)$ is a right H-comodule with respect to the structure induced by the fact that it is a rational left H^*-module, the structure being given by (6.15). It is also a right H-module, with action induced by the left H-module structure on M.
If $f \in END_A(M)$, we denote by $\sum f_0 \otimes f_1$, the image of f through the H-comodule structure map: $(h^* \cdot f)(m) = \sum h^*(f_1)f_0(m)$, $\forall h^* \in H^*$. Let $f \in END_A(M)$, $h \in H$, and $h^* \in H^*$. Then we first have for any $m \in M$

$$\sum hm_0 \otimes S(m_1) = \sum h_1m_0 \otimes S(h_2m_1)h_3 = \sum(h_1m)_0 \otimes S((h_1m)_1)h_2 \tag{6.17}$$

because $M \in {}_H\mathcal{M}_A^H$. Now we compute

$$\begin{aligned}(h^* \cdot (fh))(m) &= \sum h^*((fh)(m_0)_1S(m_1))(fh)(m_0)_0\\ &= \sum h^*(f(hm_0)_1S(m_1))f(hm_0)_0\\ &= \sum h^*(f((h_1m)_0)_1S((h_1m)_1)h_2)f((h_1m)_0)_0 \text{ (by (6.17)}\\ &= \sum((h_2 \rightharpoonup h^*) \cdot f)(h_1m)\\ &= \sum(h_2 \rightharpoonup h^*)(f_1)f_0(h_1m)\\ &= \sum h^*(f_1h_2)(f_0h_1(m)\end{aligned}$$

which shows that $END_A(M)$ is an H-submodule of $End_A(M)$, and also a Hopf module.
Now $f \in END_A(M)^{coH}$ if and only if

$$\sum f(m_0)_0 \otimes f(m_0)_1S(m_1) = f(m) \otimes 1 \tag{6.18}$$

It is clear that (6.18) is satisfied if f is H-colinear and A-linear. We assume that $f \in End_A(M)$ and (6.18) holds, and we compute

$$\sum f(m)_0 \otimes f(m)_1 = \sum f(m_0)_0 \otimes f(m_0)_1S(m_1)m_2 = \sum f(m_0) \otimes m_1,$$

where we used (6.18) for m_0. In conclusion, $END_A(M)^{coH} = End_A^H(M)$, the endomorphism ring of M in $\mathcal{M}_A^H$, and the map in the statement is an isomorphism by the fundamental theorem for Hopf modules 4.4.6.
It remains to show that it is an isomorphism of right H-comodule algebras. First, $End_A^H(M)$ is a left H-module algebra via

$$(h \cdot f)(m) = \sum h_1f(S(h_2)m),$$

and it is even a left H-module algebra, because

$$(h \cdot (fe))(m) = \sum h_1(fe)(S(h_2)m)$$

$$\begin{aligned} &= \sum h_1 f(S(h_2)h_3 e(S(h_4)m)) \\ &= \sum (h_1 \cdot f)(h_2 e(S(h_3)m)) \\ &= \sum (h_1 \cdot f)(h_2 \cdot e)(m), \end{aligned}$$

and everything is proved. ∎

Exercise 6.5.5 *If A is a right H-comodule algebra, then*

$$A \xrightarrow{\sim} END_A(A), \ \ a \longmapsto f_a, \ \ f_a(b) = ab$$

is an isomorphism of H-comodule algebras.

From Corollary 6.4.6 we obtain immediately the duality theorem for actions of co-Frobenius Hopf algebras.

Corollary 6.5.6 *If $A'\#_\sigma H$ is a crossed product with invertible σ, then we have an isomorphism of algebras*

$$(A'\#_\sigma H)\#H^{*rat} \simeq M_H^f(A'),$$

where $M_H^f(A')$ denotes the ring of matrices with rows and columns indexed by a basis of H, and with only finitely many non-zero entries in A'.

Proof: The right H^*-module structure on $End(A'\#_\sigma H_{A'})$ is given by the left H^*-module structure on $A'\#_\sigma H$: $h^* \cdot (a\#h) = \sum a\#h_1 h^*(h_2)$. We know from Proposition 6.1.10 iv) that $A'\#_\sigma H \simeq H \otimes A'$ as right A'-modules and left H^*-modules via

$$a\#h \longmapsto \sum h_4 \otimes (S^{-1}(h_1) \cdot a)\sigma(S^{-1}(h_2), h_1),$$

and so $A'\#_\sigma H_{A'}$ is free. Then $End(A'\#_\sigma H_{A'})$ is the ring of row-finite matrices with entries in A' and rows and columns indexed by a basis of H. In order to see who is $End(A'\#_\sigma H_{A'})^{rat}$ we choose the following basis of H: as before Corollary 3.2.17, write $H = \oplus E(S_\lambda)$, where the S_λ's are simple left H-comodules and $E(S_\lambda)$ denotes the injective envelope of S_λ. Then we denote by $\{h_i\}_i$ the basis of H obtained by putting together bases in the $E(S_\lambda)$'s, and use the basis $\{h_i \otimes 1\}_i$ in $H \otimes A' \simeq A'\#_\sigma H$ to write $End(A'\#_\sigma H_{A'})$ as a matrix ring. We denote by p_λ the map in H^{*rat} equal to ε on $E(S_\lambda)$ and 0 elsewhere.
In order to prove the assertion in the statement it is enough to prove that any f with $f(h_i \otimes 1) \neq 0$ and $f(h_j \otimes 1) = 0$ for $j \neq i$ is in the rational part. Say $h_i \in E(S_\lambda)$. Then it is easy to see that $f = f \cdot p_\lambda$.
The converse inclusion is clear, since for any f and any p_λ, $f \cdot p_\lambda$ is 0 outside $E(S_\lambda)$. ∎

We move next to the second duality theorem. We need first some preparations.

Lemma 6.5.7 *Let R be a ring without unit and M_R a right R-module with the property that there exists a common unit (in R) for any finite number of elements in R and M. Then*

$$M_R \simeq Hom_R(R_R, M_R) \cdot R,$$

where, for $f \in Hom_R(R_R, M_R)$ and $r, s \in R$, $(f \cdot r)(s) = f(rs)$.

Proof: The isomorphism sends $m \in M$ to $\rho_m(r) = mr$, for all $r \in R$. The inverse sends $\sum f_i \cdot r_i$ to $\sum f_i(r_i)$. ∎

Corollary 6.5.8 *If R and M are as in Lemma 6.5.7 and $M_R \simeq R_R$, then*

$$R \simeq End(M_R) \cdot R$$

(as rings.) ∎

Lemma 6.5.9 *Let $H \otimes A$ be the two-sided Hopf module from Example 6.5.2. Then*

$$H \otimes A \simeq A\#H^{*rat}$$

as right $A\#H^{*rat}$-modules, via

$$h \otimes a \longmapsto \sum a_0 \# t \leftharpoonup h a_1,$$

where t is a right integral of H.

Proof: Recall that $H \otimes A$ becomes a right $A\#H^{*rat}$-module via

$$(h \otimes a)(b\#h^*) = \sum h_1 \otimes a_0 b_0 h^*(S^{-1}(h_2 a_1 b_1)).$$

If we denote by θ the map in the statement, which is clearly a bijection, then we have to show that

$$\theta((h \otimes a)(b\#h^*)) = (\theta(h \otimes a))(b\#h^*),$$

i.e. that

$$\sum a_0 b_0 \# t \leftharpoonup h_1 a_1 b_1 h^*(S^{-1}(h_2 a_2 b_2)) = \sum a_0 b_0 \#(t \leftharpoonup h a_1 b_1) h^*.$$

If we apply the second parts to an element x, and denote $y = h a_1 b_1$ and $z = S^{-1}(y)$, then this gets down to

$$\sum t(S(z_2)x) z_1 = \sum t(S(z) x_1) x_2,$$

which is exactly Lemma 5.1.4 applied to $H^{op\ cop}$. ∎

As a consequence of the above we obtain the following

Corollary 6.5.10 *If H is co-Frobenius and A is a right H-comodule algebra, then*

$$A\#H^{*rat} \simeq End_{A\#H^{*rat}}(H\otimes A_{A\#H^{*rat}})\cdot A\#H^{*rat} = End_A^H(H\otimes A)\cdot H^{*rat}.$$

∎

Let us describe now explicitely the left H^*-module structure on $H \otimes A$ obtained via the isomorphism θ of Lemma 6.5.9. This is given by

$$h^* \cdot (h \otimes a) = \sum h^*(S(h_1)g^{-1})h_2 \otimes a \tag{6.19}$$

where $h^* \in H^*$, $h \in H$, $a \in A$ and g is the distinguished grouplike element (denoted there by a) from Proposition 5.5.4 (iii).
Indeed, we have

$$\begin{aligned}(1\#h^*)\theta(h \otimes a) &= (1\#h^*)(\sum a_0\#t \leftharpoonup ha_1)\\ &= \sum a_0\#(h^* \leftharpoonup a_1)(t \leftharpoonup ha_2)\\ &= \sum a_0\#h^*(S(h_1)g^{-1})t \leftharpoonup h_2a_1\\ &= \theta(\sum h^*(S(h_1)g^{-1})h_2 \otimes a),\end{aligned}$$

since we have, for all $h, x \in H$

$$\sum h^*(S(h_1)g^{-1})t \leftharpoonup h_2x = \sum(h^* \leftharpoonup x_1)(t \leftharpoonup hx_2).$$

The last equality may be checked as follows. Apply both sides to an element $w \in H$ and denote $y = xw$ to get

$$\sum h^*(S(h_1)g^{-1})t(h_2y) = \sum h^*(y_1)t(hy_2).$$

Now denote $u = S(gh)$ and $t' = t \leftharpoonup g^{-1}$ to obtain

$$\sum t'(S^{-1}(u_1)y)u_2 = \sum t'(S^{-1}(u)y_2)y_1,$$

which is exactly Lemma 5.1.4 applied to H^{op}, for which t' is still a left integral. This proves (6.19).

We are ready to prove the second duality theorem for co-Frobenius Hopf algebras.

Theorem 6.5.11 *Let H be a co-Frobenius Hopf algebra and A a right H-comodule algebra. Then*

$$(A\#H^{*rat})\#H \simeq M_H^f(A),$$

where $M_H^f(A)$ denotes the ring of matrices with rows and columns indexed by a basis of H, and with only finitely many non-zero entries in A.

Proof: We write first Theorem 6.5.4 for the two-sided Hopf module $H\otimes A$ from Example 6.5.2:

$$End_A^H(H\otimes A)\#H\simeq END_A(H\otimes A).$$

Now we define the right H^*-module structure on $END_A(H\otimes A)$ as follows: if $f\in END_A(H\otimes A)$ and $f=\sum f_ie_i$ for some $f_i\in End_A^H(H\otimes A)$ and $e_i\in H$, then

$$f\cdot h^*=\sum(f_i\cdot h^*)e_i \tag{6.20}$$

We now take the rational part on both sides of the above isomorphism with respect to the H^*-module structure in (6.20), and use Corollary 6.5.10 to get

$$(A\#H^{*rat})\#H\simeq END_A(H\otimes A)\cdot H^{*rat}.$$

To finish the proof, we describe $END_A(H\otimes A)\cdot H^{*rat}$ as a matrix ring. More precisely, we show that

$$END_A(H\otimes A)\cdot H^{*rat}\simeq M_H^f(A),$$

where the H^*-module structure is the one given by (6.20). We define another H^*-module structure on $END_A(H\otimes A)$ and show that the rational parts with respect to this module structure and the one given by (6.20) are the same. Define, for $h^*\in H^*$, $f\in END_A(H\otimes A)$

$$(f\odot h^*)(h\otimes a)=\sum f(h^*(S(h_1)g^{-1})h_2\otimes a).$$

We check that $END_A(H\otimes A)\cdot H^{*rat}=END_A(H\otimes A)\odot H^{*rat}$. Let $f\in END_A(H\otimes A)$, $f=\sum f_je_j$, $f_j\in End_A^H(H\otimes A)$, $e_j\in H$. Then

$$\begin{aligned}
(f\cdot h^*)(h\otimes a) &= \sum((f_j\cdot h^*)e_j)(h\otimes a)\\
&= \sum(f_j\cdot h^*)(e_jh\otimes a)\\
&= \sum h^*(S(e_{j_1}h_1)g^{-1})f_j(e_{j_2}h_2\otimes a)(\text{we used }(6.19))\\
&= \sum(S(ge_{j_1}g^{-1})\rightharpoonup h^*)(S(h_1)g^{-1})(f_jej_2)(h_2\otimes a)\\
&= \sum(f_je_{j_2})\odot(S(ge_{j_1}g^{-1})\rightharpoonup h^*)(h\otimes a),
\end{aligned}$$

which shows that $END_A(H\otimes A)\cdot H^{*rat}\subseteq END_A(H\otimes A)\odot H^{*rat}$. Conversely, if $f\in END_A(H\otimes A)$, $f=\sum f_je_j$, $f_j\in End_A^H(H\otimes A)$, $e_j\in H$, then

$$(f\odot h^*)(h\otimes a) = ((\sum f_je_j)\odot h^*)(h\otimes a)$$

$$\begin{aligned}
&= \sum h^*S(gh_1)f_j(e_jh_2 \otimes a) \\
&= \sum h^*S(gS(e_{j_1})e_{j_2}h_1)f_j(e_{j_3}h_2 \otimes a) \\
&= \sum h^*S(S(ge_{j_1}g^{-1})ge_{j_2}h_1)f_j(e_{j_3}h_2 \otimes a) \\
&= \sum h^*(S(ge_{j_2}h_1)S^2(ge_{j_1}g^{-1}))f_j(e_{j_3}h_2 \otimes a) \\
&= \sum (S^2(ge_{j_1}g^{-1}) \rightharpoonup h^*)(S(ge_{j_2}h_1))f_j(e_{j_3}h_2 \otimes a) \\
&= \sum (f_j \cdot (S^2(ge_{j_1}g^{-1}) \rightharpoonup h^*))(e_{j_2}h \otimes a) \\
&= (\sum (f_j \cdot (S^2(ge_{j_1}g^{-1}) \rightharpoonup h^*))e_{j_2})(h \otimes a),
\end{aligned}$$

showing that $END_A(H \otimes A) \odot H^{*rat} \subseteq END_A(H \otimes A) \cdot H^{*rat}$.
Now write $H = \oplus E(S_\lambda)$, where the S_λ's are simple right H-comodules, and take $\{h_i\}$ a basis in each $E(S_\lambda)$. Put them together and take $\{g^{-1}h_i \otimes 1\}$, which is an A-basis for $H \otimes A$. Use this basis to view the elements of $END_A(H \otimes A)$ as row finite matrices with entries in A. We show now that under this identification the elements of $END_A(H \otimes A) \odot H^{rat}$ are represented by finite matrices. As in the proof of Corollary 6.5.6, we denote by p_λ the linear form on H equal to ε on $E(S_\lambda)$ and 0 elsewhere. It is easy to see that for every $f \in End_A(H \otimes A)$, $f \odot p_\lambda S^{-1}$ is represented by a finite matrix for all λ. Conversely, if $f(g^{-1}h_i \otimes 1) \neq 0$ and $f(g^{-1}h_j \otimes 1) = 0$ for all $j \neq i$, then clearly $f \in END_A(H \otimes A)$. Moreover, if $h_i \in E(S_\lambda)$, then if $h_j \in E(S_\lambda)$, we have

$$\begin{aligned}
(f \odot p_\lambda S^{-1})(g^{-1}h_j \otimes 1) &= \sum p_\lambda S^{-1}(S(gg^{-1}h_{j_1})f(g^{-1}h_{j_2} \otimes 1) \\
&= \sum \varepsilon(h_{j_1})f(g^{-1}h_{j_2} \otimes 1) \\
&= f(g^{-1}h_j \otimes 1).
\end{aligned}$$

Since for $h_j \notin E(S_\lambda)$, $(f \odot p_\lambda S^{-1})(g^{-1}h_j \otimes 1) = f(g^{-1}h_j \otimes 1) = 0$, we get that $f = f \odot p_\lambda S^{-1} \in END_A(H \otimes A) \odot H^{*rat}$, and the proof is complete.∎

We end this section with some exercise concerning injective objects in the category of relative Hopf modules.

Exercise 6.5.12 *Show that ${}_A\mathcal{M}^H = \sigma_{A\#H^*}[A \otimes H]$. In particular, ${}_A\mathcal{M}^H$ is a Grothendieck category.*

Exercise 6.5.13 *Let H be a co-Frobenius Hopf algebra. Then the following assertions hold:*
(i) If $M \in {}_{H^*}\mathcal{M}$, then $M^{rat} = H^{*rat}M$.
(ii) $\sigma_{A\#H^*}[A \otimes H]$ is a localizing subcategory of ${}_{A\#H^*}\mathcal{M}$.
(iii) The radical associated to the localizing subcategory $\sigma_{A\#H^*}[A \otimes H]$, and

the identification of $\sigma_{A\#H^*}[A \otimes H]$ and ${}_A\mathcal{M}^H$ produces an exact functor $t : {}_{A\#H^*}\mathcal{M} \to {}_A\mathbf{M}^H$, given by $t(M) = H^{*rat}M$.
(iv) $H \otimes A$ is a projective generator of ${}_A\mathcal{M}^H$.

Exercise 6.5.14 *Let H be a co-Frobenius Hopf algebra, $v^* \in H^{*rat}$ and $h \in H$. Then:*
i) For $h^* \in H^*$, $\sum (v^*h^*)_0 \otimes (v^*h^*)_1 = \sum v_0^*h^* \otimes v_1^*$.
ii) $v^* \leftharpoonup h \in H^{*rat}$, and $\sum (v^* \leftharpoonup h)_0 \otimes (v^* \leftharpoonup h)_1 = \sum (v_0^* \leftharpoonup h_2) \otimes (S(h_1) \rightharpoonup v_1^*)$, (where by $v^* \mapsto v_0^* \otimes v_1^*$ we denote the right H-comodule structure of H^{*rat} induced by the rational left H^*-structure of H^{*rat}).

Exercise 6.5.15 *Let H be a co-Frobenius Hopf algebra and A an H-comodule algebra. Then the following assertions hold:*
i) Let $M \in {}_A\mathcal{M}^H$. Then $Hom_{H^*}(H^{*rat}, M)$ is a left $A\#H^*$-module by

$$((a\#h^*)f)(v^*) = \sum a_0 f((v^* \leftharpoonup a_1)h^*)$$

for any $f \in Hom_{H^*}(H^{*rat}, M)$, $a\#h^* \in A\#H^*$ and $v^* \in H^{*rat}$. If $\varphi : M \to P$ is a morphism in ${}_A\mathcal{M}^H$, then the induced application $\overline{\varphi} : Hom_{H^*}(H^{*rat}, M) \to Hom_{H^*}(H^{*rat}, P)$ is a morphism of $A\#H^*$-modules.
ii) The functor $F : {}_A\mathcal{M}^H \to {}_{A\#H^*}\mathcal{M}$, $F(M) = Hom_{H^*}(H^{*rat}, M)$ is a right adjoint of the radical functor $t : {}_{A\#H^*}\mathcal{M} \to {}_A\mathcal{M}^H$, $t(N) = H^{*rat}N$.

For the next exercises we will need the following definition: we say that a right H-comodule M has *finite support* if there exists a finite dimensional subspace X of H such that $\rho_M(M) \subseteq M \otimes X$, where $\rho_M : M \to M \otimes H$ is the comodule structure map of M. An object $M \in {}_A\mathcal{M}^H$ has finite support if M has finite support as a H-comodule.

Exercise 6.5.16 *Let H be a co-Frobenius Hopf algebra, and A a right H-comodule algebra. Then the following assertions hold:*
i) Let $M \in {}_A\mathcal{M}^H$. Then the map

$$\gamma_M : M \to Hom_{H^*}(H^{*rat}, M),$$

$\gamma_M(m)(v^*) = v^*m = \sum v^*(m_1)m_0$ for any $m \in M, v^* \in H^{*rat}$, is an injective morphism of $A\#H^*$-modules.
ii) If $M \in {}_A\mathbf{M}^H$ has finite support, then γ_M is an isomorphism of $A\#H^*$-modules.

Exercise 6.5.17 *Let H be a co-Frobenius Hopf algebra, and A an H-comodule algebra. If $M \in {}_A\mathcal{M}^H$ is an injective object with finite support, then M is injective as an A-module.*

6.6 Solutions to exercises

Exercise 6.2.6 *With the multiplication defined in (6.5), $\#(H,A)$ is an associative ring with multiplicative identity $u_H\varepsilon_H$. Moreover, A is isomorphic to a subalgebra of $\#(H,A)$ by identifying $a\in A$ with the map $h\longmapsto \varepsilon(h)a$. Also $H^*=Hom(H,k)$ is a subalgebra of $\#(H,A)$.*
Solution: We first have

$$\begin{aligned}((f\cdot g)\cdot e)(h) &= \sum (f\cdot g)(e(h_2)_1h_1)e(h_2)_0\\ &= \sum f(g(e(h_3)_2h_2)_1e(h_3)_1h_1)g(e(h_3)_2h_2)_0e(h_3)_0\\ &= \sum f((g\cdot e)(h_2)_1h_1)(g\cdot e)(h_2)_0\\ &= (f\cdot(g\cdot e))(h)\end{aligned}$$

so the multiplication is associative. The other assertions are clear.

Exercise 6.2.8 *In general, $A\#H^{*rat}$ is properly contained in $\#(H,A)^{rat}$.*
Solution: Let H be any infinite dimensional Hopf algebra with bijective antipode, let $A=H$, and consider the map $\overline{S}\in\#(H,H)$. For any $h^*\in H^*\subset \mathrm{Hom}(H,H), x\in H$, by the multiplication in $\#(H,H)$ we have

$$(h^*\cdot\overline{S})(x)=\sum h^*(\overline{S}(x_2)_2x_1)\overline{S}(x_2)_1=h^*(1)\overline{S}(x)$$

so $\overline{S}\in\#(H,H)^{rat}$. But no bijection ψ from H to H lies in $H\#H^*$. For if $\psi=\sum h_i\#h_i^*\in H\#H^*$, choose $x\in H$, x not in the finite dimensional subspace of H spanned by the h_i. However $x=\psi(\psi^{-1}(x))=\sum h_i\langle h_i^*,\psi^{-1}(x)\rangle$, a contradiction.

Exercise 6.2.12 *Let H be co-Frobenius Hopf algebra and M a unital left $A\#H^{*rat}$-module. Then for any $m\in M$ there exists an $u^*\in H^{*rat}$ such that $m=u^*\cdot m=(1\#u^*)\cdot m$, so M is a unital left H^{*rat}-module, and therefore a rational left H^*-module.*
Solution: Let $m\in M$, $m=\sum(a_i\#h_i^*)\cdot m_i$. We take $u^*\in H^{*rat}$ equal to ε on the finite dimensional subspace generated by $a_{i_1}h_{i_1}^*$, and zero elsewhere. Then $(1\#u^*)(a_i\#h_i^*=a_i\#h_i^*$ for all i, so $m=u^*\cdot m$. Then we can define an action of H^* on M by $h^*\cdot m=h^*u^*\cdot m$, if $h^*\in H^*$, $m\in M$, $u^*\in H^{*rat}$, and $m=u^*\cdot m$. The definition is correct, because H^{*rat} is an ideal of H^*, and H^{*rat} itself is a unital left H^{*rat}-module. Now $h^*\cdot m=h^*u^*\cdot m=\sum h^*(u_1^*)u_0^*\cdot m$, so M is rational.

Exercise 6.2.13 *Consider the right H-comodule algebra A with the left and right $A\#H^*$-module structures given by the fact that $A\in\mathcal{M}_A^H$ and*

$A \in {}_A\mathcal{M}^H$:

$$a \cdot (b\#h^*) = \sum a_0 b_0 h^*(S^{-1}(a_1 b_1)), \quad (b\#h^*) \cdot a = \sum b a_0 h^*(a_1).$$

Then A is a left $A\#H^*$ and right A^{coH}-bimodule, and a left A^{coH} and right $A\#H^*$-bimodule. Consequently, the map

$$\pi : A\#H^{*rat} \longrightarrow End(A_{A^{coH}}), \quad \pi(a\#l)(b) = (a\#l) \cdot b,$$

is a ring morphism.
Solution: If $c \in A^{coH}$, then

$$\begin{aligned} ((b\#h^*) \cdot a)c &= \sum b a_0 c h^*(a_1) \\ &= \sum b a_0 c_0 h^*(a_1 c_1) \\ &= \sum b(ac)_0 h^*((ac)_1) = (b\#h^*) \cdot ac, \end{aligned}$$

and a similar computation shows the other assertion.

Exercise 6.2.14 *Let A be a right H-comodule algebra and consider A as a left or right $A\#H^{*rat}$-module as in Exercise 6.2.13. Then:*
i) $A^{coH} \simeq End({}_{A\#H^{*rat}}A)$
ii) $A^{coH} \simeq End(A_{A\#H^{*rat}})$.
Solution: We prove only the first assertion. We have that for each $X \in {}_A\mathcal{M}^H \simeq Mod_l(A\#H^{*rat})$, $Hom_{A\#H^{*rat}}(A, X) \simeq Hom_A^H(A, X) \simeq X^{coH}$, which for $X = A$ gives the desired ring isomorphism.

Exercise 6.2.20 *(Maschke's Theorem for smash products) Let H be a semisimple Hopf algebra, and A a left H-module algebra. Let V be a left $A\#H$-module, and W an $A\#H$-submodule of V. If W is a direct summand in V as A-modules, then it is a direct summand in V as $A\#H$-modules.*
Solution: Let $t \in H$ be a left integral with $\varepsilon(t) = 1$. Then t is also a right integral, and $S(t) = t$. Let $\lambda : V \longrightarrow W$ be the projection as A-modules. We define

$$\lambda' : V \longrightarrow W, \quad \lambda'(v) = \sum (1\#S(t_1))\lambda((1\#t_2)v).$$

We show that λ' is a projection as $A\#H$-modules. We check first that λ' is $A\#H$-linear. Since S is bijective, we can use tensor monomials of the form $a\#S(h)$:

$$\begin{aligned} (a\#S(h))\lambda'(v) &= (a\#S(h)) \sum (1\#S(t_1))\lambda((1\#t_2)v) \\ &= \sum (a\#S(h))(1\#S(t_1))\lambda((1\#t_2)v) \end{aligned}$$

$$\begin{aligned}
&= \sum (a\#S(t_1h))\lambda((1\#t_2)v) \\
&= \sum (a\#S(t_1h_1))\lambda((1\#t_2h_2S(h_3))v) \\
&= \sum (a\#S(t_1))\lambda((1\#t_2\varepsilon(h_1)S(h_2))v)(t \text{ right integral}) \\
&= \sum (a\#S(t_1))\lambda((1\#t_2S(h))v) \\
&= \sum (1\#S(t_1)_2)(S^{-1}(S(t_1)_1)\cdot a\#1) \\
&\quad \lambda((1\#t_2S(h))v) \text{ (by Lemma 6.1.8)} \\
&= \sum (1\#S(t_1))(t_2\cdot a\#1)\lambda((1\#t_3S(h))v) \\
&= \sum (1\#S(t_1))\lambda((t_2\cdot a\#1)(1\#t_3S(h))v) \ (\lambda\ A\text{-linear}) \\
&= \sum (1\#S(t_1))\lambda((t_2\cdot a\#t_3S(h))v) \\
&= \sum (1\#S(t_1))\lambda((1\#t_2)(a\#S(h))v) \\
&= \sum (1\#S(t_1))\lambda((1\#t_2)(a\#S(h))v) \\
&= \lambda'((a\#S(h))v),
\end{aligned}$$

so λ' is $A\#H$-linear. It remains to check that it is a projection. If $w \in W$, then $(1\#t_2)w \in W$, so $\lambda((1\#t_2)w) = (1\#t_2)w$. We have thus

$$\lambda'(w) = \sum (1\#S(t_1)t_2)w = (1\#\varepsilon(t)1)w = w,$$

and the proof is complete.

Exercise 6.3.2 *If the map $[-,-]$ from the Morita context in Proposition 6.3.1 is surjective, then it is bijective.*

Solution: Assume $[-,-]$ is surjective, and let $\sum a_i \otimes b_i$ be an element in the kernel. Choose $u^* \in H^{*rat}$ a common right unit for the elements b_i (u^* may be chosen to agree with ε on the finite dimensional subspace generated by the b_{i_1}'s). Let $\sum [a'_j, b'_j] = u^*$. Then we have

$$\begin{aligned}
\sum a_i \otimes b_i &= \sum a_i \otimes b_i \cdot u^* \\
&= \sum a_i \otimes b_i \cdot [a'_j, b'_j] \\
&= \sum a_i \otimes (b_i, a'_j)b'_j \\
&= \sum a_i(b_i, a'_j) \otimes b'_j \\
&= \sum [a_i, b_i]a'_j \otimes b'_j = 0.
\end{aligned}$$

Exercise 6.3.4 *Let H be a finite dimensional Hopf algebra. Then a right*

H-comodule algebra A has a total integral if and only if the corresponding left H^*-module algebra A has an element of trace 1.
Solution: Let $\Phi : H \to A$ be a total integral, and $t \in H^*$ a left integral. Let $h \in H$ be such that $t(h) = 1$, so $\sum h_1 t(h_2) = t(h)1 = 1$. Then $\Phi(h)$ is an element of trace 1.
Conversely, if t is as above, and c is an element of trace 1, then $\Phi : H \to A$, $\Phi(h) = \sum c_0 t(c_1 S(h))$ is colinear by Lemma 5.1.4, and takes 1 to 1, hence it is a total integral.

Exercise 6.4.2 *If S is bijective, then can is bijective if and only if can′ is bijective.*
Solution: We have

$$can(a \otimes b) = \phi \circ can'(a \otimes b),$$

where $\phi : A \otimes H \longrightarrow A \otimes H$ is the map given by $\phi(a \otimes h) = (1 \otimes S^{-1}(h))\rho(a)$. This is invertible, with inverse given by $\phi^{-1}(a \otimes h) = \rho(a)(1 \otimes S(h))$.

Exercise 6.4.11 *Let H be a co-Frobenius Hopf algebra over the field k, and A a right H-comodule algebra with structure map*

$$\rho : A \longrightarrow A \otimes A \otimes H, \ \ \rho(a) = \sum a_0 \otimes a_1.$$

If A/A^{coH} is a separable Galois extension, then H is finite dimensional.
Solution: H has a direct sum decomposition

$$H = \bigoplus_{\lambda \in I} E(M_\lambda),$$

where the M_λ's are simple left subcomodules of H, and $E(M_\lambda)$ is the injective envelope. We know the $E(M_\lambda)$'s (which we are going to denote by H_λ) are finite dimensional subspaces of H. Therefore, if H is infinite dimensional it follows that I is an infinite set. Denote, for each $\lambda \in I$, by p_λ the map in H^{*rat} which is equal to ε on H_λ and equal to zero elsewhere. We also know that for any $f \in H^{*rat}$ there exists a finite set $F \subseteq I$ such that

$$f = \sum_{\lambda \in F} f p_\lambda. \tag{6.21}$$

Now the extension A/A^{coH} is a Galois extension, which means that the map

$$can : A \otimes_{A^{coH}} A \longrightarrow A \otimes H, \quad can(a \otimes b) = \sum ab_0 \otimes b_1$$

is bijective. Let us denote, for each $\lambda \in I$,

$$A_\lambda = p_\lambda \cdot A = \{\sum a_0 p_\lambda(a_1) \mid \ a \in A\}.$$

We have clearly that $A = \sum_{\lambda \in I} A_\lambda$, since for any $a \in A$ we have $a = \sum p_\lambda \cdot a$, where the p_λ's are the ones corresponding to the finite dimensional subspace of H generated by the a_1's. Furthermore, we have

$$\rho(A_\lambda) \subseteq A \otimes H_\lambda. \tag{6.22}$$

Indeed, for an $a \in A$ we have

$$\rho(p_\lambda \cdot a) = \sum a_0 \otimes a_1 p_\lambda(a_2) = \sum a_0 \otimes p_\lambda \cdot a_1.$$

Now $p_\lambda \cdot H = \{\sum h_1 p_\lambda(h_2) \mid \quad h \in H\} \subseteq H_\lambda$, since for any $\mu \neq \lambda$ we have that p_λ annihilates the left subcomodule H_μ.
We claim that $A_\lambda \neq 0$ for all $\lambda \in I$. Indeed, suppose that $A_{\lambda_0} = 0$. Then

$$can(A \otimes_{A^{coH}} A) \subseteq \sum_\lambda can(A \otimes A_\lambda) \subseteq \sum_{\lambda \neq \lambda_0} A \otimes H_\lambda,$$

by the definition of can and (6.22), and this is a contradiction because the image of can has to be all of $A \otimes H$.
We use now the fact that A/A^{coH} is a separable extension. Then there is a separabilty idempotent in $A \otimes_{A^{coH}} A$, $\sum a_i \otimes b_i$. This means that

$$\sum a_i b_i = 1, \text{ and } \sum c a_i \otimes b_i = \sum a_i \otimes b_i c, \quad \forall c \in A.$$

Denote by W the finite dimensional subspace of H generated by the elements b_{i_1}, and by $p_W \in H^{*rat}$ a map equal to ε on W. Then $p_W \leftharpoonup b_{i_1}$ are a finite number of elements in H^{*rat}. Since I is infinite, we can choose λ_0 which does not appear among the p_λ's associated to all the $p_W \leftharpoonup b_{i_1}$ as in (6.21). In other words, we assume that $(p_W \leftharpoonup b_{i_1})$ are zero on H_{λ_0}.
Pick now $c \in A_{\lambda_0}$, $c \neq 0$, and apply $Id \otimes \rho$ to the equality

$$\sum c a_i \otimes b_i = \sum a_i \otimes b_i c.$$

We get

$$\sum c a_i \otimes b_{i_0} \otimes b_{i_1} = \sum a_i \otimes b_{i_0} c_0 \otimes b_{i_1} c_1.$$

If we apply now $M \circ (I \otimes I \otimes p_W)$ (where M is the multiplication of H) to both sides of the above equality, on the left-hand side we get $\sum c a_i b_i = c$, while on the other side we get

$$\sum a_i b_{i_0} c_0 p_W(b_{i_1} c_1) = \sum a_i b_{i_0} c_0 (p_W \leftharpoonup b_{i_1})(c_1) = 0,$$

since $c_1 \in H_{\lambda_0}$ by (6.22). Therefore we have obtained that $c = 0$, which is the desired contradiction.

Exercise 6.5.5 *If A is a right H-comodule algebra, then*

$$A \xrightarrow{\sim} END_A(A), \quad a \longmapsto f_a, \quad f_a(b) = ab$$

is an isomorphism of H-comodule algebras.
Solution: If $h^* \in H^*$ and $a, b \in A$, then

$$\begin{aligned}(h^* \cdot f_a)(b) &= \sum f_a(b_0)_0 h^*(f_a(b_0)_1 S(b_1)) \\ &= \sum a_0 b_0 h^*(a_1 b_1 S(b_2)) \\ &= \sum a_0 b h^*(a_1) = \sum h^*(a_1) f_{a_0}(b)\end{aligned}$$

which proves the desired isomorphism.

Exercise 6.5.12 *Show that ${}_A\mathcal{M}^H = \sigma_{A\#H^*}[A \otimes H]$. In particular, ${}_A\mathcal{M}^H$ is a Grothendieck category.*
Solution: By Proposition 6.2.11, if $M \in {}_A\mathcal{M}^H$, then M becomes a left $A\#H^*$-module via

$$(a\#h^*) \cdot m = \sum a m_0 h^*(m_1).$$

Since M is an H-comodule, M embeds in $H^{(I)}$ for some set I (see Corollary 2.5.2). Then $A \otimes M$ embeds in $A \otimes H^{(I)} \simeq (A \otimes H)^{(I)}$, so $M \in \sigma_{A\#H^*}[A \otimes H]$.

Exercise 6.5.13 it Let H be a co-Frobenius Hopf algebra. Then the following assertions hold:
(i) If $M \in {}_{H^*}\mathcal{M}$, then $M^{rat} = H^{*rat}M$.
(ii) $\sigma_{A\#H^*}[A \otimes H]$ is a localizing subcategory of ${}_{A\#H^*}\mathcal{M}$.
(iii) The radical associated to the localizing subcategory $\sigma_{A\#H^*}[A \otimes H]$, and the identification of $\sigma_{A\#H^*}[A \otimes H]$ and ${}_A\mathcal{M}^H$ produces an exact functor $t : {}_{A\#H^*}\mathcal{M} \to {}_A\mathbf{M}^H$, given by $t(M) = H^{*rat}M$.
(iv) $H \otimes A$ is a projective generator of ${}_A\mathcal{M}^H$.
Solution: i) The proof is the same as the one in Exercise 6.2.12: we know that $H^{*rat}M \subseteq M^{rat}$. Let now $m \in M^{rat}$, and $\nu(m) = \sum m_0 \otimes m_1$, where ν is the right H-comodule structure map of M^{rat}. Since H^{*rat} is dense in H^*, there exists $h^* \in H^{*rat}$ acting as ε on the finite subspace generated by the m_1's. Then $m = h^*m \in H^{*rat}M$.
(ii) It remains to show that $\sigma_{A\#H^*}[A \otimes H]$ is closed under extensions. Let $0 \to N \to M \to P \to 0$ be an exact sequence of $A\#H^*$-modules such that $N, P \in \sigma_{A\#H^*}[A \otimes H]$. Then $N = H^{*rat}N$ and $P = H^{*rat}P$, and it can be easily seen that these imply $M = H^{*rat}M$, i.e. $M \in \sigma_{A\#H^*}[A \otimes H]$.
(iii) follows from Corollary 3.2.12.
(iv) Let $M \in {}_A\mathcal{M}^H$. By Corollary 3.3.11, H is a projective generator in

the category $\mathcal{M}^H$. Then regarding M as an object in $\mathcal{M}^H$, we have a surjective morphism of H-comodules $H^{(I)} \to M$ for some set I. The functor $A\otimes - : \mathcal{M}^H \to {}_A\mathcal{M}^H$ has a right adjoint, so it is right exact and commutes with direct sums. We obtain a surjection $(A\otimes H)^{(I)} \simeq A\otimes H^{(I)} \to A\otimes M$. Composing this with the module structure map $A\otimes M \to M$ of M, we obtain a surjective morphism $(A\otimes H)^{(I)} \to M$ in ${}_A\mathcal{M}^H$. Thus $A\otimes H$ is a generator. Since the functor $A\otimes -$ takes projectives to projectives (as a left adjoint of an exact functor), $A\otimes H$ is projective.

Exercise 6.5.14 *Let H be a co-Frobenius Hopf algebra, $v^* \in H^{*rat}$ and $h \in H$. Then:*
i) For $h^* \in H^*$, $\sum (v^*h^*)_0 \otimes (v^*h^*)_1 = \sum v_0^*h^* \otimes v_1^*$.
ii) $v^* \leftharpoonup h \in H^{*rat}$, and $\sum (v^* \leftharpoonup h)_0 \otimes (v^* \leftharpoonup h)_1 = \sum (v_0^* \leftharpoonup h_2) \otimes (S(h_1) \rightharpoonup v_1^*)$, (where by $v^* \mapsto v_0^* \otimes v_1^*$ we denote the right H-comodule structure of H^{*rat} induced by the rational left H^*-structure of H^{*rat}).
Solution: i) If $l^* \in H^*$, we have $l^*(v^*h^*) = (l^*v^*)h^* = \sum l^*(v_1^*)v_0^*h^*$.
ii) Let $h^* \in H^*$ and $l \in H$. We have

$$\begin{aligned}
(h^*(v^* \leftharpoonup h))(l) &= \sum h^*(l_1)v^*(h \rightharpoonup l_2)\\
&= \sum h^*(S(h_1)h_2 \rightharpoonup l_1)v^*(h_3 \rightharpoonup l_2)\\
&= \sum ((h^* \leftharpoonup S(h_1))v^*)(h_2 \leftharpoonup l)\\
&= \sum (h^* \rightharpoonup S(h_1))(v_1^*)v_0^*(h_2 \rightharpoonup l)\\
&= (\sum h^*(S(h_1) \rightharpoonup v_1^*)(v_0^* \leftharpoonup h_2))(l)
\end{aligned}$$

Therefore $h^*(v^* \leftharpoonup h) = \sum h^*(S(h_1) \rightharpoonup v_1^*)(v_0^* \leftharpoonup h_2)$, which proves everything.

Exercise 6.5.15 *Let H be a co-Frobenius Hopf algebra and A an H-comodule algebra. Then the following assertions hold:*
i) Let $M \in {}_A\mathcal{M}^H$. Then $Hom_{H^*}(H^{*rat}, M)$ is a left $A\#H^*$-module by

$$((a\#h^*)f)(v^*) = \sum a_0 f((v^* \leftharpoonup a_1)h^*)$$

for any $f \in Hom_{H^*}(H^{*rat}, M)$, $a\#h^* \in A\#H^*$ and $v^* \in H^{*rat}$. If $\varphi : M \to P$ is a morphism in ${}_A\mathcal{M}^H$, then the induced application $\overline{\varphi} : Hom_{H^*}(H^{*rat}, M) \to Hom_{H^*}(H^{*rat}, P)$ is a morphism of $A\#H^*$-modules.
ii) The functor $F : {}_A\mathcal{M}^H \to {}_{A\#H^*}\mathcal{M}$, $F(M) = Hom_{H^*}(H^{*rat}, M)$ is a right adjoint of the radical functor $t : {}_{A\#H^*}\mathcal{M} \to {}_A\mathcal{M}^H$, $t(N) = H^{*rat}N$.
Solution: i) We first show that $(a\#h^*)f$ is a morphism of H^*-modules. Indeed

$$l^*((a\#h^*)f)(v^*) = \sum l^*(a_0 f((v^* \leftharpoonup a_1)h^*))$$

$$\begin{aligned}
&= \sum l^*(a_1 f((v^* \leftharpoondown a_2)h^*)_1)a_0 f((v^* \leftharpoondown a_2)h^*)_0 \\
&= \sum l^*(a_1((v^* \leftharpoondown a_2)h^*)_1)a_0 f((v^* \leftharpoondown a_2)h^*)_0) \\
&\quad \text{(since } f \text{ is a morphism of right } H\text{-comodules)} \\
&= \sum l^*(a_1(v^* \leftharpoondown a_2)_1)a_0 f((v^* \leftharpoondown a_2)_0 h^*) \\
&\quad \text{(by Exercise 6.5.14}(i)) \\
&= \sum l^*(a_1 S(a_2) \rightharpoonup v_1^*)a_0 f((v_0^* \leftharpoondown a_3)h^*) \\
&\quad \text{(by Exercise 6.5.14}(ii)) \\
&= \sum l^*(v_1^*)a_0 f((v_0^* \leftharpoondown a_1)h^*) \\
&= \sum a_0 f(((l^*v^*) \leftharpoondown a_1)h^*) \\
&= ((a\#h^*)f)(l^*v^*)
\end{aligned}$$

To see that the action defines a left $A\#H^*$-module, we have

$$\begin{aligned}
((a\#h^*)(b\#l^*)f))(v^*) &= \sum a_0((b\#l^*)f)((v^* \leftharpoondown a_1)h^*) \\
&= \sum a_0 b_0 f((((v^* \leftharpoondown a_1)h^*) \leftharpoondown b_1)l^*) \\
&= \sum a_0 b_0 f((v^* \leftharpoondown a_1 b_1)(h^* \leftharpoondown b_2)l^*) \\
&= \sum ((ab_0\#(h^* \leftharpoondown b_1)l^*)f)(v^*) \\
&= (((a\#h^*)(b\#l^*))f)(v^*)
\end{aligned}$$

Now, if $f \in Hom_{H^*}(H^{*rat}, M)$, we have

$$\begin{aligned}
\overline{\varphi}((a\#h^*)f))(v^*) &= \varphi(((a\#h^*)f)(v^*)) \\
&= \sum \varphi(a_0 f((v^* \leftharpoondown a_1)h^*)) \\
&= \sum a_0 \varphi(f((v^* \leftharpoondown a_1)h^*)) \\
&= ((a\#h^*)\overline{\varphi}(f))(v^*)
\end{aligned}$$

ii) The structure defined in i) defines a functor

$$F : {}_A\mathcal{M}^H \to {}_{A\#H^*}\mathcal{M}, \; F(M) = Hom_{H^*}(H^{*rat}, M)$$

Let $N \in {}_{A\#H^*}\mathcal{M}$. Then the map

$$\gamma_N : N \to F((t(N)) = Hom_{H^*}(H^{*rat}, t(N)),$$

$\gamma_N(n)(v^*) = v^*n$, is a morphism of $A\#H^*$-modules. Indeed, we have that

$$\gamma_N((a\#h^*)n)(v^*) = (1\#v^*)(a\#h^*)n = \sum (a_0\#(v^* \leftharpoondown a_1)h^*)n$$

and

$$\begin{aligned}((a\#h^*)\gamma_N(n))(v^*) &= \sum a_0\gamma_N(n)((v^* \leftharpoonup a_1)h^*)\\ &= \sum a_0((v^* \leftharpoonup a_1)h^*n)\\ &= \sum (a_0\#(v^* \leftharpoonup a_1)h^*)n\end{aligned}$$

Let now $M \in {}_A\mathcal{M}^H$. Then the map $\delta_M : t(F(M)) \to M$, $\delta_M(v^*f) = f(v^*)$ for any $v^* \in H^{*rat}$, $f \in F(M) = Hom_{H^*}(H^{*rat}, M)$, is an isomorphism in the category ${}_A\mathcal{M}^H$.
Indeed, we first show that δ_M is well defined. Let $\sum_i v_i^* f_i = \sum_j v_j^* g_j \in t(F(M)) = H^*Hom_{H^*}(H^{*rat}, M)$, with $v_i^*, u_j^* \in H^*, f_i, g_j \in F(M)$. Since $v_i^*, u_j^* \in H^{*rat}$, there exits $l^* \in H^{*rat}$ such that $l^*v_i^* = v_i^*$ for any i and $l^*u_j^* = u_j^*$ for any j (it is enough to take some l^* such that l^* acts as ε_H on all $(v_i^*)_1$ and $(u_j^*)_1$; this is possible since H^{*rat} is dense in H^*). Then

$$\begin{aligned}\sum_i f_i(v_i^*) &= \sum_i f_i(l^*v_i^*)\\ &= \sum_i (v_i^* f_i)(l^*)\\ &= \sum_j (u_j^* g_j)(l^*)\\ &= \sum_j g_j(l^*u_j^*)\\ &= \sum_j g_j(u_j^*)\end{aligned}$$

thus the definition of δ_M is correct.
Since $\delta_M(h^*(v^*f)) = \delta_M(h^*v^*f) = f(h^*v^*) = h^*f(v^*) = h^*\delta_M(v^*f)$, δ_M is a morphism of H^*-modules, thus a morphism of H-comodules.
Finally, we prove that δ_M is a morphism of A-modules. Let $v^* \in H^{*rat}$, $f \in Hom_{H^*}(H^{*rat}, M)$, and $a \in A$. We want $\delta_M(a(v^*f)) = a\delta_M(v^*f)$. Since $a(v^*f) \in H^{*rat}Hom_{H^*}(H^{*rat}, M)$, there exists $w^* \in H^{*rat}$ and $g \in Hom_{H^*}(H^{*rat}, M)$, such that $a(v^*f) = w^*g$. This means that $\sum a_0 f((d^* \leftharpoonup a_1)v^*) = g(l^*w^*)$ for any $l^* \in H^{*rat}$. Then $\delta_M(a(v^*f)) = \delta_M(w^*g) = g(w^*)$, and $a\delta_M(v^*f) = af(v^*)$. We know that $H^{*rat} = \oplus_{p\in P}E(N_p)^*$, thus there exists a finite subset P_0 of P such that $v^* \in \oplus_{p\in P_0}E(N_p)^*$. Denoting by $E(N_p)_1$ the space spanned by all the h_1's with $h \in E(N_p)$, and $\Delta(h) = \sum h_1 \otimes h_2$, all the spaces $a_1 \rightharpoonup E(N_p)_1$, $p \in P_0$, are finite dimensional, thus there exits a finite subset $J \in P$ such that $a_1 \rightharpoonup E(N_p)$, are contained in $\oplus_{p\in J}N_p$, and all $w_1^* \in \oplus_{p\in J}N_p$.

Take $l^* \in H^{*rat}$, which is ε_H on any $E(N_p)$, $p \in J$. Then for $h \in E(N_p), p \notin P_0$ and any a_1 we have $((l^* \leftharpoonup a_1)v^*)(h) = \sum l^*(a_1 \rightharpoonup h_1)v^*(h_2) = 0$ (since $v^*(h_2) \in v^*(E(N_p)) = 0$) and for any $h \in E(N_p)$, $p \in P_0$ and any a_1,

$$\begin{aligned} ((l^* \leftharpoonup a_1)v^*)(h) &= \sum l^*(a_1 \rightharpoonup h_1)v^*(h_2) \\ &= \sum \varepsilon_H(a_1 \rightharpoonup h_1)v^*(h_2) \\ &= \varepsilon_H(a_1)v^*(h) \end{aligned}$$

Therefore $(l^* \leftharpoonup a_1)v^* = \varepsilon_H(a_1)v^*$ for any a_1, and $\sum a_0 f((l^* \leftharpoonup a_1)v^*) = \sum a_0 f(\varepsilon_H(a_1)v^*) = af(v^*)$. On the other hand

$$l^*w^* = \sum l^*(w_1^*)w_0^* = \sum \varepsilon_H(w_1^*)w_0^* = w^*$$

thus

$$\begin{aligned} a\delta_M(v^*f) &= af(v^*) \\ &= \sum a_0 f((l^* \leftharpoonup a_1)v^*) \\ &= g(l^*w^*) \\ &= g(w^*) \\ &= \delta_M(w^*g) \\ &= \delta_M(a(v^*f)) \end{aligned}$$

We show that δ_M is injective. Indeed, let $\sum_i v_i^* f_i \in t(F(M))$ such that $\delta_M(\sum_i v_i^* f_i) = 0$. Then for any $v^* \in H^{*rat}$ we have

$$(\sum_i v_i^* f_i)(v^*) = \sum_i f_i(v^* v_i^*) = \sum_i v^* f_i(v_i^*) = v^*\delta_M(\sum_i v_i^* f_i) = 0$$

thus $\sum_i v_i^* f_i = 0$. To show that δ_M is surjective, let $m \in M$, choose some $l^* \in C^{*rat}$ such that $l^*m = m$, and let $f \in Hom_{H^*}(H^{*rat}, M)$ defined by $f(h^*) = h^*m$ for any $h^* \in H^{*rat}$. Then clearly $m = l^*m = f(l^*) = \delta_M(l^*f)$, which proves that $delta_M$ is an isomorphism.
Now for $N \in {}_{A\#H^*}\mathcal{M}$ and $M \in {}_A\mathcal{M}^H$, we define the maps

$$\alpha : Hom_A^H(t(N), M) \to Hom_{A\#H^*}(N, Hom_{H^*}(H^{*rat}, M))$$

and

$$\beta : Hom_{A\#H^*}(N, Hom_{H^*}(H^{*rat}, M)) \to Hom_A^H(t(N), M)$$

by $\alpha(p) = Hom_{H^*}(H^{*rat}, p)\gamma_N$ for $p \in Hom_A^H(t(N), M)$, and $\beta(q) = \delta_M q$ for $q \in Hom_{A\#H^*}(N, Hom_{H^*}(H^{*rat}, M))$. Thus

$$\alpha(p)(n)(v^*) = p(\gamma_N(n)(v^*)) = p(v^*n)$$

for any $n \in N, v^* \in H^{*rat}$, and

$$\beta(q)(v^*n) = (\delta_M q)(v^*n) = \delta_M(v^*q(n)) = q(n)(v^*)$$

We have that

$$(\beta\alpha)(p)(v^*n) = \beta(\alpha(p))(v^*n) = \alpha(p)(n)(v^*) = p(v^*n)$$

and

$$(\alpha\beta)(q)(n)(v^*) = \alpha(\beta(q))(n)(v^*) = \beta(q)(v^*n) = q(n)(v^*)$$

showing that α and β are inverse to each other, and this ends the proof.

Exercise 6.5.16 *Let H be a co-Frobenius Hopf algebra, and A a right H-comodule algebra. Then the following assertions hold:*
i) Let $M \in {}_A\mathcal{M}^H$. Then the map

$$\gamma_M : M \to Hom_{H^*}(H^{*rat}, M),$$

$\gamma_M(m)(v^*) = v^*m = \sum v^*(m_1)m_0$ *for any* $m \in M, v^* \in H^{*rat}$, *is an injective morphism of* $A\#H^*$*-modules.*
ii) If $M \in {}_A\mathbf{M}^H$ has finite support, then γ_M is an isomorphism of $A\#H^*$-modules.

Solution: i) We already know from the solution of Exercise 6.5.15 that γ_M is a morphism of modules. The fact that it is injective follows from the density of H^{*rat} in H^*.
ii) Let $\rho_M(M) \subseteq M \otimes X$ with X a finite dimensional subspace of H, and K be a finite subset of J such that $X \subseteq \oplus_{t\in K} E(M_t)$. If $\varepsilon_j \in C^*$ is ε on $E(M_j)$ and zero on any $E(M_t)$, $t \neq j$, then obviously $\varepsilon_j(X) = 0$ for $j \notin K$, thus $\varepsilon_j M = 0$. Let $\varphi \in Hom_{H^*}(H^{*rat}, M)$, and $j \notin K$. We have $\varphi(\varepsilon_j) = \varphi(\varepsilon_j^2) = \varepsilon_j\varphi(\varepsilon_j) \in \varepsilon_j M = 0$. Thus $\varphi(\oplus_{j\notin K} C^*\varepsilon_j) = 0$.
Let $m = \sum_{t\in K} \varphi(\varepsilon_t)$. Then for $j \notin K$, $\gamma_M(m)(\varepsilon_j) = \varepsilon_j m = 0 = \varphi(\varepsilon_j)$, and for $j \in K$, $\gamma_M(m)(\varepsilon_j) = \varepsilon_j m = \sum_{t\in K} \varepsilon_j\varphi(\varepsilon_t) = \varphi(\varepsilon_j)$, showing that $\gamma_M(m) = \varphi$. Therefore γ_M is surjective.

Exercise 6.5.17 *Let H be a co-Frobenius Hopf algebra, and A an H-comodule algebra. If $M \in {}_A\mathcal{M}^H$ is an injective object with finite support, then M is injective as an A-module.*

Solution: Since the functor F from Exercise 6.5.15 has an exact left adjoint, we have that $F(M)$ is an injective $A\#H^*$-module. Exercise 6.5.16 shows that $F(M) \cong M$, thus M is an injective $A\#H^*$-module. On the other hand the restriction of scalars, Res, from ${}_{A\#H^*}\mathcal{M}$ to ${}_A\mathcal{M}$ has a left adjoint $A\#H^* \otimes_A - : {}_A\mathcal{M} \to {}_{A\#H^*}\mathcal{M}$, and this is exact, since $A\#H^*$ is a free right A-module. Thus Res takes injective objects to injective objects. In particular M is injective as an A-module.

Bibliographical notes

The main source of inspiration was S. Montgomery [149]. Lemma 6.1.3 and Proposition 6.1.4 belong to M. Cohen [58, 59]. Crossed products and their relation to Galois extensions were studied by R. Blattner, M. Cohen, S. Montgomery, [37], and Y. Doi, M. Takeuchi [78]. The last cited paper contains Theorem 6.4.12. The second condition in point b) is called the normal basis condition (an explanation of the name may be found in [149, p.128]), and the map γ in the proof is called a cleft map. The presentation of the Morita context is a shortened version of the one given in M. Beattie, S. Dăscălescu, Ş. Raianu, [29], extending the construction given by Cai and Chen in [42], [54] for the cosemisimple case. This extends the construction from the finite dimensional case due to M. Cohen, D. Fischman and S. Montgomery, [61], and M. Cohen, D. Fischman [62] for the semisimple case. This last paper contains the Maschke theorem for smash products. The Maschke theorem for crossed products belongs to R. Blattner and S. Montgomery [36]. The definition of Galois extensions appears for the first time in this form in Kreimer and Takeuchi [110] (see [149, p.123] or [150]). Corollary 6.4.7 belongs to C. Menini and M. Zuccoli [143]. Theorem 6.5.4 belongs to Ulbrich [233], as well as the characterization of strongly graded rings as Hopf-Galois extensions [234]. Conditions when the induction functor is an equivalence (the so-called Strong Structure Theorem) were given by H.-J. Schneider (see [203] and [202]). The duality theorems for co-Frobenius Hopf algebras belong to Van Daele and Zhang [237], and the proof was taken from [144]. Exercices 6.5.13-6.5.17 are from [68].

Chapter 7

Finite dimensional Hopf algebras

7.1 The order of the antipode

Throughout H is a finite dimensional Hopf algebra. We recall the following actions (module structures):

1) H^* is a left H-module via $(h \rightharpoonup h^*)(g) = h^*(gh)$ for $h, g \in H, h^* \in H^*$.

2) H^* is a right H-module via $(h^* \leftharpoonup h)(g) = h^*(hg)$ for $h, g \in H, h^* \in H^*$.

3) H is a left H^*-module via $h^* \rightharpoonup h = \sum h^*(h_2)h_1$ for $h^* \in H^*, h \in H$.

4) H is a right H^*-module via $h \leftharpoonup h^* = \sum h^*(h_1)h_2$ for $h^* \in H^*, h \in H$.

As in Chapter 5, if $g \in H$ is a grouplike element, we denote by

$$L_g = \{m \in H^* | h^*m = h^*(g)m \text{ for any } h^* \in H^* \}$$

and

$$R_g = \{n \in H^* | nh^* = h^*(g)n \text{ for any } h^* \in H^* \},$$

which are ideals of H^*, $L_1 = \int_l, R_1 = \int_r$. Also recall from Proposition 5.5.3 that L_g and R_g are 1-dimensional, and there exists a grouplike element (called the distinguished grouplike) a such that $R_a = L_1$.

We can perform the same constructions on the dual algebra H^*. More precisely, for any $\eta \in G(H^*) = Alg(H, k)$ we can define

$$L_\eta = \{ x \in H \mid hx = \eta(h)x \text{ for any } h \in H \}$$

$$R_\eta = \{ y \in H \mid yh = \eta(h)y \text{ for any } h \in H \}$$

We remark that if we keep the same definition we gave for L_g ($g \in H$), then L_η should be a subspace of H^{**}. The set L_η, as defined above, is just the preimage of this subspace via the canonical isomorphism $\theta : H \to H^{**}$. From the above it follows that the subspaces L_η and R_η are ideals of dimension 1 in H, and there exists $\alpha \in G(H^*)$ such that $R_\alpha = L_\varepsilon$. This element α is the distinguished grouplike element in H^*.

Remark 7.1.1 *Using Remark 5.5.11 and Exercise 5.5.10, we see that if H is semisimple and cosemisimple, then the distinguished grouplikes in H and H^* are equal to 1 and ε, respectively.* ∎

Lemma 7.1.2 *Let $\eta \in G(H^*)$, $g \in G(H)$, $m, n \in H^*$ and $x \in L_\eta$ such that $m \rightharpoonup x = g = x \leftharpoonup n$. Then $m \in L_g$ and $n \in R_g$.*

Proof: Let $h^*, g^* \in H^*$. Then

$$\begin{aligned}(g^*h^*m)(x) &= \sum (g^*h^*)(x_1 m(x_2)) \\ &= (g^*h^*)(g) \\ &= g^*(g)h^*(g) \\ &= \sum g^*(m(x_2)x_1)h^*(g) \\ &= (g^*h^*(g)m)(x)\end{aligned}$$

which shows that $(g^*(h^*m - h^*(g)m))(x) = 0$, so $(h^*m - h^*(g)m)(x \leftharpoonup H^*) = 0$.
But $x \leftharpoonup A^* = A$, since $L_\eta \leftharpoonup \eta = L_\varepsilon$ by the remarks preceding Proposition 5.5.4, and $L_\varepsilon \leftharpoonup H^* = H$ by Theorem 5.2.3 (applied for the dual of H^{op}). This shows that $h^*m = h^*(g)m$, and so $m \in L_g$. The fact that $n \in R_g$ is proved in a similar way. ∎

Corollary 7.1.3 *If $m \in H^*$, $x \in L_\varepsilon$, and $m \rightharpoonup x = 1$, then $m \in L_1$ and $x \leftharpoonup m = a$.*

Proof: Lemma 7.1.2 shows that $m \in L_1$. If $h^* \in H^*$, then

$$\begin{aligned}h^*(x \leftharpoonup m) &= \sum h^*(x_2)m(x_1) \\ &= (mh^*)(x) \\ &= h^*(a)m(x) \quad (\text{since } m \in L_1 = R_a) \\ &= h^*(m(x)a)\end{aligned}$$

Applying ε to the relation $\sum m(x_2)x_1 = 1$ we get $m(x) = 1$. This shows that $x \leftharpoonup m = a$. ∎

Lemma 7.1.4 *Let $x \in L_\eta$, $g \in G(H)$, $m \in H^*$ such that $m \rightharpoonup x = g$. Then for any $h^* \in H^*$ we have*

$$\eta(g)h^*(1) = \sum h^*(x_1)m(gx_2)$$

Proof: We compute

$$\begin{aligned}
\eta(g)h^*(1) &= \sum \eta(g)h_1^*(g^{-1})h_2^*(g) \quad (\Delta(h^*) = \sum h_1^* \otimes h_2^*)\\
&= h_1^*(g^{-1})h_2^*(m(x_2)x_1\eta(g)) \quad (g = m \to x)\\
&= \sum h_1^*(g^{-1})h_2^*(m(gx_2)gx_1) \quad (\eta(g)x = gx)\\
&= \sum h^*(g^{-1}gx_1)m(gx_2) \quad \text{(convolution)}\\
&= \sum h^*(x_1)m(gx_2)
\end{aligned}$$

∎

Lemma 7.1.5 *Let $g \in G(H)$, $\eta \in G(H^*)$, $x \in L_\eta$, and $m \in H^*$ such that $m \rightharpoonup x = g$. Then for any $h \in H$ we have*

$$S(g^{-1}(\eta \rightharpoonup h)) = (m \leftharpoonup h) \rightharpoonup x$$

Proof: Let $h^* \in H^*$. Then

$$\begin{aligned}
&h^*(S(g^{-1}(\eta \to h))) =\\
&= \sum h^*(S(h_1)g)\eta(h_2)\\
&= \sum \eta(g)h^*(S(h_1)g)\eta(g^{-1}h_2) \quad (\eta \text{ algebra map})\\
&= \eta(g)((h^*S)\eta)(g^{-1}h) \quad \text{(convolution)}\\
&= \sum((h_1^*S)\eta)(g^{-1}h)\eta(g)h_2^*(1)\\
&\qquad \text{(counit property for } h^*)\\
&= \sum((h_1^*S)\eta)(g^{-1}h)h_2^*(m(gx_2)x_1)\\
&\qquad \text{(by Lemma 7.1.4 for } h_2^*)\\
&= \sum(h_1^*S)(g^{-1}h_1)\eta(g^{-1}h_2)h_2^*(m(gx_2)x_1) \quad \text{(convolution)}\\
&= \sum h_1^*(S(h_1)g)h_2^*(m(gg^{-1}h_3x_2)g^{-1}h_2x_1)\\
&\qquad \text{(since } \eta(g^{-1}h_2x = g^{-1}h_2x)\\
&= \sum h^*(S(h_1)gg^{-1}h_2x_1m(h_3x_2))\\
&= \sum h^*(x_1m(hx_2))\\
&= h^*((m \leftharpoonup h) \rightharpoonup x)
\end{aligned}$$

∎

If we write the formula from Lemma 7.1.5 for the Hopf algebras H, H^{cop}, $H^{op,cop}$ and H^{op}, we get that for any $h \in H$ the following relations hold:

$$\text{If } x \in L_\eta, m \rightharpoonup x = g, \text{ then } S(g^{-1}(\eta \rightharpoonup h)) = (m \leftharpoonup h) \rightharpoonup x \tag{7.1}$$

$$\text{If } x \in R_\eta, m \rightharpoonup x = g, \text{ then } S^{-1}((\eta \rightharpoonup h)g^{-1}) = (h \rightharpoonup m) \rightharpoonup x \tag{7.2}$$

$$\text{If } x \in R_\eta, x \leftharpoonup n = g, \text{ then } S((h \leftharpoonup \eta)g^{-1}) = x \leftharpoonup (h \rightharpoonup n) \tag{7.3}$$

$$\text{If } x \in L_\eta, x \leftharpoonup n = g, \text{ then } S^{-1}(g^{-1}(h \leftharpoonup \eta)) = x \leftharpoonup (n \leftharpoonup h) \tag{7.4}$$

In particular

$$\text{If } x \in L_\varepsilon, m \rightharpoonup x = 1, \text{ then } S(h) = (m \leftharpoonup h) \rightharpoonup x \tag{7.5}$$

$$\text{If } x \in R_\alpha = L_\varepsilon, m \rightharpoonup x = 1, \text{ then } S^{-1}(\alpha \rightharpoonup h) = (h \rightharpoonup m) \rightharpoonup x \tag{7.6}$$

$$\text{If } x \in R_\alpha = L_\varepsilon, x \leftharpoonup n = a, \text{ then } S((h \leftharpoonup \alpha)a^{-1}) = x \leftharpoonup (h \rightharpoonup n) \tag{7.7}$$

$$\text{If } x \in L_\varepsilon, x \leftharpoonup n = g, \text{ then } S^{-1}(g^{-1}h) = x \leftharpoonup (n \leftharpoonup h) \tag{7.8}$$

Theorem 7.1.6 *For any $h \in H$ we have*

$$S^4(h) = a^{-1}(\alpha \rightharpoonup h \leftharpoonup \alpha^{-1})a$$

Proof: Let $x \in L_\varepsilon = R_\alpha$, and $m \in H^*$ with $m \rightarrow x = 1$. Corollary 7.1.3 shows that $m \in L_1$ and $x \leftarrow m = a$. Moreover, we have

$$\begin{aligned}
(S^4(h) \rightharpoonup m) \rightharpoonup x &= S^{-1}(\alpha \rightharpoonup S^4(h)) \quad \text{(by (7.6))}\\
&= S^{-1}(S^4(\alpha \rightharpoonup h))\\
&= S(S^2(\alpha \rightharpoonup h))\\
&= (m \leftharpoonup S^2(\alpha \rightharpoonup h)) \rightharpoonup x \quad \text{(by (7.5))}
\end{aligned}$$

Since the map from H^* to H, sending $h^* \in H^*$ to $h^* \rightharpoonup x \in H$ is bijective, we obtain

$$S^4(h) \rightharpoonup m = m \leftharpoonup S^2(\alpha \rightharpoonup h)$$

On the other hand,

$$\begin{aligned}
& x \leftharpoonup (m \leftharpoonup S^2(\alpha \rightharpoonup h)) =\\
=\ & S^{-1}(a^{-1}S^2(\alpha \rightharpoonup h)) \quad \text{(by (7.8))}\\
=\ & S^{-1}(S^2(a^{-1}(\alpha \rightharpoonup h)))\\
=\ & S(a^{-1}(\alpha \rightharpoonup h))\\
=\ & S(a^{-1}(\alpha \rightharpoonup h)aa^{-1})\\
=\ & S(((a^{-1}(\alpha \rightharpoonup h \leftharpoonup \alpha^{-1})a) \leftharpoonup \alpha)a^{-1})\\
& \qquad \text{(since } a \leftharpoonup \alpha = \alpha(a)a)\\
=\ & x \leftharpoonup ((a^{-1}(\alpha \rightharpoonup h \leftharpoonup \alpha^{-1})a) \rightharpoonup m) \quad \text{(by (7.7))}
\end{aligned}$$

Since the map $h^* \mapsto x \leftharpoonup h^*$ from H^* to H is bijective, we obtain that

$$m \leftharpoonup S^2(\alpha \rightharpoonup h) = (a^{-1}(\alpha \rightharpoonup h \leftharpoonup \alpha^{-1})a) \rightharpoonup m$$

We got that $S^4(h) \rightharpoonup m = (a^{-1}(\alpha \rightharpoonup h \leftharpoonup \alpha^{-1})a) \rightharpoonup m$, and then the formula follows from the bijectivity of the map $h \mapsto h \rightharpoonup m$ from H to H^*. ∎

Theorem 7.1.7 *(Radford) Let H be a finite dimensional Hopf algebra. Then the antipode S has finite order.*

Proof: Using the formula from Theorem 7.1.6 we obtain by induction that

$$S^{4n}(h) = a^{-n}(\alpha^n \rightharpoonup h \leftharpoonup \alpha^{-n})a^n$$

for any positive integer n. Since $G(H)$ and $G(H^*)$ are finite groups, their elements have finite orders, so there exists p for which $a^p = 1$ and $\alpha^p = \varepsilon$. Then it follows that $S^{4p} = Id$. ∎

Remark 7.1.8 *The proof of the preceding theorem not only shows that the order of antipode is finite, but also provides a hint on how to estimate the order.* ∎

7.2 The Nichols-Zoeller Theorem

In this section we prove a fundamental result about finite dimensional Hopf algebras, which extends to finite dimensional Hopf algebras the well known Lagrange Theorem for groups. Everywhere in this section H will be a finite dimensional Hopf algebra and B a Hopf subalgebra of H. If M and N are left H-modules, then $M \otimes N$ has a left H-module structure (via the comultiplication of H) given by $h(x \otimes y) = \sum h_1 x \otimes h_2 y$ for any $h \in H, x \in M, y \in N$. Hence $M \otimes N$ is a left B-module by restricting the scalars. Any tensor product of H-modules will be regarded as an H-module (and by restricting scalars as a B-module) in this way unless otherwise specified.

Proposition 7.2.1 *If $M \in {}_B^H\mathcal{M}$, then $H \otimes M \simeq M^{(\dim(H))}$ as left B-modules.*

Proof: Let $U = H \otimes M$ regarded as a B-module as above, and $V = H \otimes M$ with the left B-module structure given by $b(h \otimes m) = h \otimes bm$ for any $b \in B, h \in H, m \in M$. Since B acts only on the second tensor position of

V, we have $V \simeq M^{(\dim(H))}$ as left B-modules. We show that the B-modules U and V are isomorphic. Indeed, let $f : V \to U$ and $g : U \to V$ by

$$f(h \otimes m) = \sum m_{(-1)}h \otimes m_{(0)}$$

$$g(h \otimes m) = \sum S^{(-1)}(m_{(-1)})h \otimes m_{(0)}$$

for any $h \in H, m \in M$, where we denote as usual by $m \mapsto \sum m_{(-1)} \otimes m_{(0)}$ the left H-comodule structure of M. We have that

$$\begin{aligned} gf(h \otimes m) &= \sum g(m_{(-1)}h \otimes m_{(0)}) \\ &= \sum S^{(-1)}(m_{(-1)})m_{(-2)}h \otimes m_{(0)} \\ &= \sum \varepsilon(m_{(-1)})h \otimes m_{(0)} \\ &= h \otimes m \end{aligned}$$

and

$$\begin{aligned} fg(h \otimes m) &= f(\sum S^{(-1)}(m_{(-1)})h \otimes m_{(0)}) \\ &= \sum m_{(-1)}S^{(-1)}(m_{(-2)})h \otimes m_{(0)} \\ &= \sum \varepsilon(m_{(-1)})h \otimes m_{(0)} \\ &= h \otimes m \end{aligned}$$

showing that f and g are inverse each other. On the other hand

$$\begin{aligned} f(b(h \otimes m)) &= f(h \otimes bm) \\ &= \sum (bm)_{(-1)}h \otimes (bm)_{(0)} \\ &= \sum b_1 m_{(-1)}h \otimes b_2 m_{(0)} \\ &= \sum b(m_{(-1)}h \otimes m_{(0)}) \\ &= bf(h \otimes m) \end{aligned}$$

so f and g provide an isomorphism of B-modules. ∎

Proposition 7.2.2 *Let W be a left B-module. Then $B \otimes W \simeq W \otimes B \simeq B^{(\dim(W))}$ as left B-modules.*

Proof: We know that $B \otimes W$ is a left B-module. It is also a left B-comodule with the comodule strcture given by the association $b \otimes w \mapsto \sum b_1 \otimes b_2 \otimes w$. In this way $B \otimes W$ becomes a left B-Hopf module and the fundamental theorem of Hopf modules (a left hand side version) tells us that $B \otimes W \simeq B^{(\dim(W))}$.

Let us consider now the Hopf algebra B^{cop}, with the same multiplication as B and with comultiplication given by $c \mapsto \sum c_{(1)} \otimes c_{(2)} = \sum c_2 \otimes c_1$. In particular W is a left B^{cop}-module, so applying the isomorphism proved above we obtain that $B^{cop} \otimes W \simeq (B^{cop})^{(\dim(W))}$ as left B^{cop}-modules. The left B^{cop}-module structure of $B^{cop} \otimes W$ is given by $b(c \otimes w) = \sum b_{(1)}c \otimes b_{(2)}w = \sum b_2 c \otimes b_1 w$, therefore since $B = B^{cop}$ as algebras, we see that $B^{cop} \otimes W$ is isomorphic to $W \otimes B$ as left B-modules (the isomorphism is the twist map), so $W \otimes B \simeq (B^{cop})^{(\dim(W))} = B^{(\dim(W))}$. ∎

Lemma 7.2.3 *Let A be a finite dimensional k-algebra and M a finitely generated left A-module. Then M is A-faithful if and only if A embeds in $M^{(n)}$ as an A-module for some positive integer n.*

Proof: If A embeds in $M^{(n)}$ as an A-module for some positive integer n, then $ann_A(M) = ann_A(M^{(n)}) \subseteq ann_A(A) = 0$, so M is A-faithful. Conversely, if M is A-faithful, let $\{m_1, \dots, m_n\}$ be a basis of the k-vector space M. Then the map $f : A \to M^{(n)}$ defined by $f(a) = (am_1, \dots, am_n)$ for any $a \in A$ is an A-module morphism with $Ker(f) = \bigcap_{i=1,n} ann_A(m_i) = ann_A(M) = 0$. ∎

Corollary 7.2.4 *Let A be a finite dimensional k-algebra which is injective as a left A-module, and let $P_1, \dots, P_t$ be the isomorphism types of principal indecomposable left A-modules. If M is a finitely generated left A-module, then M is A-faithful if and only if each P_i is isomorphic to a direct summand of the A-module M.*

Proof: Lemma 7.2.3 tells that M is A-faithful if and only if A embeds in $M^{(n)}$ for some positive integer n. Since A is selfinjective, this is equivalent to the fact that $M^{(n)} \simeq A \oplus X$ for some positive integer n and some A-module X. Decomposing both sides as direct sums of indecomposables, the Krull-Schmidt theorem shows that this is equivalent to the fact that M contains a direct summand isomorphic to P_i for any $i = 1, \dots, t$. ∎

Proposition 7.2.5 *Let A be a finite dimensional k-algebra such that A is injective as a left A-module. If W is a finitely generated left A-module, then there exists a positive integer r such that $W^{(r)} \simeq F \oplus E$ for a free A-module F and an A-module E which is not faithful.*

Proof: If W is not faithful we simply take $r = 1, F = 0$ and $E = W$. Assume now that W is A-faithful. Let $A \simeq P_1^{(n_1)} \oplus \dots \oplus P_t^{(n_t)}$, where $P_1, \dots, P_t$ are the isomorphism types of principal indecomposable A-modules. Corollary 7.2.4 shows that $W \simeq P_1^{(m_1)} \oplus \dots \oplus P_t^{(m_t)} \oplus Q$ for some $m_1, \dots, m_t > 0$ and some A-module Q such that any direct summand of Q is not isomorphic to any P_i. Let r be the least common multiple of the numbers $n_1, \ldots, n_t$. We have that

$$W^{(r)} \simeq P_1^{(rm_1)} \oplus \ldots \oplus P_t^{(rm_t)} \oplus Q^{(r)}$$

Let $\alpha = min(\frac{rm_1}{n_1}, \ldots, \frac{rm_t}{n_t})$, say $\alpha = \frac{rm_i}{n_i}$. Then

$$W^{(r)} \simeq A^{(\alpha)} \oplus P_1^{(rm_1 - \alpha n_1)} \oplus \ldots \oplus P_t^{(rm_t - \alpha n_t)} \oplus Q^{(r)}$$

This ends the proof if we denote $F = A^{(\alpha)}$, which is free, and $E = P_1^{(rm_1-\alpha n_1)} \oplus \ldots \oplus P_t^{(rm_t - \alpha n_t)} \oplus Q^{(r)}$, which is not faithful since it does not contain any direct summand isomorphic to P_i (note that $rm_i - \alpha n_i = 0$ and that we have used again the Krull-Schmidt theorem). ∎

Proposition 7.2.6 *Let W be a finitely generated left B-module such that $W^{(r)}$ is a free B-module for some positive integer r. Then W is a free B-module.*

Proof: Take $B = B_1 \oplus \ldots \oplus B_n$, a direct sum of indecomposable B-modules. If t is a nonzero left integral of B and $t = t_1 + \ldots + t_n$ is the representation of t in the above direct sum, we see that

$$\begin{aligned} bt_1 + \ldots + bt_n &= bt \\ &= \varepsilon(b)t_1 + \ldots + \varepsilon(b)t_n \\ &= \varepsilon(b)t \end{aligned}$$

for any $b \in B$, showing that $t_1, \ldots, t_n$ are left integrals of B. Since the space of left integrals has dimension 1, we have that there exists a unique j such that $t_j \neq 0$, and then $t = t_j$. Hence B_j is not isomorphic to any other B_i, $i \neq j$, since B_j contains a nonzero integral and B_i doesn't, and if $f : B_j \to B_i$ were an isomorphism of B-modules we would clearly have that $f(t)$ is a nonzero left integral.

Let us take now $P_1 = B_j, P_2, \ldots, P_s$ the isomorphism types of principal indecomposable B-modules, and $B \simeq P_1^{(n_1)} \oplus \ldots \oplus P_s^{(n_s)}$ the representation of B as a sum of such modules. Note that $n_1 = 1$. We know that $W^{(r)}$ is free as a B-module, say $W^{(r)} \simeq B^{(p)}$ for some positive integer p. Since

$$W^{(r)} \simeq B^{(p)} \simeq P_1^{(pn_1)} \oplus \ldots \oplus P_s^{(pn_s)}$$

the Krull-Schmidt theorem shows us that the decomposition of W as a sum of indecomposables is of the form $W \simeq P_1^{(m_1)} \oplus \ldots \oplus P_s^{(m_s)}$ for some $m_1, \ldots, m_s$. Moreover, since $W^{(r)} \simeq P_1^{(rm_1)} \oplus \ldots \oplus P_s^{(rm_s)}$, we must have $pn_i = rm_i$. In particular $p = rm_1$. Then for any i we have that $pn_i = rm_1 n_i = rm_i$, so $m_i = m_1 n_i$. We obtain that $W \simeq B^{(m_1)}$, a free B-module. ∎

Proposition 7.2.7 *Let W be a finitely generated left B-module such that there exists a faithful B-module L with $L \otimes W \simeq W^{(\dim(L))}$ as B-modules. Then W is a free B-module.*

Proof: We know from Exercise 5.3.5 that B is an injective left B-module. Then we can apply Proposition 7.2.5 and find that $W^{(r)} \simeq F \oplus E$ for some positive integer r, some free B-module F and some B-module E which is not faithful. Proposition 7.2.6 shows that it is enough to prove that $W^{(r)}$ is free. We have that

$$L \otimes W^{(r)} \simeq (L \otimes W)^{(r)} \simeq (W^{(\dim(L))})^{(r)} \simeq (W^{(r)})^{(\dim(L))}$$

so we can replace W by $W^{(r)}$, and thus assume that $W \simeq F \oplus E$. Similarly there exists a positive integer s such that $L^{(s)} \simeq F' \oplus E'$ with F' free and E' not faithful. Since L is faithful, $L^{(s)}$ is also faithful, so $F' \neq 0$. Since

$$L^{(s)} \otimes W \simeq (L \otimes W)^{(s)} \simeq (W^{(\dim(L))})^{(s)} \simeq W^{(\dim(L^{(s)}))}$$

and we can replace L by $L^{(s)}$. We have reduced to the case $L \simeq F' \oplus E'$. Denote $t = \dim(L)$. Since $L \otimes W \simeq W^{(t)}$, we obtain that

$$F^{(t)} \oplus E^{(t)} \simeq (L \otimes F) \oplus (L \otimes E) \tag{7.9}$$

Since F is free, say $F \simeq B^{(q)}$, we see that

$$\begin{aligned} L \otimes F &\simeq L \otimes B^{(q)} \\ &\simeq (L \otimes B)^{(q)} \\ &\simeq (B^{(\dim(L))})^{(q)} \quad \text{(by Proposition 7.2.2)} \\ &\simeq B^{(tq)} \\ &\simeq F^{(t)} \end{aligned}$$

Equation (7.9) and the Krull-Schmidt theorem imply now that $E^{(t)} \simeq L \otimes E$. If $E \neq 0$ we have that

$$E^{(t)} \simeq L \otimes E \simeq (F' \otimes E) \oplus (E' \otimes E)$$

Proposition 7.2.2 tells then that $F' \otimes E$ is nonzero and free, hence it is faithful, and then so is $E^{(t)}$, a contradiction. This shows that $E = 0$ and then W is free. ∎

Lemma 7.2.8 *If any finite dimensional $M \in {}_B^H\mathcal{M}$ is free as a B-module, then any object $M \in {}_B^H\mathcal{M}$ is free as a B-module.*

Proof: We first note that any nonzero $M \in {}_B^H\mathcal{M}$ contains a nonzero finite dimensional subobject in the category ${}_B^H\mathcal{M}$. Indeed, let N be a finite dimensional nonzero H-subcomodule of M (for example a simple H-subcomodule). Then BN is a finite dimensional subobject of M in the category ${}_B^H\mathcal{M}$. For a nonzero $M \in {}_B^H\mathcal{M}$ we define the set $\mathcal{F}$ consisting of all non-empty subsets X of M with the property that BX is a subobject of M in the category ${}_B^H\mathcal{M}$, and BX is a free B-module with basis X. By the first remark, $\mathcal{F}$ is non-empty. We order $\mathcal{F}$ by inclusion. If $(X_i)_{i\in I}$ is a totally ordered subset of $\mathcal{F}$, then clearly $X = \cup_{i\in I}X_i$ is a basis of the B-module BX, and $BX = \sum_{i\in I} BX_i$ is a subobject of M in ${}_B^H\mathcal{M}$, so $X \in \mathcal{F}$. Thus Zorn's Lemma applies and we find a maximal element $Y \in \mathcal{F}$. If $BY \neq M$, then M/BY is a nonzero object of ${}_B^H\mathcal{M}$, so it contains a nonzero subobject S/BY, where $BY \subseteq S \subseteq M$ and $S \in {}_B^H\mathcal{M}$. Let Z be a basis of S/BY and $Y' \subseteq S$ such that $\pi(Y') = Z$, where $\pi : S \to S/BY$ is the natural projection. Then S is a free B-module with basis $Y \cup Y'$, so $Y \cup Y' \in \mathcal{F}$, a contradiction with the maximality of Y. Therefore we must have $BY = M$, so M is a free B-module with basis Y. ∎

Theorem 7.2.9 *(Nichols-Zoeller Theorem) Let H be a finite dimensional Hopf algebra and B a Hopf subalgebra. Then any $M \in {}_B^H\mathcal{M}$ is free as a B-module. In particular H is a free left B-module and* $\dim(B)$ *divides* $\dim(H)$.

Proof: Lemma 7.2.8 shows that it is enough to prove the statement for finite dimensional $M \in {}_B^H\mathcal{M}$. Let M be such an object. Since H is finitely generated and faithful as a left B-module, and from Proposition 7.2.1 $H \otimes M \simeq M^{(\dim(H))}$ as B-modules, we obtain from Proposition 7.2.7 that M is a free B-module. The last part of the statement follows by taking $M = H$. ∎

Corollary 7.2.10 *If H is a finite dimensional Hopf algebra, then the order of $G(H)$ divides* $\dim(H)$. ∎

As an application we give the following result which will be a fundamental tool in classification results for Hopf algebras. If H is a Hopf algebra, we will denote by $H^+ = Ker(\varepsilon)$, which is an ideal of H. A Hopf subalgebra K of H is called normal if $K^+H = HK^+$.

Theorem 7.2.11 *Let A be a finite dimensional Hopf algebra, B a normal Hopf subalgebra of A, and A/B^+A the associated factor Hopf algebra. Then A is isomorphic as an algebra to a certain crossed product $B\#_\sigma A/B^+A$.*

Proof: We prove the assertion in a series of steps.
Step I. B^+A is a Hopf ideal of A.

It is clearly an ideal of A. Since $\varepsilon = (\varepsilon \otimes \varepsilon)\Delta$, if $b \in Ker(\varepsilon)$, then $\Delta(b) \in Ker(\varepsilon \otimes \varepsilon) = B^+ \otimes B + B \otimes B^+$, so B^+A is also a coideal. Finally, since $S(B^+) \subseteq B^+$, it follows that the antipode stabilizes B^+A.
Step II. A becomes a right H-comodule algebra via the canonical projection $\pi : A \to H = A/(B^+A)$, and $B = A^{coH}$.
The canonical inclusion $i : B \to A$ is a morphism of left B-modules, and since ${}_BB$ is injective (B is a finite dimensional Hopf algebra), i splits, i.e. there exists a left B-module map $\theta : A \to B$ with $\theta i = I_B$. Let

$$Q : A \longrightarrow A, \quad Q(a) = \sum S(a_1)i\theta(a_2).$$

We show that $Q(B^+A) = 0$. Indeed, if $b \in B$ and $a \in A$, then

$$\begin{aligned} Q(ba) &= \sum S(b_1a_1)i\theta(b_2a_2) \\ &= \sum S(a_1)S(b_1)b_2i\theta(a_2) \\ &= \varepsilon(b)\sum S(a_1)i\theta(a_2) = 0. \end{aligned}$$

It follows that there exists $\overline{Q} : H \to A$ a linear map such that $\overline{Q}\pi = Q$. Thus from $\sum a_1Q(a_2) = i\theta(a)$ we deduce that $\sum a_1\overline{Q}\pi(a_2) = i\theta(a)$. Let $a \in A^{coH}$, i.e. $\sum a_1 \otimes \pi(a_2) = a \otimes \pi(1)$. Then

$$\begin{aligned} i\theta(a) &= \sum a_1\overline{Q}\pi(a_2) \\ &= \sum M(I \otimes \overline{Q})(a_1 \otimes \pi(a_2)) \\ &= M(I \otimes \overline{Q})(a \otimes \pi(1)) \\ &= a\overline{Q}\pi(1) \\ &= aQ(1) = a, \end{aligned}$$

so $a = i\theta(a) \in B$. Conversely, if $b \in B$, then from $\sum b_1 \otimes b_2 = b \otimes 1 + \sum b_1 \otimes (b_2 - \varepsilon(b_2)1)$ we obtain that $\sum b_1 \otimes \pi(b_2) = b \otimes \pi(1)$, i.e. $b \in A^{coH}$.
Step III. The extension A/B is H-Galois.
Recall from Example 6.4.8 1) that the canonical Galois map

$$\beta : A \otimes A \longrightarrow A \otimes A, \quad \beta(a \otimes b) = \sum ab_1 \otimes b_2$$

is bijective with inverse $\beta^{-1}(a \otimes b) = \sum aS(b_1) \otimes b_2$. If M denotes the multiplication of A, then if we denote

$$K = (M \otimes I - I \otimes M)(A \otimes B \otimes A),$$

we have $\beta(K) = A \otimes B^+A$. Indeed, if $a, a' \in A$, $b \in B$, and $x = ab \otimes a' - a \otimes ba' \in K$, then

$$\begin{aligned}\beta(x) &= \sum (aba_1' \otimes a_2' - ab_1a_1' \otimes b_2a_2') \\ &= \sum (ab_1a_1' \otimes \varepsilon(b_2)a_2' - ab_1a_1' \otimes b_2a_2') \\ &= \sum (ab_1a_1' \otimes (\varepsilon(b_2)1 - b_2)a_2')\end{aligned}$$

which is in $A \otimes B^+A$, since $\varepsilon(b)1 - b \in B^+$ for all $b \in B$. Conversely, for $a, a' \in A$, $b \in B^+$, we have

$$\begin{aligned}&\beta^{-1}(a \otimes ba') = \\ =\ & \sum aS(b_1a_1') \otimes b_2a_2' \\ =\ & \sum aS(a_1')S(b_1) \otimes b_2a_2' \\ =\ & \sum (aS(a_1')S(b_1) \otimes b_2a_2' - aS(a_1') \otimes S(b_1)b_2a_2') \\ =\ & (M \otimes I - I \otimes M)(\sum aS(a_1') \otimes S(b_1) \otimes b_2a_2') \in K.\end{aligned}$$

Now β induces an isomorphism from $(A \otimes A)/K \simeq A \otimes_B A$ to $(A \otimes A)/(A \otimes B^+A) \simeq A \otimes H$, which is exactly the Galois map for the extension A/B.
Step IV. We have that $A \simeq B \otimes H$ as left B-modules and right H-comodules. Recall first the multiplication in the smash product $A\#H^*$:

$$(a\#h^*)(b\#g^*) = \sum ab_0\#(h^* \leftharpoondown b_1)g^*,$$

where $(h^* \leftharpoondown x)(y) = h^*(xy)$. It follows that $B \otimes H^*$ is a subring of $A\#H^*$. We know from Nichols-Zoeller that ${}_BA$ is free of finite rank. Applying the same to A^{op}, we get that ${}_{B^{op}}A^{op}$ is free, then using the algebra isomorphism $S : B^{op} \to B$ it follows that A_B^{op} is free, and thus A_B is free (with the same rank as ${}_BA$). Denote by l the rank of A_B. Since the extension A/B is Galois, the map

$$can : A \otimes_B A \longrightarrow A \otimes H, \quad can(a \otimes b) = \sum ab_0 \otimes b_1 \tag{7.10}$$

is an isomorphism of $A-B$-bimodules, and hence we have that $A_B^{(l)} \cong (B_B^{(l)} \otimes_B A)_B \cong (A \otimes_B A)_B \cong (A \otimes H)_B \cong A_B^{(n)}$. By Krull-Schmidt we get $l = n$, i.e. A_B is free of rank $n = dim_k(H)$.
By the above, we have that ${}_BA$ is also free and $rank({}_BA) = n$. Now, A has an element of trace 1. Indeed, if $t \in H^*$ is a left integral, and $h \in H$ is such that $t(h)1 = \pi(1) = \sum h_1t(h_2)$, then an element $a \in A$ with $\pi(a) = h$

is an element of trace 1:

$$\begin{aligned} t \cdot a &= \sum t(\pi(a_2))a_1 \\ &= \sum t(\pi(a_1))f(\pi(a_2)) \quad (f \text{ is a left inverse for } \pi) \\ &= \sum t(\pi(a)_1)f(\pi(a)_2) \\ &= \sum t(h_1)f(h_2) \\ &= f(\sum t(h_1)h_2) \\ &= f(\pi(1)) = 1. \end{aligned}$$

The extension A/B is also Galois, so the categories ${}_B\mathcal{M}$ and ${}_A\mathcal{M}^H$ are equivalent via the induced functor $A \otimes_B -$. If P_1, P_2,...,P_s are the only projective indecomposables in ${}_B\mathcal{M}$ it follows that $A\otimes_B P_1$, $A\otimes_B P_2$,...,$A\otimes_B P_s$ are the only projective indecomposables in ${}_A\mathcal{M}^H \simeq {}_{A\#H^*}\mathcal{M}$. Write

$$B \simeq P_1^{k_1} \oplus P_2^{k_2} \oplus \ldots P_s^{k_s}.$$

Now $A\#H^*$ is projective in ${}_A\mathcal{M}^H$ so

$$A\#H^* \simeq (A \otimes_B P_1)^{l_1} \oplus (A \otimes_B P_2)^{l_2} \oplus \ldots (A \otimes_B P_s)^{l_s} \tag{7.11}$$

in this category, and in particular as left A-modules. But $A\#H^* \simeq A^n$ as left A-modules, and again from this and from (7.11) we get as above that $l_i = nk_i$ and so

$$A\#H^* \simeq A^n \tag{7.12}$$

as left $A\#H^*$-modules, therefore as left $B \otimes H^*$-modules.
We have now that

$$A \otimes H^* \simeq A\#H^* \tag{7.13}$$

as left $B \otimes H^*$-modules, via

$$\phi : A \otimes H^* \longrightarrow A\#H^*, \;\; \phi(a \otimes h^*) = \sum a_0 \otimes h^* \leftharpoonup a_1.$$

Now it is clear that ϕ is bijective with inverse

$$\phi^{-1} : A\#H^* \longrightarrow A \otimes H^*, \;\; \phi^{-1}(a\#h^*) = \sum a_0 \otimes h^* \leftharpoonup S^{-1}(a_1),$$

and ϕ is left $B \otimes H^*$-linear because

$$\begin{aligned} \phi((b \otimes g^*)(a \otimes h^*)) &= \phi(ba \otimes g^*h^*) \\ &= \sum ba_0\#(g^*h^*) \leftharpoonup a_1 \\ &= \sum ba_0\#(g^* \leftharpoonup a_1)(h^* \leftharpoonup a_2) \\ &= (b \otimes g^*)(\sum a_0\#h^* \leftharpoonup a_1) = (b \otimes g^*)\phi(a \otimes h^*). \end{aligned}$$

Since ${}_BA$ is free of rank n, we get from (7.13) that

$$A\#H^* \simeq (B \otimes H^*)^n$$

as left $B \otimes H^*$-modules. Combining this with (7.12) we obtain that

$$A^n \simeq A\#H^* \simeq (B \otimes H^*)^n \tag{7.14}$$

as left $B \otimes H^*$-modules.
Since $B \otimes H^*$ is finite dimensional, we can write

$$B \otimes H^* \simeq P_1^{k_1} \oplus \ldots \oplus P_s^{k_s},$$

an indecomposable decomposition. Now ${}_{A\#H^*}A$ is projective, $A\#H^*$ is free over $B \otimes H^*$, so A is also projective as a left $B \otimes H^*$-module. Thus

$$A \simeq P_1^{t_1} \oplus \ldots \oplus P_s^{t_s}$$

as left $B \otimes H^*$-modules. By (7.14) we have now

$$P_1^{k_1 n} \oplus \ldots \oplus P_s^{k_s n} \simeq P_1^{t_1 n} \oplus \ldots \oplus P_s^{t_s n}$$

as left $B \otimes H^*$-modules, so by Krull-Schmidt we obtain that $k_i = t_i$, $i = 1, \ldots, s$, i.e. $A \simeq B \otimes H^*$ as left $B \otimes H^*$-modules. But $H^* \simeq H$ as left H^*-modules by Theorem 5.2.3, so $A \simeq B \otimes H$ as left B-modules and right H-comodules.
The result follows now from Theorem 6.4.12. ∎

7.3 Matrix subcoalgebras of Hopf algebras

We say that a k-coalgebra C is a matrix coalgebra if $C \simeq M^c(n, k)$ for some positive integer n. This is equivalent to the fact that C has a basis $(c_{ij})_{1 \leq i,j \leq n}$, with comultiplication Δ and counit ε defined by

$$\Delta(c_{ij}) = \sum_{1 \leq p \leq n} c_{ip} \otimes c_{pj}, \quad \varepsilon(c_{ij}) = \delta_{ij}$$

for any $1 \leq i, j \leq n$. A basis of C for which the comultiplication and the counit work as above is called a comatrix basis of C. Of course, a matrix coalgebra might have several comatrix bases. Let C be a matrix coalgebra, and we fix a comatrix basis $(c_{ij})_{1 \leq i,j \leq n}$ of C. We know (see Exercise 1.3.11) that $C^* \simeq M_n(k)$, the matrix algebra, where the matrix units of C^* are the elements $(E_{ij})_{1 \leq i,j \leq n} \subseteq C^*$ defined by $E_{ij}(c_{rs}) = \delta_{ir}\delta_{js}$. We identify C^* and $M_n(k)$, in particular we can consider the trace $Tr(c^*)$

of an element $c^* \in C^*$, which is the sum of the coefficients of all E_{ii}'s in the representation of c^* in the basis $(E_{ij})_{1\le i,j\le n}$ of C^*. We define a bilinear form $(\ |\ ) : C \times C \to k$ by $(c_{ij}|c_{rs}) = \delta_{is}\delta_{jr}$ for any $1 \le i,j,r,s \le n$. This form induces a linear morphism $\xi : C \to C^*$ by $\xi(c)(d) = (c|d)$ for any $c, d \in C$. We clearly have that $\xi(c_{ij}) = E_{ji}$ for any i,j, thus ξ is an isomorphism of vector spaces.

Lemma 7.3.1 *For any $c, d \in C$ we have that:*
(i) $(c|d) = Tr(\xi(c)\xi(d))$.
(ii) $\varepsilon(c) = \sum_{i=1,n}(c|c_{ii}) = Tr(\xi(c))$.

Proof: (i) It is enough to check the formula for elements of a basis of C, i.e. we have that

$$\begin{aligned}
Tr(\xi(c_{ij})\xi(c_{rs})) &= Tr(E_{ji}E_{sr}) \\
&= \delta_{is}Tr(E_{jr}) \\
&= \delta_{is}\delta_{jr} \\
&= (c_{ij}|c_{rs})
\end{aligned}$$

(ii) Again we check on elements of the basis. We have that $\varepsilon(c_{jr}) = \delta_{jr}$,

$$\begin{aligned}
\sum_{i=1,n}(c_{jr}|c_{ii}) &= \sum_{i=1,n}\delta_{ij}\delta_{ir} \\
&= \delta_{jr}
\end{aligned}$$

and $Tr(\xi(c_{jr})) = Tr(E_{rj}) = \delta_{jr}$, which ends the proof. ∎

Since ξ is a linear isomorphism, we can transfer the k-algebra structure of $C^* = M_n(k)$ on the space C. Thus C becomes an algebra with the multiplication $\circ$ defined by

$$c \circ d = \xi^{-1}(\xi(c)\xi(d))$$

for any $c, d \in C$. In particular we have that

$$\begin{aligned}
c_{ij} \circ c_{rs} &= \xi^{-1}(E_{ji}E_{sr}) \\
&= \delta_{is}\xi^{-1}(E_{jr}) \\
&= \delta_{is}c_{rj}
\end{aligned}$$

The identity element of the algebra $(C, \circ)$ is $\xi^{-1}(\sum_{i=1,n} E_{ii}) = \sum_{i=1,n} c_{ii}$. We denote $\chi_C = \sum_{i=1,n} c_{ii}$. Note that $(C, \circ)$ is the unique algebra structure on the space C making ξ an algebra morphism. In order to avoid confusions (for eg. in the situation where C is a subcoalgebra of a Hopf algebra, and there exists already a multiplication on elements of C) we will denote by $c^{(r)}$ the element $c \circ c \circ \ldots \circ c$ (c appears r times), and by $c^{(-1)}$ the inverse of an invertible c in $(C, \circ)$. We need a set of formulas.

Lemma 7.3.2 *Let $c, d, e \in C$. Then the following formulas hold.*
(i) $(c|d) = (d|c)$.
(ii) $c \circ d = \sum(c_1|d)c_2 = \sum(c|d_2)d_1$.
(iii) $(c|d) = \varepsilon(c \circ d)$.
(iv) $(x|y \circ z) = (x \circ y|z) = (c \circ d|e)$ *for any cyclic permutation* $\{x, y, z\}$ *of the set* $\{c, d, e\}$.
(v) $(c \circ d|e) = \sum(c|e_1)(d|e_2)$.

Proof: We use for the proof the well known commutation formula for traces $Tr(AB) = Tr(BA)$ for any matrices $A, B \in M_n(k)$.
(i) $(c|d) = Tr(\xi(c)\xi(d)) = Tr(\xi(d)\xi(c)) = (d|c)$.
(ii) It is enough to check for basis elements. Take $c = c_{ij}$ and $d = c_{rs}$. Then $c \circ d = \delta_{is}c_{rj}$ and

$$\begin{aligned}
\sum(c_1|d)c_2 &= \sum_{p=1,n}(c_{ip}|c_{rs})c_{pj} \\
&= \sum_{p=1,n}\delta_{is}\delta_{pr}c_{pj} \\
&= \delta_{is}c_{rj}
\end{aligned}$$

The second formula can be proved similarly.
(iii) Apply ε to (ii) and use the counit property.
(iv) We have that

$$\begin{aligned}
(x|y \circ z) &= Tr(\xi(x)\xi(y \circ z)) \\
&= Tr(\xi(x)\xi(\xi^{-1}(\xi(y)\xi(z))) \\
&= Tr(\xi(x)\xi(y)\xi(z)) \\
&= Tr(\xi(c)\xi(d)\xi(e)) \text{ (by the commutation formula for traces)} \\
&= (c \circ d|e)
\end{aligned}$$

The other equality follows now from (i).
(v)

$$\begin{aligned}
\sum(c|e_1)(d|e_2) &= (c|\sum(d|e_2)e_1) \\
&= (c|d \circ e) \quad \text{(by } (ii)) \\
&= (c \circ d|e) \quad \text{(by } (iv))
\end{aligned}$$

∎

We prove now a Skolem-Noether type result for C.

Proposition 7.3.3 *Let $\phi : C \to C$ be a linear morphism. Then ϕ is a coalgebra morphism if and only if there exists $t \in C$, invertible in the* *algebra* $(C, \circ)$, *such that* $\phi(c) = t^{(-1)} \circ c \circ t$ *for any* $c \in C$. *Moreover, in this case we have that* $Tr(\phi) = \varepsilon(t)\varepsilon(t^{(-1)})$.

Proof: We transfer the problem to the dual algebra of C (which we identified with $M_n(k)$), then use Skolem-Noether theorem there and transfer it back. Thus we have that $\phi : C \to C$ is a coalgebra morphism if and only if $\phi^* : C^* \to C^*$ is an algebra morphism. By using Skolem-Noether theorem, this is equivalent to the existence of some invertible $T \in C^*$ such that $\phi^*(c^*) = Tc^*T^{-1}$ for any $c^* \in C^*$, which applied to an element $c \in C$ means that

$$c^*(\phi(c)) = \sum T(c_1)c^*(c_2)T^{-1}(c_3)$$

for any $c^* \in C^*$. This is equivalent to

$$\phi(c) = \sum T(c_1)T^{-1}(c_3)c_2$$

Let $t = \xi^{-1}(T)$, which is an invertible element in the algebra $(C, \circ)$. Since $T(d) = \xi(t)(d) = (t|d)$ for any $d \in C$, the proof of the equivalence in the statement is finished if we show that for an invertible t in $(C, \circ)$ and an element $c \in C$ we have that

$$\sum (t|c_1)(t^{(-1)}|c_3)c_2 = t^{(-1)} \circ c \circ t$$

This is equivalent to

$$\xi(\sum (t|c_1)(t^{(-1)}|c_3)c_2) = \xi(t^{(-1)} \circ c \circ t)$$

which applied to some $d \in C$ means that

$$\sum (t|c_1)(t^{(-1)}|c_3)(c_2|d) = (t^{(-1)} \circ c \circ t|d)$$

But

$$\begin{aligned}
\sum (t|c_1)(t^{(-1)}|c_3)(c_2|d) &= \sum (t|c_1)(d|c_2)(t^{(-1)}|c_3) \\
&= \sum (t \circ d|c_1)(t^{(-1)}|c_2) \text{ (by Proposition 7.3.2}(v)) \\
&= (t \circ d \circ t^{(-1)}|c) \text{ (by Proposition 7.3.2}(v)) \\
&= (t^{(-1)} \circ c \circ t|d) \text{ (by Proposition 7.3.2}(iv))
\end{aligned}$$

which is what we wanted. For the second part, if ϕ is a coalgebra morphism, we have showed that

$$\phi(c_{ij}) = t^{(-1)} \circ c_{ij} \circ t = \sum_{1 \le p,q \le n} (t|c_{ip})(t^{(-1)}|c_{qj})c_{pq}$$

for any i and j, and this shows that

$$\begin{aligned} Tr(\phi) &= \sum_{1\leq i,j\leq n} (t|c_{ii})(t^{(-1)}|c_{jj}) \\ &= \varepsilon(t)\varepsilon(t^{(-1)}) \end{aligned}$$

∎

The bilinear form $(\ |\ )$ was defined in terms of the comatrix basis $(c_{ij})_{1\leq i,j\leq n}$ of the matrix coalgebra C. At this point we are able to show the following.

Corollary 7.3.4 *The bilinear form $(\ |\ ) : C \times C \to k$ does not depend on the choice of the comatrix basis $(c_{ij})_{1\leq i,j\leq n}$.*

Proof: Let $(c'_{ij})_{1\leq i,j\leq n}$ be another comatrix basis of C, and let $[\ ,\ ]$ be the bilinear form defined by $(c'_{ij})_{1\leq i,j\leq n}$. Then the linear map $\phi : C \to C$ defined by $\phi(c_{ij}) = c'_{ij}$ for any i, j is a coalgebra morphism, so we can apply the previous proposition and find an element t invertible in $(C, \circ)$, where $\circ$ is the multiplication defined on C by the form $(\ |\ )$ associated to the basis $(c_{ij})_{1\leq i,j\leq n}$, such that $\phi(c) = t^{(-1)} \circ c \circ t$ for any $c \in C$. In particular we have that $c'_{ij} = t^{(-1)} \circ c_{ij} \circ t$ for any i, j. Then

$$\begin{aligned} (c'_{ij}|c'_{rs}) &= (t^{(-1)} \circ c_{ij} \circ t|t^{(-1)} \circ c_{rs} \circ t) \\ &= (c_{ij}|c_{rs}) \text{ (by Proposition 7.3.2}(iv)) \\ &= (c_{ij}|c_{rs}) \\ &= \delta_{is}\delta_{jr} \\ &= [c'_{ij}|c'_{rs}] \end{aligned}$$

which shows that $(\ |\ ) = [\ |\ ]$. ∎

Remark 7.3.5 *An immediate consequence of the corollary is that the map ξ and the algebra structure $(C, \circ)$, in particular the identity element of this, do not depend on the choice of the comatrix basis $(c_{ij})_{1\leq i,j\leq n}$. Thus we can regard the element χ_C as a distinguished element of the matrix coalgebra C, no matter what comatrix basis we choose in C.* ∎

Let H be a Hopf algebra which has a nonzero left integral $\lambda \in H^*$. We know that the map $\phi : H \to H^*$, $\phi(h) = \lambda \leftharpoonup h$, is an isomorphism of right H-Hopf modules (Theorem 4.4.6). Since ϕ is a morphism of right H-comodules, it is also a morphism of left H^*-modules, which means that for any $h \in H$ and $p \in H^*$ we have

$$\lambda \leftharpoonup (p \rightharpoonup h) = p(\lambda \leftharpoonup h) \tag{7.15}$$

If we apply (7.15) to an element $a \in H$ we obtain that

$$\sum p(a_1)\lambda(a_2 S(h)) = \sum p(h_2)\lambda(aS(h_1))$$

which can be rewritten as

$$\lambda((a \leftharpoonup p)S(h)) = \lambda(aS(p \rightharpoonup h)) \tag{7.16}$$

Lemma 7.3.6 *Let H be a Hopf algebra with antipode S, $\lambda \in H^*$ a left integral, and C, D subcoalgebras of H such that $C \cap D = 0$. Then $\lambda(cS(d)) = 0$ for any elements $c \in C, d \in D$.*

Proof: Take X a linear subspace of H such that $H = C \oplus D \oplus X$, and pick $p \in H^*$ such that the restriction of p to D is 0 and the restriction of p to C is ε. Then for $c \in C, d \in D$ we have that

$$\begin{aligned} \lambda(cS(d)) &= \lambda((c \leftharpoonup p)S(d)) \\ &= \lambda(cS(p \rightharpoonup d)) \quad \text{(by formula (7.16))} \\ &= 0 \end{aligned}$$

∎

We know that a cosemisimple Hopf algebra has nonzero integrals, so it has a bijective antipode. The next result gives more information about the antipode.

Theorem 7.3.7 *Let H be a cosemisimple Hopf algebra with antipode S. Then $S^2(C) = C$ for any subcoalgebra C.*

Proof: Exercises 5.5.9 and 5.5.10 guarantee the existence of a left integral $\lambda \in H^*$ with $\lambda(1) = 1$, and moreover $\lambda S = \lambda$. The existence of a nonzero integral shows that the antipode is bijective. Since any nonzero subcoalgebra is a sum of simple subcoalgebras (see Exercise 3.1.6), it is enough to prove that $S^2(C) = C$ for any simple subcoalgebra C. Indeed, if C is simple, then $S^2(C)$ is a simple subcoalgebra of H, since S^2 is an injective morphism of coalgebras. Then we have either $S^2(C) = C$ or $C \cap S^2(C) = 0$. If we were in the second situation, then for any $d, c \in C$ we would have $\lambda(S^2(c)S(d)) = 0$ from Lemma 7.3.6. But

$$\begin{aligned} \lambda(S^2(c)S(d)) &= \lambda(S(dS(c))) \\ &= (\lambda S)(dS(c)) \\ &= \lambda(dS(c)) \end{aligned}$$

so we obtain that $\lambda(dS(c)) = 0$ for any $c, d \in C$. In particular for any $c \in C$ we have

$$\begin{aligned} \varepsilon(c) &= \lambda(\varepsilon(c)1) \\ &= \sum \lambda(c_1 S(c_2)) \\ &= 0 \end{aligned}$$

which implies that $C = 0$ (from the counit property), a contradiction. It remains that $S^2(C) = C$. ∎

Proposition 7.3.8 *Let H be a Hopf algebra with antipode S, $\lambda \in H^*$ a left integral, $C \subseteq H$ a matrix subcoalgebra with comatrix basis $(c_{ij})_{1\leq i,j\leq n}$. Then the following assertions hold.*
(1) If $i \neq j$, then $\lambda(c_{ir}S(c_{sj})) = 0$ for any r, s.
(2) $\lambda(c_{ir}S(c_{si})) = \lambda(c_{jr}S(c_{sj}))$ for any i, j, r, s.

Proof: Let X be a linear complement of C in H. We first note that for $c, d \in C$ we have that $\sum (c_1|d)c_2 = c \leftharpoonup p$, where $p \in H^*$ is defined by $p(h) = (h|d)$ for $h \in C$ and $p(h) = 0$ for $h \in X$. Then by Lemma 7.3.2(ii) we obtain $c \circ d = c \leftharpoonup p$. Similarly $c \circ d = q \rightharpoonup d$, where $q(h) = (h|c)$ for $h \in C$ and $q(h) = 0$ for $h \in X$. Let now pick some $1 \leq i, j, r, v, s \leq n$, and take $p \in H^*$ such that $p(h) = (h|c_{jv})$ for $h \in C$ and $p(h) = 0$ for $h \in X$. Then

$$\begin{aligned} \lambda((c_{ir} \circ c_{jv})S(c_{sj})) &= \lambda((c_{ir} \leftharpoonup p)S(c_{sj})) \\ &= \lambda(c_{ir}S(p \rightharpoonup c_{sj})) \quad \text{(by (7.16))} \\ &= \lambda(c_{ir}S(c_{jv} \circ c_{sj})) \end{aligned}$$

Use now $c_{ir} \circ c_{jv} = \delta_{iv}c_{jr}$ and $c_{jv} \circ c_{sj} = c_{sv}$ and obtain

$$\delta_{iv}\lambda(c_{jr}S(c_{sj})) = \lambda(c_{ir}S(c_{sv}))$$

For $v = j$ we obtain

$$\delta_{ij}\lambda(c_{jr}S(c_{sj})) = \lambda(c_{ir}S(c_{sj}))$$

which for $i \neq j$ shows relation (1).
For $v = i$ we obtain relation (2). ∎

Theorem 7.3.9 *(The orthogonality relations for matrix subcoalgebras) Let H be a Hopf algebra, $\lambda \in H^*$ a left integral, and C, D matrix subcoalgebras of H. Then $\lambda(\chi_C S(\chi_D)) = \delta_{C,D}\lambda(1)$.*

Proof: If $C \neq D$ we apply Lemma 7.3.6 to the elements $\chi_C \in C$ and $\chi_D \in D$ and find that $\lambda(\chi_C S(\chi_D)) = 0$.
If $C = D$, then

$$\begin{aligned}
\lambda(\chi_C S(\chi_C)) &= \sum_{1\leq i,j\leq n} \lambda(c_{ii}S(c_{jj})) \\
&= \sum_{1\leq n} \lambda(c_{ii}S(c_{ii})) \quad \text{(by Proposition 7.3.8(1))} \\
&= \sum_{1\leq i\leq n} \lambda(c_{1i}S(c_{i1})) \quad \text{(by Proposition 7.3.8(2))} \\
&= \lambda(\varepsilon(c_{11})1) \\
&= \lambda(1)
\end{aligned}$$

∎

For further use we need the following.

Lemma 7.3.10 *Let H be a cosemisimple Hopf algebra, $\lambda \in H^*$ a left integral, and C a matrix subcoalgebra of H. Let $t \in C$ an invertible element in $(C, \circ)$ such that $S^2(c) = t^{(-1)} \circ c \circ t$ for any $c \in C$. Then $\varepsilon(t) \neq 0$ and $\varepsilon(t^{(-1)}) \neq 0$.*

Proof: Let X be a linear complement of C in H, and define $\phi, \psi \in H^*$ by $\psi(h) = \lambda(\chi_C S(h))$ for any $h \in H$, $\phi(h) = (t|h)$ for any $h \in C$ and $\phi(h) = 0$ for any $h \in X$. Let $c \in C$ and $p \in H^*$ such that $p(h) = (h|c)$ for $h \in C$ and $p(h) = 0$ for $h \in X$. We have seen that $p \rightharpoonup d = c \circ d$ and $d \leftharpoonup p = d \circ c$ for any $d \in C$. Then for any $d \in C$ we have

$$\begin{aligned}
\psi(c \circ d) &= \lambda(\chi_C S(c \circ d)) \\
&= \lambda(\chi_C S(p \rightharpoonup d)) \\
&= \lambda((\chi_C \leftharpoonup p) S(d)) \quad \text{(by (7.16))} \\
&= \lambda((\chi_C \circ c) S(d)) \\
&= \lambda(cS(d))
\end{aligned}$$

We have showed that for any $c, d \in C$ we have that

$$\psi(c \circ d) = \lambda(cS(d)) \tag{7.17}$$

Then

$$\begin{aligned}
\psi(c \circ d) &= \lambda(cS(d)) \\
&= \lambda S(cS(d)) \\
&= \lambda(S^2(d)S(c)) \\
&= \lambda((t^{(-1)} \circ d \circ t)S(c)) \\
&= \psi(t^{(-1)} \circ d \circ t \circ c) \quad \text{(by (7.17))}
\end{aligned}$$

This means that ψ is zero on the space V spanned by all $c \circ d - t^{(-1)} \circ d \circ t \circ c$ with $c, d \in C$. On the other hand

$$\begin{aligned}
\phi(t^{(-1)} \circ d \circ t \circ c) &= (t|t^{(-1)} \circ d \circ t \circ c) \\
&= (t|c \circ d) \text{ (by Lemma 7.3.2}(iv)) \\
&= \phi(c \circ d)
\end{aligned}$$

so $\phi(V) = 0$.
Let $C^* \simeq M_n(k)$. Since $\operatorname{codim}(< AB - BA|A, B \in M_n(k) >) = 1$ in $M_n(k)$, by transferring this fact via the isomorphism $\xi : (C, \circ) \to M_n(k)$, we obtain that $\operatorname{codim}(< c \circ d - d \circ c|c, d \in C >) = 1$ in C (by $< S >$ we denote the linear subspace spanned by the set S). Since t is invertible in $(C, \circ)$, this implies that $\operatorname{codim}(< (t \circ c) \circ d - d \circ (t \circ c)|c, d \in C >) = 1$ in C, and then $\operatorname{codim}(< t^{(-1)}(t \circ c \circ d - d \circ t \circ c)|c, d \in C >) = 1$ in C, which means that the codimension of V in C is 1.
Since $t \neq 0$ we have that $\phi \neq 0$ (otherwise the image of t in C^* through the isomorphism ξ would be zero). Since both ϕ and ψ are zero on V, we obtain that there exists $\alpha \in k$ such that $\psi = \alpha\phi$. The orthogonality relation shows that $\psi(\chi_C) = \lambda(\chi_C S(\chi_C)) = 1$. But

$$\begin{aligned}
\phi(\chi_C) &= (t|\chi_C) \\
&= \sum_{1 \leq i \leq n} (t|c_{ii}) \\
&= \varepsilon(t)
\end{aligned}$$

so $1 = \alpha\varepsilon(t)$, which implies that $\varepsilon(t) \neq 0$. To obtain that $\varepsilon(t^{(-1)}) \neq 0$ we regard everything in the Hopf algebra $H^{op,cop}$, where t is replaced by $t^{(-1)}$.
∎

7.4 Cosemisimplicity, semisimplicity, and the square of the antipode

In this section H will denote a finite dimensional Hopf algebra and $\lambda \in H^*$ a left integral, $\phi : H \to H^*$, $\phi(h) = \lambda \leftharpoonup h$, the isomorphism of right H-Hopf modules. We recall from the previous section that for any $h \in H$ and $p \in H^*$ we have (formula (7.15))

$$\lambda \leftharpoonup (p \rightharpoonup h) = p(\lambda \leftharpoonup h)$$

and for any $a, h \in H$ and $p \in H^*$ we have (formula (7.16)

$$\lambda((a \leftharpoonup p)S(h)) = \lambda(aS(p \rightharpoonup h))$$

Let $\Lambda = \phi^{-1}(\varepsilon)$. For any $p \in H^*$ we have that

$$p = p\varepsilon = p\phi(\Lambda) = \phi(p \rightharpoonup \Lambda)$$

thus $\phi^{-1}(p) = p \rightharpoonup \Lambda$ for any $p \in H^*$. If we apply the equality $\phi^{-1}\phi = Id$ to an $h \in H$, we obtain that $h = (\lambda \leftharpoonup h) \rightharpoonup \Lambda$, which in particular for $h = 1$ shows that $\lambda \rightharpoonup \Lambda = 1$, and then if we apply ε we obtain that $\lambda(\Lambda) = 1$. If we apply the relation $\phi\phi^{-1} = Id$ to ε we find that $\lambda \leftharpoonup \Lambda = \varepsilon$.
On the other hand for any $h \in H$ we have that

$$\begin{aligned} \phi(\Lambda h) &= \phi(\Lambda) \leftharpoonup h \\ &= \varepsilon \leftharpoonup h \\ &= \varepsilon(h)\varepsilon \\ &= \phi(\varepsilon(h)\Lambda) \end{aligned}$$

showing that $\Lambda h = \varepsilon(h)\Lambda$. Thus $\Lambda \in H$ is a right integral.

For any $q \in H^*$ we denote by $R(q) : H^* \longrightarrow H^*$ the linear morphism induced by the right multiplication with q, i.e. $R(q)(p) = pq$ for any $p \in H^*$. We also denote by $\eta : H^* \otimes H \longrightarrow End(H^*)$, $\eta(q \otimes h)(p) = p(h)q$ for any $p, q \in H^*$, $h \in H$. Then η is a linear isomorphism (Lemma 1.3.2). With this notation equation (7.15) can be written $R(\lambda \leftharpoonup h)(p) = \sum \eta((\lambda \leftharpoonup h_1) \otimes h_2)(p)$, or

$$R(\lambda \leftharpoonup h) = \sum \eta((\lambda \leftharpoonup h_1) \otimes h_2) \qquad (7.18)$$

If $f : H \longrightarrow H$ is a linear morphism, denote by $f^* : H^* \longrightarrow H^*$ the dual morphism of f. Then for any $p, q \in H^*$, $a, h \in H$ we have

$$\begin{aligned} ((\eta(q \otimes h) \circ f^*)(p))(a) &= (\eta(q \otimes h)(pf))(a) \\ &= (pf(h)q)(a) \\ &= p(f(h))q(a) \\ &= ((\eta(q \otimes f(h)))(p))(a) \end{aligned}$$

so $\eta(q \otimes h) \circ f^* = \eta(q \otimes f(h))$, which combined with the relation (7.18) shows that

$$R(\lambda \leftharpoonup h) \circ f^* = \sum \eta((\lambda \leftharpoonup h_1) \otimes f(h_2)) \qquad (7.19)$$

We recall that for a finite dimensional vector space V with basis $(v_i)_{1 \le i \le n}$ and dual basis $(v_i)^*_{1 \le i \le n}$ in V^*, the trace of a linear endomorphism $u : V \longrightarrow V$ is

$$Tr(u) = \sum_{1 \le i \le n} v_i^*(u(v_i))$$

This does not depend on the choosen basis of V, and in fact it is just the trace of the matrix of u in the basis $(v_i)_{1\leq i\leq n}$. In particular, the fact that $Tr(AB) = Tr(BA)$ for any $A, B \in M_n(k)$ shows that $Tr(uv) = Tr(vu)$ for any $u, v \in End_k(V)$. For the dual morphism $u^* : V^* \to V^*$ we obtain

$$\begin{aligned} Tr(u^*) &= \sum_{i=1,n} v_i^{**}(u^*(v_i^*)) \\ &= \sum_{1\leq i\leq n} u^*(v_i^*)(v_i) \\ &= \sum_{1\leq i\leq n} v_i^*(u(v_i)) \\ &= Tr(u) \end{aligned}$$

In particular, if $q \in H^*$ and $h \in H$ we have that

$$\begin{aligned} Tr(\eta(q \otimes h)) &= \sum_{1\leq i\leq n} \eta(q \otimes h)(v_i^*)(v_i) \\ &= \sum_{1\leq i\leq n} (v_i^*(h)q)(v_i) \\ &= q(\sum_{1\leq i\leq n} v_i^*(h)v_i) \\ &= q(h) \end{aligned}$$

thus

$$Tr(\eta(q \otimes h)) = q(h) \tag{7.20}$$

If we write equation (7.19) for $h = \Lambda$ and use the fact that $R(\varepsilon) = Id$, we obtain

$$f^* = \sum \eta((\lambda \leftharpoonup \Lambda_1) \otimes f(\Lambda_2)) \tag{7.21}$$

Equation (7.21) shows by using (7.20) that

$$Tr(f) = Tr(f^*) = (\lambda \leftharpoonup \Lambda_1)(f(\Lambda_2)) = \sum \lambda(f(\Lambda_2)S(\Lambda_1)) \tag{7.22}$$

We are able to prove now an important result characterizing semisimple cosemisimple Hopf algebras.

Theorem 7.4.1 *Let H be a finite dimensional Hopf algebra with antipode S. Then H is semisimple and cosemisimple if and only if $Tr(S^2) \neq 0$.*

Proof: We have that

$$\begin{aligned} Tr(S^2) &= \sum \lambda(S^2(\Lambda_2)S(\Lambda_1)) \text{ (by (7.22))} \\ &= \sum \lambda S(\Lambda_1 S(\Lambda_2)) \\ &= \lambda(\varepsilon(\Lambda)S(1)) \\ &= \lambda(1)\varepsilon(\Lambda) \end{aligned}$$

This ends the proof if we use the facts that H is semisimple if and only if $\varepsilon(\Lambda) \neq 0$ (Theorem 5.2.10) and H is cosemisimple if and only if $\lambda(1) \neq 0$ (Exercise 5.5.9). ∎

We define for any $h \in H$ and $p \in H^*$ the linear morphisms $l(h) : H \to H$ and $l(p) : H \to H$ by

$$l(h)(a) = ha, \quad l(p)(a) = p \rightharpoonup a$$

for any $a \in H$. We have that

$$\begin{aligned} Tr(l(h) \circ S^2 \circ l(p)) &= \sum \lambda(hS^2(p \rightharpoonup \Lambda_2)S(\Lambda_1)) \text{ (by (7.22))} \\ &= \sum \lambda(hS(\Lambda_1 S(p \rightharpoonup \Lambda_2))) \\ &= \sum \lambda(hS(\Lambda_1 S(\Lambda_2)p(\Lambda_3))) \\ &= \sum \lambda(hS(\varepsilon(\Lambda_1)p(\Lambda_2))) \\ &= \lambda(h)p(\Lambda) \end{aligned}$$

We have obtained

$$Tr(l(h) \circ S^2 \circ l(p)) = \lambda(h)p(\Lambda) \tag{7.23}$$

Exercise 7.4.2 *Show that $l(p)^* = R(p)$ for any $p \in H^*$. In particular $Tr(l(p)) = Tr(R(p))$.*

Let us consider the element $x \in H$ such that

$$p(x) = Tr(l(p)) = Tr(R(p))$$

for any $p \in H^*$. Such an element x exists and is unique. Indeed, if $i : H \to H^{**}$ is the natural isomorphism, and $h^{**} \in H^{**}$ is defined by $h^{**}(p) = Tr(l(p))$ for any $p \in H^*$, we just take $x = i^{-1}(h^{**})$.

Exercise 7.4.3 *Show that if $S^2 = Id$ and H is cosemisimple, then x is a nonzero right integral in H.*

Lemma 7.4.4 *We have that* $Tr(l(x) \circ S^2) = \lambda(1)\varepsilon(\Lambda) = Tr(S^2)$.

Proof: If we write (7.19) for $f = Id$ we obtain

$$R(\lambda \leftharpoonup h) = \sum \eta((\lambda \leftharpoonup h_1) \otimes h_2)$$

Then for any $h \in H$

$$\begin{aligned}
(\lambda \leftharpoonup h)(x) &= Tr(R(\lambda \leftharpoonup h)) \text{ (definition of } x) \\
&= Tr(\sum \eta((\lambda \leftharpoonup h_1) \otimes h_2)) \quad \text{(by (7.19))} \\
&= \sum (\lambda \leftharpoonup h_1)(h_2) \\
&= \sum \lambda(h_2 S(h_1))
\end{aligned}$$

We obtain

$$(\lambda \leftharpoonup h)(x) = \sum \lambda(h_2 S(h_1)) \tag{7.24}$$

For $h = 1$, this shows that $\lambda(x) = \lambda(1)$. We use now (7.23) for $h = x$ and $p = \varepsilon$ and obtain

$$\begin{aligned}
Tr(l(x) \circ S^2) &= \lambda(x)\varepsilon(\Lambda) \\
&= \lambda(1)\varepsilon(\Lambda) \\
&= Tr(S^2)
\end{aligned}$$

■

Lemma 7.4.5 *The following formulas hold:*
(i) $\sum x_1 \otimes x_2 = \sum x_2 \otimes x_1$.
(ii) $x^2 = \dim(H)x = \varepsilon(x)x$.
(iii) $S^2(x) = x$.
(iv) $Tr(S^2) = \dim(H) Tr(S^2_{|xH})$.

Proof: (i) Let $\psi : H^* \otimes H^* \to (H \otimes H)^*$ be the linear isomorphism defined by $\psi(p \otimes q)(g \otimes h) = p(g)q(h)$ for any $p, q \in H^*$, $g, h \in H$. Then for proving that $\sum x_1 \otimes x_2 = \sum x_2 \otimes x_1$ it is enough to show that

$$\psi(p \otimes q)(\sum x_1 \otimes x_2) = \psi(p \otimes q)(\sum x_2 \otimes x_1)$$

for any $p, q \in H^*$. This can be seen as follows

$$\begin{aligned}
\psi(p \otimes q)(\sum x_1 \otimes x_2) &= (pq)(x) \\
&= Tr(l(pq)) \quad \text{(by the definition of } x) \\
&= Tr(l(p) \circ l(q))
\end{aligned}$$

$$\begin{aligned}
&= Tr(l(q) \circ l(p)) \\
&= Tr(l(qp)) \\
&= (qp)(x) \\
&= \psi(p \otimes q)(\sum x_2 \otimes x_1)
\end{aligned}$$

(ii) For any $h \in H$ we have that

$$\begin{aligned}
(\lambda \leftharpoondown h)(x^2) &= (\lambda \leftharpoondown hS^{-1}(x))(x) \\
&= \sum \lambda(h_2 S^{-1}(x_1) S(h_1 S^{-1}(x_2))) \\
&= \sum \lambda(h_2 S^{-1}(x_1) x_2 S(h_1)) \\
&= \sum \lambda(h_2 S^{-1}(x_2) x_1 S(h_1)) \text{ (by (}i\text{))} \\
&= \varepsilon(x) \sum \lambda(h_2 S(h_1)) \\
&= \varepsilon(x)(\lambda \leftharpoondown h)(x) \text{ (by (7.24))} \\
&= (\lambda \leftharpoondown h)(\varepsilon(x)x)
\end{aligned}$$

for any $h \in H$. Since $H^* = \{\lambda \leftharpoondown h | h \in H\}$ we obtain that $x^2 = \varepsilon(x)x$. On the other hand

$$\begin{aligned}
\varepsilon(x) &= Tr(l(\varepsilon)) \\
&= Tr(Id_H) \\
&= \dim(H)
\end{aligned}$$

which completes the proof of (ii).
(iii) Let $p \in H^*$ and $h \in H$. We have that

$$\begin{aligned}
l(p \circ S^2)(h) &= (p \circ S^2) \rightharpoonup h \\
&= \sum p(S^2(h_2)) h_1 \\
&= \sum S^{-2}(p(S^2(h_2)) S^2(h_1)) \\
&= S^{-2}(p \rightharpoonup S^2(h)) \\
&= S^{-2}(l(p)(S^2(h))) \\
&= (S^{-2} \circ l(p) \circ S^2)(h)
\end{aligned}$$

thus $l(p \circ S^2) = S^{-2} \circ l(p) \circ S^2$. Then for any $p \in H^*$ we have

$$\begin{aligned}
p(S^2(x)) &= (p \circ S^2)(x) \\
&= Tr(l(p \circ S^2)) \text{ (definition of } x\text{)} \\
&= Tr(S^{-2} \circ l(p) \circ S^2)
\end{aligned}$$

$$\begin{aligned} &= Tr(S^2 \circ S^{-2} \circ l(p)) \\ &= Tr(l(p)) \\ &= p(x) \end{aligned}$$

which shows that $S^2(x) = x$.
(iv) Let $T = l(x) \circ S^2$. We know from Lemma 7.4.4 that $Tr(T) = Tr(S^2)$. We have that

$$\begin{aligned} T(xh) &= (l(x) \circ S^2)(xh) \\ &= xS^2(xh) \\ &= xS^2(x)S^2(h) \\ &= x^2S^2(h) \\ &= \dim(H)xS^2(h) \\ &= \dim(H)S^2(x)S^2(h) \\ &= \dim(H)S^2(xh) \end{aligned}$$

which shows that $T_{|xH} = \dim(H)S^2_{|xH}$. Since obviously $Im(T) \subseteq xH$, we can regard $T_{|xH}$ as a linear endomorphism of the space xH, and then

$$Tr(T_{|xH}) = \dim(H)Tr(S^2_{|xH})$$

But since $Im(T) \subseteq xH$, we have that $Tr(T) = Tr(T_{|xH})$, so we obtain

$$Tr(S^2) = Tr(T) = Tr(T_{|xH}) = \dim(H)Tr(S^2_{|xH})$$

∎

Theorem 7.4.6 *(Larson-Radford) Let k be a field of characteristic zero and H a finite dimensional Hopf algebra over k, with antipode S. The following assertions are equivalent.*
(i) H is cosemisimple.
(ii) H is semisimple.
(iii) $S^2 = Id$.

Proof: (iii)⇒(i) and (iii)⇒(ii) follow directly from Theorem 7.4.1 since $Tr(S^2) = Tr(Id) = \dim(H)$.
(i)⇒(ii) We first use Exercises 4.2.17, 5.5.12 and 5.2.13 to reduce to the case where k is algebraically closed. Let C be a matrix subcoalgebra of H. We know that $S^2(C) = C$ (Theorem 7.3.7) and that there exists an invertible t in the algebra $(C, \circ)$ such that $S^2(c) = t^{(-1)} \circ c \circ t$ for any $c \in C$ (Proposition 7.3.3). Let r be the order of S^2 (which is finite by Theorem 7.1.7). Then $c = S^{2r}(c) = t^{(-r)} \circ c \circ t^{(r)}$ for any $c \in C$, so $t^{(r)}$ is in the

center of the algebra $(C, \circ)$. Taking account of the algebra isomorphism $\xi : C \longrightarrow M_n(k)$ we have that the center of $(C, \circ)$ is $k\chi_C$, thus $t^{(r)} = \alpha\chi_C$ for some $\alpha \in k$. Since t is invertible we have that $\alpha \neq 0$, and then replacing t by $\frac{1}{\alpha^{1/r}}t$ (which still verifies $S^2(c) = t^{(-1)} \circ c \circ t$), we can assume that $t^{(r)} = \chi_C$. Then $\xi(t)^r = I$, the identity matrix, so the minimal polynomial of $\xi(t)$ divides $X^r - 1$, and hence it has only simple roots. This implies that the matrix $\xi(t)$ is diagonalizable with eigenvalues r-th roots of unity. Since k has characteristic zero we may assume that the field of rational numbers $\mathbf{Q} \subseteq k$, and then, since k is algebraically closed, that the field $\overline{\mathbf{Q}}$ (regarded as a subfield of the complex numbers) is contained in k. Since the inverse of a complex root of unity is the conjugate of that root, we obtain that $\xi(t^{(-1)})$ is diagonalizable with eigenvalues the (complex) conjugates of the eigenvalues of $\xi(t)$. In particular

$$Tr(\xi(t^{(-1)}))Tr(\xi(t)) = \overline{Tr(\xi(t))}Tr(\xi(t)) \in \mathbf{R}_+$$

Proposition 7.3.3 tells that

$$Tr(S^2_{|C}) = \varepsilon(t)\varepsilon(t^{(-1)}) = Tr(\xi(t^{(-1)}))Tr(\xi(t))$$

On the other hand $\varepsilon(t), \varepsilon(t^{(-1)}) \neq 0$ by Lemma 7.3.10, so $Tr(S^2_{|C}) > 0$. We conclude that $Tr(S^2)$ is a sum of positive numbers, since H is a direct sum of matrix subcoalgebras, so $Tr(S^2) > 0$. In particular $Tr(S^2) \neq 0$, showing that H is semisimple.
(ii)$\Rightarrow$(i) If H is semisimple, then H^* is cosemisimple, and by (i)$\Rightarrow$(ii) we obtain that H^* is semisimple, so H is cosemisimple.
(i)$\Rightarrow$(iii) Let H be cosemisimple. So H is also semisimple and then the distinguished grouplike elements of H and H^* are 1 and ε (by Remark 7.1.1). Using the formula of Theorem 7.1.6 we obtain $S^4 = Id$. Then S^2 is diagonalizable and any eigenvalue of S^2 is either 1 or -1. It follows that $Tr(S^2) \leq \dim(H)$. We have already seen that $Tr(S^2) > 0$. On the other hand $Tr(S^2) = (\dim(H))Tr(S^2_{|xH})$ by Lemma 7.4.5, which shows that $\dim(H)$ divides $Tr(S^2)$. Since $0 < Tr(S^2) \leq \dim(H)$, we must have $Tr(S^2) = \dim(H)$, and this forces all the eigenvalues of S^2 to be equal to 1. We obtain $S^2 = Id$. ∎

Exercise 7.4.7 *Let k be a field of characteristic zero and H a semisimple Hopf algebra over k. Show that a right (or left) integral t in H is cocommutative, i.e. $\sum t_1 \otimes t_2 = \sum t_2 \otimes t_1$.*

Exercise 7.4.8 *Let k be a field of characteristic zero and H be a finite dimensional Hopf algebra over k. Show that:*
(i) If H is commutative, then $H \simeq (kG)^*$ for some finite group G.
(ii) If H is cocommutative, then $H \simeq kG$ for a finite group G.

Exercise 7.4.9 *Let H be a finite dimensional Hopf algebra over a field of characteristic zero, and let S be the antipode of H. Show that S has odd order if and only if $H \simeq kG$, where $G = C_2 \times C_2 \times \ldots \times C_2$, and in this case $S = Id$, so the order of S is 1.*

7.5 Character theory for semisimple Hopf algebras

In this section H will be a semisimple Hopf algebra over an algebraically closed field k of characteristic 0. Let $V \in {}_H\mathcal{M}$ be a finite dimensional H-module with basis $(v_i)_{1\leq i\leq n}$ and dual basis $(v_i)^*_{1\leq i\leq n}$ in V^*. We can regard V as a representation of the algebra H, i.e. an algebra morphism $\rho : H \to End_k(V)$, defined by $\rho(h)(v) = hv$ for any $h \in H, v \in V$. Then the character $\chi(V)$ of the H-module V is defined to be the character of the representation ρ. This means that $\chi(V) \in H^*$, $\chi(V)(h) = Tr(\rho(h))$ for any $h \in H$. In terms of the choosen basis we have

$$\chi(V)(h) = \sum_{1\leq i\leq n} v_i^*(hv_i)$$

Exercise 7.5.1 *Let $V, W \in {}_H\mathcal{M}$ be finite dimensional. Then $\chi(V\oplus W) = \chi(V) + \chi(W)$ and $\chi(V \otimes W) = \chi(V)\chi(W)$.*

The antipode S of H can be used to construct a left H-module structure on the dual of a left H-module. If $V \in {}_H\mathcal{M}$ is finite dimensional, then $V^* = Hom_k(H, k)$ has an induced structure of a right H-module and then we transfer this action to the left by using the antipode. We obtain that $V^* \in {}_H\mathcal{M}$ by

$$hv^*(v) = v^*(S(h)v)$$

for any $h \in H, v^* \in V^*, v \in V$.

Exercise 7.5.2 *Show that for a finite dimensional $V \in {}_H\mathcal{M}$ we have $\chi(V^*) = S^*(\chi(V))$, where S^* is the dual map of S.*

Proposition 7.5.3 *1) If $f : V \to W$ is a morphism of finite dimensional left H-modules, then $f^* : W^* \to V^*$ is a morphism of left H-modules.*
2) If V is a finite dimensional left H-module, then $V^{**} \simeq V$ as left H-modules.

Proof: 1) Let $h \in H, w^* \in W^*$ and $v \in V$. Then

$$f^*(hw^*)(v) \quad = \quad (hw^*)(f(v))$$

$$\begin{aligned} &= w^*(S(h)f(v)) \\ &= w^*(f(S(h)v)) \\ &= f^*(w^*)(S(h)v) \\ &= (hf^*(w^*))(v) \end{aligned}$$

2) We show that the natural linear isomorphism $i : V \to V^{**}$ defined by $i(v)(v^*) = v^*(v)$ for any $v \in V, v^* \in V^*$, is also a morphism of left H-modules. Indeed, we have that

$$\begin{aligned} (hi(v))(v^*) &= i(v)(S(h)v^*) \\ &= (S(h)v^*)(v) \\ &= v^*(S^2(h)v) \\ &= v^*(hv) \quad (\text{since } S^2 = Id) \\ &= i(hv)(v^*) \end{aligned}$$

∎

Corollary 7.5.4 *If V is a simple left H-module, then V^* is also a simple left H-module.*

Proof: Let $f : X \to V^*$ be the inclusion morphism of a left H-submodule of V^*. Then $f^* : V^{**} \to X^*$ is a surjective morphism of left H-modules. Since $V^{**} \simeq V$, thus it is a simple H-module, we obtain that either $f^* = 0$, and then $X = 0$, or f^* is an isomorphism, and then $f = Id$ and $X = V^*$. ∎

If V is a simple left H-module, then we can also regard V as a simple right H^*-comodule. The coalgebra C associated to V (i.e. the minimal subcoalgebra of H^* such that V is a C-comodule) is a simple coalgebra, so it is a matrix coalgebra, since k is algebraically closed (see Exercise 2.5.4 and Exercise 3.1.2). The following lemma gives a description of the character of V in terms of the associated coalgebra C.

Lemma 7.5.5 *Let V be a simple left H-module and C be the coalgebra associated to the simple right H^*-comodule V. Then $\chi(V) = \chi_C$.*

Proof: We know that C has a comatrix basis $(c_{ij})_{1 \le i,j \le n}$, where $n = \dim(V)$, such that the coaction on the elements of a basis $(v_i)_{1 \le i \le n}$ works by $\rho(v_i) = \sum_{1 \le j \le n} v_j \otimes c_{ij}$, where $\rho : V \to V \otimes H^*$ denotes the comodule structure map of V. This implies that the action of H on V works by $hv_i = \sum_{1 \le j \le n} c_{ij}(h)v_j$ for any $h \in H$ and $1 \le i \le n$. In terms of this coaction, the character of the H-module V is given by

$$\chi(V)(h) = \sum_{1 \le i \le n} v_i^*(hv_i)$$

$$\begin{aligned} &= \sum_{1\leq i,j\leq n} c_{ij}(h)v_i^*(v_j) \\ &= \sum_{1\leq i\leq n} c_{ii}(h) \end{aligned}$$

We obtain that $\chi(V) = \sum_{1\leq i\leq n} c_{ii} = \chi_C$. ∎

Let H be a semisimple Hopf algebra, $V_1, \ldots, V_n$ the isomorphism types of simple left H-modules, and $\chi_1 = \chi(V_1), \ldots, \chi_n = \chi(V_n) \in H^*$ their characters (usualy called the irreducible characters of H). We choose V_1 to be the trivial H-module, i.e. $V_1 = k$ with the action given by $h\alpha = \varepsilon(h)\alpha$ for any $h \in H$ and $\alpha \in k$. We know from Corollary 7.5.4 that for any i, the left H-module V_i^* is simple, so there exists a unique $\bar{i} \in \{1, \ldots, n\}$ such that $V_i^* \simeq V_{\bar{i}}$. Since $V^{**} \simeq V$ as H-modules, the assignement $i \mapsto \bar{i}$ provides an involutory permutation of the set $\{1, \ldots, n\}$. Moreover $S^*(\chi_i) = \chi_{\bar{i}}$ and $\dim(V_{\bar{i}}) = \dim(V_i)$.

Let $H \simeq M_{d_1}(k) \times \ldots \times M_{d_n}(k)$ be the representation of the algebra H as a product of matrix rings, such that V_i is the unique isomorphism type of simple left H-module produced by $M_{d_i}(k)$, in particular $\dim(V_i) = d_i$. Moreover, the decomposition of the left H-module H as a sum of simple H-modules is $H \simeq \oplus_{1\leq i\leq n} V_i^{(d_i)}$, in particular $\chi(H) = \sum_{1\leq i\leq n} d_i\chi_i$. Passing to the dual coalgebra H^* of H, we have that $H^* = \oplus C_i$, a direct sum of simple subcoalgebras, where $C_i \simeq (M_{d_i}(k))^* \simeq M^c(d_i, k)$ for any $1 \leq i \leq n$. In view of Exercise 2.2.18, V_i is a simple H^*-comodule, and C_i is the simple subcoalgebra associated to V_i. In particular $\chi_i = \chi_{C_i}$. The orthogonality relations for matrix subcoalgebras of a Hopf algebra (Theorem 7.3.9) can be written in our context as follows.

Theorem 7.5.6 *Let H be a semisimple Hopf algebra with antipode S, $\chi_1, \ldots, \chi_n \in H^*$ the irreducible characters of H, and $\Lambda^* \in H^{**}$ an integral. Then for any $1 \leq i, j \leq n$ we have $\Lambda^*(\chi_i S^*(\chi_j)) = \delta_{i,j}\Lambda^*(\varepsilon)$.* ∎

Let

$$C_{\mathbf{Q}}(H) = \sum_{1\leq i\leq n} \mathbf{Q}\chi_i$$

be the $\mathbf{Q}$-subspace of H^* spanned by $\chi_1, \ldots, \chi_n$. In fact $C_{\mathbf{Q}}(H)$ is a $\mathbf{Q}$-subalgebra of H^*. Indeed, for any $1 \leq i, j \leq n$, $\chi_i\chi_j = \chi(V_i)\chi(V_j) = \chi(V_i \otimes V_j)$, which is a linear combination of $\chi_1, \ldots, \chi_n$ with nonnegative integer coefficients, since $V_i \otimes V_j$, as a left H-module, is a direct sum of simple H-modules. The $\mathbf{Q}$-algebra $C_{\mathbf{Q}}(H)$ is called the $\mathbf{Q}$-algebra of characters of H.

Similarly, the k-subspace of H^* spanned by $\chi_1, \ldots, \chi_n$ is a k-subalgebra of H^*, denoted by $C_k(H)$, and called the k-algebra of characters. An immediate consequence of the orthogonality relations is the following.

Proposition 7.5.7 *The irreducible characters $\chi_1, \ldots, \chi_n$ are linearly independent over k (inside H^*).*

Proof: Let $\Lambda^* \in H^{**}$ be an integral with $\Lambda^*(\varepsilon) = 1$. If $\sum_{1\leq i\leq n} \alpha_i\chi_i = 0$ for some scalars $\alpha_i \in k$, we have that for any t

$$\begin{aligned} 0 &= \Lambda^*(\sum_{1\leq i\leq n} \alpha_i\chi_i S^*(\chi_t)) \\ &= \sum_{1\leq i\leq n} \alpha_i\Lambda^*(\chi_i S^*(\chi_t)) \\ &= \alpha_t\Lambda^*(\chi_t S^*(\chi_t)) \\ &= \alpha_t\Lambda^*(\varepsilon) \\ &= \alpha_t \end{aligned}$$

∎

Corollary 7.5.8 *There exists an isomorphism of k-algebras $C_k(H) \simeq k\otimes_{\mathbf{Q}} C_{\mathbf{Q}}(H)$ mapping $\chi_i \in C_k(H)$ to $1 \otimes \chi_i \in k \otimes_{\mathbf{Q}} C_{\mathbf{Q}}(H)$.* ∎

Lemma 7.5.9 *Let $M \in {}_H\mathcal{M}$ and $M = X_1 \oplus \ldots \oplus X_r$ a representation of M as a sum of simple H-modules. Then $M^H = \oplus\{X_i | X_i \simeq V_1\}$.*

Proof: Let $m \in M^H$ and $m = m_1 + \ldots + m_r$ with $m_i \in X_i$ for any $1 \leq i \leq t$. Then

$$\begin{aligned} \varepsilon(h)m_1 + \ldots + \varepsilon(h)m_r &= \varepsilon(h)m \\ &= hm \\ &= hm_1 + \ldots + hm_r \end{aligned}$$

showing that $hm_i = \varepsilon(h)m_i$ for any for any i and $h \in H$, i.e. $m_i \in X_i^H$ for any i. Thus $M^H = X_1^H \oplus \ldots \oplus X_r^H$. The characterization of M^H follows immediately from the fact that if X is an H-module, the subspace of invariants X^H is an H-submodule, and if X is simple, then either $X^H = 0$, or $X = X^H \simeq V_1$. ∎

Lemma 7.5.10 *Let V and W be simple left H-modules. Then* $\dim(V \otimes W^*)^H = 1$ *if V and W are isomorphic, and* $\dim(V \otimes W^*)^H = 0$ *if V and W are not isomorphic.*

Proof: Let $\phi : V\otimes W^* \to Hom_k(W, V)$ be the natural linear isomorphism, i.e. $\phi(v \otimes w^*)(w) = w^*(w)v$ for any $v \in V, w^* \in W^*, w \in W$. We can transfer via ϕ the H-module structure of $V \otimes W^*$ to $Hom_k(W, V)$. This means that if $f = \phi(v \otimes w^*) \in Hom_k(W, V)$ (in fact we should take a sum of tensor monomials in $V \otimes W^*$, but we write like this for simplicity), then for any $h \in H$ and $w \in W$ we have

$$\begin{aligned}
(hf)(w) &= (h\phi(v \otimes w^*))(w) \\
&= \phi(h(v \otimes w^*))(w) \\
&= \sum \phi(h_1 v \otimes h_2 w^*)(w) \\
&= \sum (h_2 w^*)(w)(h_1 v) \\
&= \sum w^*(S(h_2)w)(h_1 v) \\
&= \sum h_1(w^*(S(h_2)w)v) \\
&= \sum h_1 \phi(v \otimes w^*)(S(h_2)w) \\
&= \sum h_1 f(S(h_2)w)
\end{aligned}$$

Thus

$$(hf)(w) = \sum h_1 f(S(h_2)w)$$

Now we have $Hom_k(W,V)^H = Hom_H(W,V)$. Indeed, if $f \in Hom_H(W,V)$, then $(hf)(w) = \sum h_1 f(S(h_2)w) = \sum f(h_1 S(h_2)w) = \varepsilon(h)f(w)$, so $f \in Hom_k(W,V)^H$. Conversely, let $f \in Hom_k(W,V)^H$. Then for any $h \in H, w \in W$

$$\begin{aligned}
hf(w) &= \sum h_1 f(\varepsilon(h_2)w) \\
&= \sum h_1 f(S(h_2)(h_3 w)) \\
&= \sum \varepsilon(h_1) f(h_2 w) \\
&= f(hw)
\end{aligned}$$

so f is a morphism of H-modules. Therefore $(V \otimes W^*)^H \simeq Hom_H(W,V)$. The result follows now by using Schur's lemma. ∎

Proposition 7.5.11 *Let $\chi_1, \ldots, \chi_n$ be the irreducible characters of H. Then for any i and j we have $\chi_i \chi_{\bar{j}} = \delta_{ij}\chi_1 + \sum_{2 \le r \le n} a_r \chi_r$ for some nonnegative integers $a_2, \ldots, a_n$.*

Proof: We know that $\chi_i \chi_{\bar{j}} = \chi(V_i \otimes V_j^*)$, which is a linear combination of the irreducible characters with nonnegative integer coefficients. Moreover, the coefficient of χ_1 is the number of appearances of V_1 in the decomposition of $V_i \otimes V_j^*$ as a sum of simple modules. Lemma 7.5.9 shows that this number is $\dim(V \otimes W^*)^H$, and this is δ_{ij} by the previous lemma. ∎

Theorem 7.5.12 *The $\mathbf{Q}$-algebra of characters $C_{\mathbf{Q}}(H)$ is semisimple.*

Proof: We first show that if $u \in C_{\mathbf{Q}}(H)$, $u \neq 0$, then $uS^*(u) \neq 0$. Indeed, let $u = \sum_{1\leq i\leq n} x_i\chi_i$, for some $x_1, \ldots, x_n \in \mathbf{Q}$, not all zero. Then

$$\begin{aligned} uS^*(u) &= (\sum_i x_i\chi_i)(\sum_j x_j\chi_{\bar{j}}) \\ &= \sum_{i,j} x_ix_j\chi_i\chi_{\bar{j}} \end{aligned}$$

By Lemma 7.5.11, the coefficient of χ_1 in the representation of $uS^*(u)$ as a rational linear combination of $\chi_1, \ldots, \chi_n$ is $\sum_i x_i^2 \neq 0$, so $uS^*(u) \neq 0$. Since $C_{\mathbf{Q}}(H)$ is finite dimensional, to end the proof we only need to show that $C_{\mathbf{Q}}(H)$ does not have nonzero nilpotents. Indeed, if z were a nonzero nilpotent, let $v = zS^*(z)$. The above remark shows that $v \neq 0$, and clearly $S^*(v) = v$. Then $v^2 = vS^*(v) \neq 0$, and continuing by induction we obtain that $v^{2^m} \neq 0$ for any positive integer m. But z lies in the Jacobson radical of $C_{\mathbf{Q}}(H)$, and then so does v. In particular v is itself a nilpotent, a contradiction. ∎

Exercise 7.5.13 *Let $C \simeq M^c(m,k)$ be a matrix coalgebra and $x \in C$ such that $\sum x_1 \otimes x_2 = \sum x_2 \otimes x_1$. Then there exists $\alpha \in k$ such that $x = \alpha\chi_C$.*

Proposition 7.5.14 *If H is a semisimple Hopf algebra and $\lambda \in H^*$ an integral with $\lambda(1) = 1$, then $\chi(H) = \sum_{1\leq i\leq n} d_i\chi_i = \dim(H)\lambda$.*

Proof: Let $\lambda = \sum_{1\leq i\leq n} \lambda_i$, with $\lambda_i \in C_i$ for any i. Since $\Delta(\lambda) = T\Delta(\lambda)$ (by Exercise 7.4.7), and $\Delta(\lambda_i) \in C_i \otimes C_i$, we see that $\Delta(\lambda_i) = T\Delta(\lambda_i)$ for any i. According to Exercise 7.5.13, we must have $\lambda_i = \alpha_i\chi_{C_i} = \chi_i$ for some $\alpha_i \in k$. If Λ^* is an integral in H^{**} such that $\Lambda^*(\varepsilon) \neq 0$, then for any j we have that

$$\begin{aligned} \Lambda^*(\varepsilon)\alpha_j &= \sum_{1\leq i\leq n} \alpha_i\Lambda^*(\chi_iS^*(\chi_{\bar{j}})) \text{ (orthogonality relations)} \\ &= \Lambda^*(\lambda S^*(\chi_{\bar{j}}) \\ &= \Lambda^*(S^*(\lambda)S^*(\chi_{\bar{j}}) \text{ (since } S^*(\lambda) = \lambda) \\ &= \Lambda^*(S^*(\chi_{\bar{j}}\lambda) \\ &= \Lambda^*(\chi_{\bar{j}}(1)\lambda) \\ &= d_{\bar{j}}\Lambda^*(\lambda) \\ &= d_j\Lambda^*(\lambda) \text{ (since } d_j = d_{\bar{j}}) \end{aligned}$$

Since $\Lambda^*(\varepsilon) \neq 0$, we obtain that $\alpha_j = \frac{\Lambda^*(\lambda)}{\Lambda^*(\varepsilon)}d_j$, so then $\sum_{1\leq i\leq n} d_i\chi_i = \alpha\lambda$ for some $\alpha \in k$. Evaluating at 1 we see that

$$\alpha = \sum_{1\leq i\leq n} d_i\chi_i(1) = \sum_{1\leq i\leq n} d_i^2 = \dim(H)$$

showing the required formula. ∎

Corollary 7.5.15 *Let $\lambda \in H^*$ be an integral such that $\lambda(1) = 1$, and denote by $Z(H)$ the center of the underlying algebra of H. Then $C_k(H) = Z(H) \rightharpoonup \lambda$.*

Proof: We know that $H \simeq M_{d_1}(k) \times \ldots \times M_{d_n}(k)$. Denote by $c_1, \ldots, c_n$ the images in H of the identity matrices in $M_{d_1}(k), \ldots, M_{d_n}(k)$ via this isomorphism. Then c_i acts as identity on the simple H-module V_i, and $c_i V_j = 0$ for any $j \neq i$. We obviously have $Z(H) = \oplus_{1 \leq i \leq n} k c_i$, and $\sum_{1 \leq i \leq n} c_i = 1$. Then for any $1 \leq j \leq n$, and $h \in H$ we have

$$\begin{aligned}
(c_j \rightharpoonup \lambda)(h) &= \lambda(h c_j) \\
&= (\dim(H))^{-1} \sum_{1 \leq i \leq n} d_i \chi_i(h c_j) \\
&= (\dim(H))^{-1} d_j \chi_j(h c_j) \\
&= (\dim(H))^{-1} d_j \chi_j(h) \quad (\text{since } c_j x = x \text{ for } x \in V_j)
\end{aligned}$$

so $c_j \rightharpoonup \lambda = (\dim(H))^{-1} d_j \chi_j$ for any j, and this clearly ends the proof. ∎

The following is just a reformulation of the result in Proposition 7.5.14 for the dual Hopf algebra, but we will also need it in this form.

Corollary 7.5.16 *Let $\Lambda^* \in H^{**}$ be an integral such that $\Lambda^*(\varepsilon) = 1$. Then the character of the left H^*-module H^* is* $\dim(H)\Lambda^*$. ∎

7.6 The Class Equation and applications

Lemma 7.6.1 *Let A be a semisimple $\mathbf{Q}$-algebra with basis $\{a_1, \ldots, a_n\}$ such that $a_i a_j \in \sum_{1 \leq t \leq n} \mathbf{Z} a_t$ for any i, j. Then for any field extension $\overline{\mathbf{Q}} \subseteq \mathcal{K}$, there exists an isomorphism of $\mathcal{K}$-algebras*

$$\phi : \mathcal{K} \otimes_{\mathbf{Q}} A \rightarrow \prod_{\alpha = 1, s} M_{r_\alpha}(\mathcal{K})$$

for some positive integers $s, r_1, \ldots, r_n$, such that for any $a \in A$, $\phi(1 \otimes a) = \sum_{\alpha, i, j} r_{\alpha i j} E_{\alpha i j}$ with all $r_{\alpha i j}$ algebraic integers, where for any $1 \leq \alpha \leq s$ we denoted by $(E_{\alpha i j})_{1 \leq i, j \leq r_\alpha}$ the matrix units in $M_{r_\alpha}(\mathcal{K})$.

Proof: Let K be a splitting field of the $\mathbf{Q}$-algebra A such that $\mathbf{Q} \subseteq K \subseteq \overline{\mathbf{Q}}$ and $\mathbf{Q} \subseteq K$ is a finite field extension (see for example [112, page 113]). Any finite extension of $\mathbf{Q}$ will be considered inside $\overline{\mathbf{Q}}$. Then $K \otimes_{\mathbf{Q}} A \simeq \prod_{\alpha = 1, s} M_{r_\alpha}(K)$ for some positive integers $s, r_1, \ldots, r_n$. This K-algebra isomorphism can be also written in the form $K \otimes_{\mathbf{Q}} A \simeq \prod_{\alpha=1,s} End_K(V_\alpha)$, where $V_1, \ldots, V_s$ are the isomorphism types of simple left $K \otimes_{\mathbf{Q}} A$-modules. Since K is a splitting field of A, we have that $End_K(V_\alpha) \simeq K$ for any $1 \leq \alpha \leq s$.

We show that for any simple left $K \otimes_{\mathbf{Q}} A$-module F, say of dimension r over K, there exists a basis of the $\mathcal{K}$-vector space $\mathcal{K} \otimes_K F$ such that for the associated matrix basis of $End_{\mathcal{K}}(\mathcal{K} \otimes_K F) \simeq M_r(\mathcal{K})$, any endomorphism $\gamma_a \in End_{\mathcal{K}}(\mathcal{K} \otimes_K F)$, $\gamma_a(x) = ax$, the left multiplication with the element $a \in A$, is a linear combination of the matrix basis with coefficients algebraic integers. The required isomorphism ϕ follows immediately from here.

So let us take a simple $K \otimes_{\mathbf{Q}} A$-module F. Then F is a K-vector space by $\alpha x = (\alpha \otimes 1)x$, and a left A-module by $ax = (1 \otimes a)x$, for $\alpha \in K, a \in A, x \in F$. Moreover, $\alpha(ax) = a(\alpha x)$ for such α, a, x. Let $\{h_1, \ldots, h_r\}$ be a basis of F over K. We denote by R the ring of algebraic integers of K. It is known that R is a Dedekind ring and K is its field of fractions (see for example [65, page 108]). Now we define

$$U = \sum_{\substack{1 \leq i \leq n \\ 1 \leq p \leq r}} R(a_i h_p)$$

which is an R-submodule of F. Then U is a torsionfree finitely generated R-module. Indeed, for any $u \in U$, we have $u \in F$, and then $ann_R(u) \subseteq ann_K(u) = 0$. We prove now that the morphism

$$\phi : K \otimes_R U \to F, \quad \phi(\alpha \otimes u) = \alpha u$$

is an isomorphism of K-vector spaces. It is surjective, since

$$\begin{aligned} Im(\phi) &= \sum_{i,p} KRa_i h_p \\ &= \sum_{i,p} Ka_i h_p \\ &= \sum_{p} (K \otimes_{\mathbf{Q}} A) h_p \\ &= F \end{aligned}$$

where the last equality follows from the fact that F is a simple $K \otimes_{\mathbf{Q}} A$-module. To show that ϕ is injective, let $\phi(\sum_i \alpha_i \otimes_R x_i) = \sum_i \alpha_i x_i = 0$, for some $\alpha_i \in K$, $x_i \in U$. Since K is the field of fractions of R, there exists a nonzero $N \in R$ (in fact even $N \in \mathbf{Z}$) such that $N\alpha_i \in R$ for any i. Then

$$\sum_i \alpha_i \otimes_R x_i = \sum_i N^{-1} N\alpha_i \otimes_R x_i$$

$$\begin{aligned} &= \sum_i N^{-1} \otimes_R N\alpha_i x_i \\ &= N^{-1} \otimes_R N(\sum_i \alpha_i x_i) \\ &= 0 \end{aligned}$$

Then U is a projective R-module, since it is finitely generated torsionfree over the Dedekind ring R (see [65, Theorem 22.5]). In particular U is R-flat, so $R \otimes_R U$ embeds naturally in $K \otimes_R U$. Obviously, $\phi(R \otimes_R U) = U$. The structure theorem of finitely generated torsionfree modules over a Dedekind ring ([65, Theorem 22.5]) tells that there exist $(w_q)_{1\leq q\leq r} \subseteq U$ and fractional ideals $(I_q)_{1\leq q\leq r}$ of R (i.e. finitely generated R-submodules of K) such that $R\otimes_R U = \oplus_{1\leq q\leq r} I_q(1\otimes w_q)$, an internal direct sum of R-submodules. Since ϕ is an isomorphism of R-modules, we have that

$$U = \phi(R \otimes_R U) = \oplus_{1\leq q\leq r} I_q w_q$$

an internal direct sum of R-submodules. Note that since I_q is not necessarily contained in R, and U is just an R-module, the product $I_q w_q$ makes sense only if we regard everything inside F, which is a K-vector space. However, $I_q w_q \subseteq U$ for any q. A classical result for Dedekind rings ([65, Theorem 20.14]) ensures us that there exists a finite extension $K \subseteq K'$, with the ring of algebraic integers of K' denoted by R', such that all the extensions of the fractional ideals I_q to K' are principal, i.e. there exist $(\sigma_q)_{1\leq q\leq r} \subseteq K'$ such that $R'I_q = R'\sigma_q$ for any q. K' is also a splitting field of A and the simple modules over $K' \otimes_{\mathbf{Q}} A$ are obtained from the simple modules over $K' \otimes_{\mathbf{Q}} A$ by extending scalars from K to K'. We extend all the construction from K to K'. Thus we take $F' = K' \otimes_K F$, which is a simple $K' \otimes_{\mathbf{Q}} A$-module by $(\alpha' \otimes a)(\beta' \otimes x) = \alpha'\beta' \otimes ax$ for any $\alpha', \beta' \in K'$, $a \in A$, $x \in F$. A basis of F' over K' is $\{1 \otimes h_p | 1 \leq p \leq r\}$. We construct U' inside F' in a way similar to the construction of U inside F, i.e.

$$U' = \sum_{i,p} R'a_i(1 \otimes_K h_p) = \sum_{i,p} R'(1 \otimes a_i h_p)$$

On the other hand

$$F' = K' \otimes_K F \simeq K' \otimes_K K \otimes_R U \simeq K' \otimes_R U$$

The above isomorphism $\psi : K' \otimes_R U \to F'$ is given by $\psi(\alpha' \otimes_R x) = \alpha' \otimes_K x$ for any $\alpha' \in K'$ and $x \in F$. It is easily checked that $\psi(R' \otimes_R U) = U'$. This implies that

$$\begin{aligned} U' &= \psi(R' \otimes_R (\oplus_{1\leq q\leq r} I_q w_q)) \\ &= \psi(\oplus_q (R' \otimes_R I_q w_q)) \\ &= \oplus_q \psi(R' \otimes_R I_q w_q) \end{aligned}$$

Since $R'I_q = R'\sigma_q$, it is easy to see that $\psi(R' \otimes_R I_q w_q) = R'(\sigma_q \otimes_K w_q)$. We obtain that $U' = \oplus_q R'(\sigma_q \otimes_K w_q)$, a direct sum of R'-submodules. It follows that the elements $(u_q)_{1\leq q\leq r}$ are linearly independent over R' (note that the annihilators of these elements are zero, since we work inside the K'-vector space F'), and then they are obviously linearly independent over K' (inside F'), thus forming a basis of F' over K'. Moreover, for any $1 \leq j \leq n$ we have that $a_jU' \subseteq U'$. Indeed, if $r' \in R'$, $1 \leq i \leq n$ and $1 \leq p \leq r$, then $a_ja_i = \sum_{1\leq t\leq n} z_ta_t$ from the hypotesis on the basis $(a_i)_i$ of A, and then

$$\begin{aligned} a_j(r' \otimes_K a_ih_p) &= r' \otimes_K a_ja_ih_p \\ &= \sum_t r' \otimes_K z_ta_th_p \\ &= \sum_t r'z_t \otimes_K a_th_p \end{aligned}$$

thus $a_jU' \subseteq U'$. Since $U' = \oplus_q R'u_q$, we obtain that $a_ju_q = \sum_t r'_tu_t$ for some $(r'_t)_t \subseteq R'$. This means that for the basis $(u_q)_{1\leq q\leq r}$ of the K'-vector space F', the endomorphisms $\gamma_a \in End_{K'}(F')$ given by multiplication with elements $a \in A$, can be expressed as linear combinations of the matrix basis of $End_{K'}(F')$ associated to $(u_q)_{1\leq q\leq r}$ with algebraic integer coefficients. Obviously, this fact can be extended by scalars to any field extension of K', in particular to $\mathcal{K}$ (since $\mathbf{Q} \subseteq K \subseteq K' \subseteq \overline{\mathbf{Q}} \subseteq \mathcal{K}$). ∎

We apply the previous lemma for $A = C_{\mathbf{Q}}(H)$ and $\mathcal{K} = k$, where H is a semisimple Hopf algebra over the algebraic closed field k. We find that there exist some positive integers $s, r_1, \ldots, r_n$ and an isomorphism of k-algebras $\phi : k \otimes_{\mathbf{Q}} A \rightarrow \prod_{\alpha=1,s} M_{r_\alpha}(k)$ such that for any $a \in A$, $\phi(1 \otimes a) = \sum_{\alpha,i,j} r_{\alpha ij}E_{\alpha ij}$ with all $r_{\alpha ij}$ algebraic integers, where for any $1 \leq \alpha \leq s$ we denoted by $(E_{\alpha ij})_{1\leq i,j\leq r_\alpha}$ the matrix units in $M_{r_\alpha}(k)$. Let $\phi_1 : C_k(H) \simeq k \otimes_{\mathbf{Q}} (H)$ the natural isomorphism of k-algebras which takes χ_i to $1 \otimes \chi_i$ for any i (Corollary 7.5.8). Then by denoting $e_{\alpha ij} = \phi_1^{-1}\phi^{-1}(E_{\alpha ij}) \in C_k(H)$, for any $1 \leq \alpha \leq s, 1 \leq i,j \leq r_\alpha$, we obtain a family $(e_{\alpha ij})_{\alpha,i,j}$ such that

$$e_{\alpha ij}e_{\beta uv} = \delta_{\alpha\beta}\delta_{ju}e_{\alpha iv}$$

for any $\alpha, \beta, i, j, u, v$, and $\varepsilon = \sum_{\alpha,i} e_{\alpha ii}$. In particular $(e_{\alpha ii})_{\alpha,i}$ is a complete system of orthogonal primitive idempotents of $C_k(H)$. Also, for any $1 \leq u \leq n$

$$\chi_u = \sum_{\alpha,i,j} r_{u,\alpha ij}e_{\alpha ij}$$

for some algebraic integers $(r_{u,\alpha ij})_{\alpha,i,j}$.

If we denote by $tr : H^* \rightarrow k$ the character of the left H^*-module H^*, we have that $tr(e_{\alpha ii})$ is a positive integer for any α and i. Indeed, since $e_{\alpha ii}$ is an idempotent, the left multiplication by $e_{\alpha ii}$ is an idempotent endomorphism of H^*, so it is diagonalizable and has eigenvalues either 0 or 1, and not all of them 0 (since $e_{\alpha ii} \neq 0$). Then $tr(e_{\alpha ii})$, which is the trace of this endomorphism is a positive integer. On the other hand, for any α and any $i \neq j$, $tr(e_{\alpha ij}) = 0$, since $e_{\alpha ij} = e_{\alpha ii}e_{\alpha ij} - e_{\alpha ij}e_{\alpha ii}$, and $tr(xy) = tr(yx)$ for any $x, y \in H^*$.

Exercise 7.6.2 *Show that for any idempotent* $e \in H^*$, $tr(e) = \dim(eH^*)$. *This provides another way to see that* $tr(e_{\alpha ii})$ *is a positive integer.*

Theorem 7.6.3 *For any* $1 \leq \alpha \leq s$ *and* $1 \leq i \leq r_\alpha$, *the integer* $tr(e_{\alpha ii})$ *divides* $\dim(H)$.

Proof: Let $\Lambda^* \in H^{**}$ be an integral such that $\Lambda^*(\varepsilon) = 1$. We know that $tr = \dim(H)\Lambda^*$ (Corollary 7.5.16). This shows that for any α and any $i \neq q$ we have $\Lambda^*(e_{\alpha iq}) = \frac{1}{\dim(H)} tr(e_{\alpha iq}) = 0$. We use the orthogonality relations and obtain that for any $1 \leq u, v \leq n$

$$\begin{aligned}
\delta_{uv} &= \Lambda^*(\chi_u S^*(\chi_v)) \\
&= \Lambda^*(\chi_u \chi_{\overline{v}}) \\
&= \Lambda^*(\sum_{\alpha,\beta,i,j,p,q} r_{u,\alpha ij} r_{\overline{v},\alpha pq} e_{\alpha ij} e_{\beta pq}) \\
&= \sum_{\alpha,i,j,q} r_{u,\alpha ij} r_{\overline{v},\alpha jq} \Lambda^*(e_{\alpha iq}) \\
&= \sum_{\alpha,i,j} r_{u,\alpha ij} r_{\overline{v},\alpha ji} \Lambda^*(e_{\alpha ii}) \\
&= \sum_{\alpha,i,j} (r_{u,\alpha ij} \sqrt{\Lambda^*(e_{\alpha ii})})(r_{\overline{v},\alpha ji} \sqrt{\Lambda^*(e_{\alpha ii})})
\end{aligned}$$

Let $I = \{1, \ldots, n\}$ and $J = \{(\alpha, i, j) | 1 \leq \alpha \leq s, 1 \leq i, j \leq r_\alpha\}$. Then I and J are sets with n elements and the above relation can be written using matrices as $XY = Id$, where

$$X = (x_{u,\alpha ij})_{u \in I, (\alpha,i,j) \in J} \in M_{I,J}(k) \text{ and } Y = (y_{\alpha ij,u})_{(\alpha,i,j) \in J, u \in I} \in M_{J,I}(k)$$

are matrices defined by

$$x_{u,\alpha ij} = r_{u,\alpha ij} \sqrt{\Lambda^*(e_{\alpha ii})}, \quad y_{\alpha ij,u}) = r_{\overline{u},\alpha ji} \sqrt{\Lambda^*(e_{\alpha ii})})$$

Thus X is an invertible $n \times n$-matrix and Y is its inverse matrix. Then YX is also the identity matrix, in particular for any α and i we have that

$1 = \sum_u y_{\alpha ii,u} x_{u,\alpha ii}$. This means that

$$1 = \sum_u r_{\overline{u},\alpha ii} r_{u,\alpha ii} \Lambda^*(e_{\alpha ii})$$

In particular $\frac{1}{\Lambda^*(e_{\alpha ii})} = \sum_u r_{\overline{u},\alpha ii} r_{u,\alpha ii}$ is an algebraic integer.
On the other hand, using again the formula $tr = \dim(H)\Lambda^*$ we find

$$\frac{1}{\Lambda^*(e_{\alpha ii})} = \frac{\dim(H)}{tr(e_{\alpha ii})}$$

is a rational number. We obtain that $\frac{1}{\Lambda^*(e_{\alpha ii})}$ is an integer, which ends the proof. ∎

Thus for a semisimple Hopf algebra H over the algebraic closed field k, with the character algebra over k

$$C_k(H) \simeq \prod_{\alpha=1,s} M_{r_\alpha}(k).$$

We have seen that $(e_{\alpha ii})_{1\leq\alpha\leq s, 1\leq i\leq r_\alpha}$ is a complete set of primitive orthogonal idempotents of $C_k(H)$, and $tr(e_{\alpha ii}) = \dim(e_i H^*)$ divides $\dim(H)$ for any α and i. Then $(e_{\alpha ii})_{1\leq\alpha\leq s, 1\leq i\leq r_\alpha}$ is a complete set of orthogonal idempotents of H^*, so $H^* = \oplus_{1\leq\alpha\leq s, 1\leq i\leq r_\alpha} e_{\alpha ii} H^*$. In particular $\dim(H) = \sum_{1\leq\alpha\leq s, 1\leq i\leq r_\alpha} \dim(e_{\alpha ii} H^*)$.

Now we are in the position to give the structure of Hopf algebras of prime dimension.

Theorem 7.6.4 *(Kac-Zhu) Let H be a Hopf algebra of prime dimension p over the algebraic closed field k. Then $H \simeq kC_p$.*

Proof: If $p = 2$, the result follows from Exercise 4.3.7. So we assume that p is odd. If H has a non-trivial grouplike element g, then g has order p by the Nichols-Zoeller theorem, and then $H \simeq kC_p$. Similarly, if H^* has a non-trivial grouplike element, then $H^* \simeq kC_p$, and then $H \simeq (kC_p)^* \simeq kC_p$ (see Exercise 4.3.6). If neither H nor H^* has non-trivial grouplike elements, then the distinguished grouplike elements of H and H^* are 1 and ε, and then by Theorem 7.1.6 we have $S^4 = Id$. Therefore S^2 is diagonalizable with eigenvalues 1 and -1. In particular, since p is odd, $Tr(S^2) \neq 0$, so by Theorem 7.4.1, H is semisimple.
Use the complete system of orthogonal idempotents $(e_{\alpha ii})_{1\leq\alpha\leq s, 1\leq i\leq r_\alpha}$ of H^*, to see that $p = tr(\varepsilon) = \sum_{1\leq\alpha\leq s, 1\leq i\leq r_\alpha} tr(e_{\alpha ii})$. Also, by Theorem 7.6.3, each $tr(e_{\alpha ii})$ divides p, so it is either 1 or p. If $tr(e_{\alpha ii}) = p$ for

some α and i, then $s = 1$ and $r_1 = 1$, since any $tr(e_{\alpha ii})$ is nonzero. In particular $\dim(C_k(H)) = 1$, i.e. H has only one simple module, so H is a matrix algebra. This is impossible since a non-trivial matrix algebra does not have a Hopf algebra structure. It follows that all $tr(e_{\alpha ii})$ are 1, and that their number is p. This implies that $p = \sum_{1\leq\alpha\leq s} r_\alpha$. But $\sum_{1\leq\alpha\leq s} r_\alpha^2 = \dim(C_k(H)) \leq \dim(H) = p$, so we must have $\dim(C_k(H)) = p$, i.e. $C_k(H) = H^*$, and $r_\alpha = 1$ for any $1 \leq \alpha \leq s$. Then $H^* = C_k(H) \simeq k\times k\times\ldots\times k$ (p of k). Then H is isomorphic to a group algebra by Exercise 4.3.8. ∎

We have used as ingredients in the proof of the previous theorem the facts that the complete set $(e_{\alpha ii})_{1\leq\alpha\leq s, 1\leq i\leq r_\alpha}$ of primitive orthogonal idempotents of $C_k(H)$ satisfies $\dim(H) = \sum_{1\leq\alpha\leq s,1\leq i\leq r_\alpha} \dim(e_{\alpha ii}H^*)$, and each $\dim(e_{\alpha ii}H^*) = tr(e_{\alpha ii})$ divides $\dim(H)$. We show that these relations are satisfied by any complete system of primitive orthogonal idempotents of $C_k(H)$.

Theorem 7.6.5 *(The Class Equation). Let H be a semisimple algebra over the algebraic closed field k, and $(e_i)_{1\leq i\leq m}$ be a complete set of primitive orthogonal idempotents of $C_k(H)$. Then $\dim(H) = \sum_{1\leq i\leq m}\dim(e_iH^*)$ and $\dim(e_iH^*)$ divides $\dim(H)$ for any $1 \leq i \leq m$. Moreover, $\dim(e_iH^*) = 1$ for some i.*

Proof: Since a complete system $(e_i)_{1\leq i\leq m}$ of primitive orthogonal idempotents of $C_k(H)$ provides a decomposition $C_k(H) = \oplus_{1\leq i\leq m} e_iC_k(H)$ of indecomposable right $C_k(H)$-submodules, for any other such system $(f_i)_{1\leq i\leq m'}$, we must have $m = m'$ and $e_1C_k(H),\ldots,e_mC_k(H)$ are pairwise isomorphic as right $C_k(H)$-modules to $f_1C_k(H),\ldots,f_mC_k(H)$. This implies that $e_1H^*,\ldots,e_mH^*$ are pairwise isomorphic as right H^*-modules to $f_1H^*,\ldots,f_mH^*$ (see next exercise). Thus $\dim(e_1H^*),\ldots,\dim(e_mH^*)$ are pairwise equal to $\dim(f_1H^*),\ldots,\dim(f_mH^*)$.
The first part of the statement follows now from the existence of a complete system of primitive orthogonal idempotents satisfying the required relations, namely $(e_{\alpha ii})_{1\leq\alpha\leq s,1\leq i\leq r_\alpha}$.
For the second part, if $\lambda \in H^*$ is an integral with $\lambda(1) = 1$, we know that $\lambda \in C_k(H)$ (Proposition 7.5.14), and since $\lambda^2 = \lambda(1)\lambda = \lambda$, we see that λ is an idempotent of $C_k(H)$. Moreover, it is a primitive idempotent, since $\dim(\lambda H^*) = 1$, and then $\dim(\lambda C_k(H)) = 1$. ∎

Exercise 7.6.6 *Let A be a k-subalgebra of the k-algebra B, and e, e' idempotents of A such that $eA \simeq e'A$ as right A-modules. Then $eB \simeq e'B$ as right B-modules.*

Theorem 7.6.7 *Let H be a semisimple Hopf algebra of dimension p^n over the algebraic closed field k, where p is a prime and n a positive integer. Then H contains a non-trivial central grouplike element.*

Proof: Let $\lambda \in H^*$ an integral such that $\lambda(1) = 1$. If we take a complete system $(e_i)_{1 \leq i \leq m}$ of primitive orthogonal idempotents of $C_k(H)$ such that $e_1 = \lambda$, then the Class Equation can be written as

$$p^n = 1 + \sum_{2 \leq i \leq m} \dim(e_i H^*).$$

Since any $\dim(e_i H^*)$ divides $\dim(H) = p^n$, we see that there exists some $i \geq 2$ such that $\dim(e_i H^*) = 1$, thus $e_i H^* = k e_i$. The structure of the 1-dimensional ideals of H^* shows that there exists a grouplike element g in H such that $e_i = \alpha g \rightharpoonup \lambda$ for some $\alpha \in k$. Since $i \geq 2$, g is non-trivial (otherwise $e_i = \lambda = e_1$). On the other hand, Corollary 7.5.15 shows that g must be central. ∎

Corollary 7.6.8 *Let p be a prime number. Then a semisimple Hopf algebra of dimension p^2 over an algebraic closed field of characteristic zero is isomorphic as a Hopf algebra either to $k[C_p \times C_p]$ or to kC_{p^2}.*

Proof: Let H be semisimple of dimension p^2. Theorem 7.6.7 guarantees the existence of a central grouplike element $g \in H$. If g has order p^2, then the group of grouplike elements of H has order p^2, and then $H \simeq kC_{p^2}$. If g has order p, then let K be the Hopf subalgebra generated by g, this is the group algebra of a group of order p. Since g is central in H, K is contained in the center of H, in particular it is a normal Hopf subalgebra, and then we can form the Hopf algebra H/K^+H. Moreover, by Theorem 7.2.11, $H \simeq K\sharp_\sigma H/K^+H$ as algebras, for some crossed product of K and H/K^+H. In particular $dim(H/K^+H) = p$, and then by Theorem 7.6.4 $H/K^+H \simeq kC_p$. Since K is central in H, the weak action of H/K^+H on K is trivial (see Remark 6.4.13), so H is a twisted product of K and H/K^+H. By Exercise 7.6.9 below, we see that H must be commutative. Since H is semisimple and commutative, we see that as an algebra H is a product of copies of k. Now Exercise 4.3.8 shows that $H \simeq (kG)^*$ for some group G with p^2 elements. Since such a G is either $C_p \times C_p$ or C_{p^2}, and in both cases kG is selfdual, we obtain the result. ∎

Exercise 7.6.9 *Show that if the algebra A is commutative, then a twisted product of A and kC_p is commutative.*

7.7 The Taft-Wilson Theorem

Lemma 7.7.1 *Let D be a finite dimensional pointed coalgebra, E a subcoalgebra of D and $\pi : E \to E_0$ a coalgebra morphism such that $\pi \circ i = Id$, where $i : E_0 \to E$ is the inclusion map. Then π can be extended to a coalgebra morphism $\pi' : D \to D_0$ such that $\pi' i' = Id$, where $i' : D_0 \to D$ is the inclusion map.*

Proof: Since π is a coalgebra morphism, $Ker(\pi)$ is a coideal of E, and then also a coideal of D, and we can consider the factor coalgebra $F = D/Ker(\pi)$. Let $p : D \to F$ be the natural projection and $\phi = p \circ i' : D_0 \to F$. We have that

$$\begin{aligned} Ker(\phi) &= D_0 \cap Ker(\pi) \\ &= D_0 \cap E \cap Ker(\pi) \\ &= E_0 \cap Ker(\pi) \\ &= 0 \end{aligned}$$

so ϕ is injective. By Exercise 5.5.2, $Im(\phi) = p(D_0) = F_0$. Then $\phi^* : F^* \to D_0^*$ is a surjective morphism of algebras and $Ker(\phi^*) = F_0^\perp = J(F)^*$. We have that $F^*/J(F^*) = F^*/F_0^\perp \simeq F_0^*$, which is a finite direct product of copies of k as an algebra, so it is a separable algebra. By Wedderburn-Malcev Principal Theorem [183, page 209] there exists a subalgebra A of F^* such that $F^* = J(F^*) \oplus A$ as k-vector spaces. Then $A \simeq F^*/J(F^*) \simeq D_0^*$ as algebras, so there exists an algebra morphism $\gamma : D_0^* \to F^*$ such that $\phi^* \circ \gamma = Id_{D_0^*}$. Since D_0 and F are finite dimensional, there exists a coalgebra morphism $\psi : F \to D_0$ such that $\gamma = \psi^*$. Then $\phi^* \circ \psi^* = Id_{D_0^*}$, so $\psi \circ \phi = Id_{D_0}$. Then $\pi' = \psi \circ p : D \to D_0$ is a coalgebra morphism extending π, and $\pi' \circ i' = \psi \circ p \circ i' = \psi \circ \phi = Id_{D_0}$. ∎

Theorem 7.7.2 *Let C be a pointed Hopf algebra. Then there exists a coideal I of C such that $C = I \oplus C_0$.*

Proof: Let $\mathcal{F}$ be the set of all pairs (D, π), where D is a subcoalgebra of C and $\pi : D \to D_0$ is a coalgebra morphism such that $\pi \circ i = Id_{D_0}$, where $i : D_0 \to D$ is the inclusion map. $\mathcal{F}$ is non-empty since $(C_0, Id_{C_0}) \in \mathcal{F}$. The set $\mathcal{F}$ is ordered by $(D, \pi) \leq (D', \pi')$ if $D \subseteq D'$ and π is the restriction of π' to D. It is easy to check that the ordered set $(\mathcal{F}, \leq)$ is inductive, and then by Zorn's Lemma one gets a maximal element (D, π) of $\mathcal{F}$. If $D \neq C$, let $c \in C - D$, and let B be the subcoalgebra generated by c. The restriction of π to $B \cap D$ induces a surjective coalgebra morphism $\pi_1 : B \cap D \to (B \cap D)_0$ such that $\pi_1 \circ i_1 = Id_{(B\cap D)_0}$, where $i : (B \cap D)_0 \to B \cap D$ is the inclusion map. Apply Lemma 7.7.1 and extend π_1 to $\pi' : D \to D_0$

such that $\pi' \circ i' = Id_{D_0}$, where $i' : D_0 \to D$ is the inclusion map. Then π and π' produce a coalgebra morphism $\gamma : D + B \to (D + B)_0 = D_0 + B_0$ such that $\gamma \circ j = Id_{D_0+B_0}$, where $j : D_0 + B_0 \to D + B$ is the inclusion map. Since $(D + B, \gamma) \in \mathcal{F}$ and $(D, \pi) < (D + B, \gamma)$, we find a contradiction. Thus $D = C$, which ends the proof. ∎

Let C be a coalgebra. For any $p \in C^*$ we denote by $l(p), r(p) : C \to C$ the maps defined by $l(p)(c) = p \rightharpoonup c = \sum p(c_2)c_1$ and $r(p)(c) = c \leftharpoonup p = \sum p(c_1)c_2$ for any $c \in C$. Clearly $l(p)$ is a morphism of right C^*-modules, since C is a C^*-bimodule. Then $l(p)$ is a morphism of left C-comodules, so

$$(I \otimes l(p)) \circ \Delta = \Delta \circ l(p) \tag{7.25}$$

Similarly $r(p)$ is a morphism of right C-comodules, so

$$(r(p) \otimes I) \circ \Delta = \Delta \circ r(p) \tag{7.26}$$

For any $p, q \in C^*, c \in C$ we have that

$$\begin{aligned}
(l(p) \otimes r(q)) \circ \Delta(c) &= \sum l(p)(c_1) \otimes r(q)(c_2) \\
&= \sum p(c_2)q(c_3)c_1 \otimes c_4 \\
&= \sum (pq)(c_2)c_1 \otimes c_3 \\
&= \sum c_1 \otimes r(pq)(c_2) \\
&= ((I \otimes r(pq)) \circ \Delta)(c)
\end{aligned}$$

and also

$$\begin{aligned}
(l(p) \otimes r(q)) \circ \Delta(c) &= \sum (pq)(c_2)c_1 \otimes c_3 \\
&= \sum l(pq)(c_1) \otimes c_2 \\
&= ((l(pq) \otimes I) \circ \Delta)(c)
\end{aligned}$$

We have obtained that

$$(l(p) \otimes r(q)) \circ \Delta = (I \otimes r(pq)) \circ \Delta = (l(pq) \otimes I) \circ \Delta \tag{7.27}$$

Lemma 7.7.3 *Let $E \subseteq C^*$ be a family of idempotents such that $\sum_{e \in E} e = \varepsilon$, i.e. for any $c \in C$ the set $\{e \in E | e(c) \neq 0\}$ is finite and $\sum_{e \in E} e(c) = \varepsilon(c)$. Then*

$$\Delta \circ l(p) \circ r(q) = \sum_{e \in E} ((r(q) \circ l(e)) \otimes (l(p) \circ r(e))) \circ \Delta$$

for any $p, q \in C^*$.

Proof: The condition $\sum_{e\in E} e = \varepsilon$ shows that $\sum_{e\in E} r(e) = \sum_{e\in E} l(e) = I$, the identity map of C. We have that

$$\begin{aligned}\sum_{e\in E}(l(e)\otimes r(e))\circ\Delta &= \sum_{e\in E}(I\otimes r(e^2))\circ\Delta \text{ (by (7.27))}\\ &= \sum_{e\in E}(I\otimes r(e))\circ\Delta \text{ (e is an idempotent)}\\ &= (I\otimes I)\circ\Delta\\ &= \Delta\end{aligned}$$

Then

$$\begin{aligned}\Delta\circ l(p)\circ r(q) &= (I\otimes l(p))\circ\Delta\circ r(q) \text{ (by (7.25))}\\ &= (I\otimes l(p))\circ(r(q)\otimes I)\circ\Delta \text{ (by (7.26))}\\ &= (r(q)\otimes l(p))\circ\Delta\\ &= \sum_{e\in E}(r(q)\otimes l(p))\circ(l(e)\otimes r(e))\circ\Delta\\ &= \sum_{e\in E}((r(q)\circ l(e))\otimes(l(p)\circ r(e)))\circ\Delta\end{aligned}$$

∎

Let C be a pointed coalgebra with coradical $C_0 = kG$ and I a coideal of C such that $C = I\oplus C_0$. For any $x\in G$ we consider the element $p_x\in C^*$ such that $p_x(I) = 0$ and $p_x(y) = \delta_{xy}$ for any $y\in G$. Then $E = \{p_x | x\in G\}$ is a system of orthogonal idempotents with $\sum_{x\in G} p_x = \varepsilon$. Let us denote

$$c^y = p_y \rightharpoonup c,\ {}^xc = c\leftharpoonup p_x,\ {}^xc^y = p_y\rightharpoonup c\leftharpoonup p_x$$

Lemma 7.7.3 shows that

$$\Delta({}^xc^y) = \sum_{z\in G} {}^xc_1^z\otimes {}^zc_2^y \tag{7.28}$$

for any $c\in C$, $x, y\in G$. If we denote ${}^xC^y = \{{}^xc^y | c\in C\}$, then $C = \oplus_{x,y\in G}\, {}^xC^y$ since E is a complete system of orthogonal idempotents. For any subspace S of C we denote $S^+ = S\cap Ker(\varepsilon)$.

Lemma 7.7.4 *(i) If $x\neq y$, then $({}^xC^y)^+ = {}^xC^y$.*
(ii) If $x\in G$, then ${}^xC^x = ({}^xC^x)^+\oplus kx$.

Proof: Let $c\in C$ and $x, y\in G$. Then

$$\varepsilon({}^xc^y) = \varepsilon(\sum p_x(c_1)p_y(c_3)c_2)$$

$$\begin{aligned} &= \sum p_x(c_1)\varepsilon(c_2)p_y(c_3) \\ &= \sum p_x(c_1)p_y(c_2) \\ &= (p_xp_y)(c) \end{aligned}$$

and this is 0 when $x \neq y$ and $p_x(c)$ when $x = y$. This shows that (i) holds, and since $x = {}^x x^x$, that $\varepsilon({}^x x^x) = p_x(x) = 1$. Thus the sum $kx + ({}^x C^x)^+$ is direct and it is contained in ${}^x C^x$.
If $c \in C$, then $\varepsilon({}^x c^x - p_x(c)x) = p_x(c) - p_x(c) = 0$, so

$${}^x c^x = p_x(c)x + ({}^x c^x - p_x(c)x) \in kx + ({}^x C^x)^+$$

and (ii) follows. ∎

Lemma 7.7.5 *(i)* $I = \cap_{x\in G} Ker(p_x)$ *and* $p_y \rightharpoonup I \subseteq I, I \leftharpoonup p_x \subseteq I$ *for any* $x, y \in G$.
(ii) $({}^x C^y)^+ \subseteq I$ *for any* $x, y \in G$.
(iii) $I = \oplus_{x,y\in G}({}^x C^y)^+$.

Proof: (i) Clearly $I \subseteq \cap_{x\in G} Ker(p_x)$. Let $c \in \cap_{x\in G} Ker(p_x)$, and write $c = d + \sum_{x\in G} \alpha_x x$ for some $d \in I$ and scalars $\alpha_x \in k$. Then for any $g \in G$ we have $0 = p_x(c) = \alpha_x$, so $c = d \in I$. Thus $I = \cap_{x\in G} Ker(p_x)$.
If $c \in I$ we have that $\Delta(c) \in C \otimes I + I \otimes C$, and then $c \leftharpoonup p_x = \sum p_x(c_1)c_2 \in I$. Thus $I \leftharpoonup p_x \subseteq I$. Similarly $p_y \rightharpoonup I \subseteq I$.
(ii) Let $x \neq y$ and $c \in {}^x C^y = ({}^x C^y)^+$. Write $c = d + z$ with $d \in I$ and $z \in C_0$. Then $c = {}^x c^y = {}^x d^y + {}^x z^y = {}^x d^y \in I$.
If $x = y$, let $c \in ({}^x C^x)^+$ and write $c = d + z$ with $d \in I$ and $z \in C_0$. Then $d + z = c = {}^x c^x = {}^x d^x + {}^x z^x$, and since ${}^x z^x = \alpha x$ for some $\alpha \in k$ and ${}^x d^x \in I$, we obtain that $z = \alpha x$ and $d = {}^x d^x$. Then $0 = \varepsilon(c) = \varepsilon(d) + \alpha = \alpha$, so $c = d \in I$.
(iii) We have that

$$C = \oplus_{x,y\in G}\, {}^x C^y = (\oplus_{x,y\in G}({}^x C^y)^+) \oplus (\oplus_{x\in G} kx) = C_0 \oplus (\oplus_{x,y\in G}({}^x C^y)^+)$$

Since $\oplus_{x,y\in G}({}^x C^y)^+ \subseteq I$ by (ii), and $C = I \oplus C_0$, we obtain that $I = \oplus_{x,y\in G}({}^x C^y)^+$. ∎

Denote $I_n = C_n \cap I$. Since $C = I \oplus C_0$ and $C_0 \subseteq C_n$ for any n, we have that $C_n = (C_n \cap I) \oplus C_0 = I_n \oplus C_0$.

Lemma 7.7.6 *For any* n *we have* $I_n = \oplus_{x,y\in G}(I_n \cap ({}^x C^y)^+) = \oplus_{x,y\in G}(C_n \cap ({}^x C^y)^+)$.

Proof: We clearly have that $I_n \cap ({}^x C^y)^+ = C_n \cap ({}^x C^y)^+$ for any n. If $c \in I_n$ and $c = \sum_{x,y\in G} c_{x,y}$ with $c_{x,y} \in ({}^x C^y)^+$, then $c_{x,y} = p_y \rightharpoonup c \leftharpoonup p_x \in C_n$

since C_n is a subcoalgebra, so then $c_{x,y} \in C_n \cap ({}^xC^y)^+$ for any x, y, proving the claim. ∎

Let g and h be two grouplike elements of C. An element $c \in C$ is called a (g,h)-primitive element if $\Delta(c) = c \otimes g + h \otimes c$. The set of all (g,h)-primitive elements is denoted by $P_{g,h}(C)$. Obviously $g - h \in P_{g,h}(C)$.

Theorem 7.7.7 *(The Taft-Wilson Theorem) Let C be a pointed coalgebra with coradical $C_0 = kG$. Then the following assertions hold.*
1) If $n \geq 1$, then for any $c \in C_n$ there exists a family $(c_{g,h})_{g,h\in G} \subseteq C$ with finitely many nonzero elements, such that $c = \sum_{g,h\in G} c_{g,h}$ and for any $g, h \in G$ there exists $w \in C_{n-1} \otimes C_{n-1}$ with

$$\Delta(c_{g,h}) = c_{g,h} \otimes g + h \otimes c_{g,h} + w$$

2) If for any $g, h \in G$ we choose a linear complement $P'_{g,h}(C)$ of $k(g-h)$ in $P_{g,h}(C)$, then $C_1 = kG \oplus (\oplus_{g,h\in G} P'_{g,h}(C))$.

Proof: 1) Since $C_n = C_0 \oplus (\oplus_{x,y\in G}(C_n \cap ({}^xC^y)^+))$ and $\Delta(C_0) \subseteq C_0 \otimes C_0$, it is enough to consider the case where $c \in C_n \cap ({}^xC^y)^+$ for some $x, y \in G$. Since $c \in C_n$ and the coradical filtration is a coalgebra filtration (Exercise 3.1.11) we see that

$$\Delta(c) \in \sum_{i=0,n} C_i \otimes C_{n-i} \subseteq I_n \otimes C_0 + C_0 \otimes I_n + C_{n-1} \otimes C_{n-1}$$

so

$$\Delta(c) = \sum_{g\in G} c_g \otimes g + \sum_{h\in G} h \otimes d_h + \sum_i a_i \otimes b_i$$

for some $(c_g)_{g\in G} \subseteq I_n$, $(d_h)_{h\in G} \subseteq I_n$, $(a_i)_i, (b_i)_i \subseteq C_{n-1}$. Since $c = {}^xc^y$ we have that

$$\begin{aligned}
\Delta(c) &= \Delta({}^xc^y) \\
&= \sum_{z\in G} {}^xc_1^z \otimes {}^zc_2^y \\
&= \sum_{g,z\in G} {}^xc_g^z \otimes {}^zg^y + \sum_{h,z\in G} {}^xh^z \otimes {}^zd_h^y + \sum_{i,z} {}^xa_i^z \otimes {}^zb_i^y \\
&= {}^xc_y^y \otimes y + x \otimes {}^xd_x^y + \gamma
\end{aligned}$$

where $\gamma = \sum_{i,z} {}^xa_i^z \otimes {}^zb_i^y \in C_{n-1} \otimes C_{n-1}$ since $p_g \rightharpoonup C_{n-1} \subseteq C_{n-1}$ and $C_{n-1} \leftharpoonup p_h \subseteq C_{n-1}$ for any $g, h \in G$. Therefore

$$\Delta(c) = {}^xc_y^y \otimes y + x \otimes {}^xd_x^y + \gamma \tag{7.29}$$

By the counit property and the fact that $\varepsilon(I) = 0$ we find that $c = {}^x c_y^y + u$ for some $u \in C_{n-1}$ and $c = {}^x d_x^y + v$ for some $v \in C_{n-1}$. Replacing in (7.29) we obtain

$$\begin{aligned}\Delta(c) &= c \otimes y + x \otimes c + \gamma - u \otimes y - x \otimes v \\ &= c \otimes y + x \otimes c + w\end{aligned}$$

where $w = \gamma - u \otimes y - x \otimes v \in C_{n-1} \otimes C_{n-1}$.
2) We know that $C_1 = C_0 \oplus I_1$ and $I_1 = C_1 \cap I = \oplus_{x,y \in G}(C_1 \cap ({}^x C^y)^+)$. We prove that

$$P_{y,x}(C) = k(y-x) \oplus (C_1 \cap ({}^x C^y)^+) \tag{7.30}$$

Let $c \in C_1 \cap ({}^x C^y)^+$. The proof of 1) shows that

$$\Delta(c) = c \otimes y + x \otimes c + \sum_{g,h \in G} \alpha_{g,h} g \otimes h$$

for some $\alpha_{g,h} \in k$. Since $c = {}^x c^y$ we have that

$$\begin{aligned}\Delta(c) &= \Delta({}^x c^y) \\ &= c \otimes y + x \otimes c + \sum_{g,h,z \in G} \alpha_{g,h}\, {}^x g^z \otimes {}^z h^y \\ &= c \otimes y + x \otimes c + \delta_{x,y} \alpha_{x,y} x \otimes y\end{aligned}$$

Applying $I \otimes \varepsilon$ and using the fact that $\varepsilon(c) = 0$ we get $c = c + \delta_{x,y}\alpha_{x,y} y$, so $\delta_{x,y}\alpha_{x,y} = 0$. Then $\Delta(c) = c \otimes y + x \otimes c$, i.e. $c \in P_{y,x}(C)$, proving an inclusion in (7.30).
For the converse inclusion let $c \in P_{y,x}(C)$, i.e. $\Delta(c) = c \otimes y + x \otimes c$. For any $g, h \in G$ we have

$$\begin{aligned}\Delta({}^g c^h) &= \sum_z {}^g c^z \otimes {}^z y^h + \sum_z {}^g x^z \otimes {}^z c^h \\ &= \delta_{h,y}\, {}^g c^y \otimes y + \delta_{g,x} x \otimes {}^x c^h \\ &= \delta_{h,y}\, {}^g c^h \otimes y + \delta_{g,x} x \otimes {}^g c^h\end{aligned}$$

If $h \neq y$ and $g \neq x$ we obtain $\Delta({}^g c^h) = 0$, so ${}^g c^h = 0$.
If $h = y$ and $g \neq x$, then $\Delta({}^g c^y) = {}^g c^y \otimes y$, so by applying $\varepsilon \otimes I$ we see that ${}^g c^y \in ky$.
If $h \neq y$ and $g = x$, then $\Delta({}^x c^h) = x \otimes {}^x c^h$, so similarly ${}^x c^h \in kx$.
If $h = y$ and $g = x$ we find ${}^x c^y \in P_{y,x}(C)$.
Taking into account all these cases and the fact that $c = \sum_{g,h \in G} {}^g c^h$, we find $c = {}^x c^y + \alpha x + \beta y$ for some $\alpha, \beta \in k$. Since both c and ${}^x c^y$ are in $P_{y,x}(C)$ we obtain that $\alpha x + \beta y \in P_{y,x}(C)$. But $\alpha x + \beta y = \alpha(x - y) + (\alpha + \beta) y$, so

$(\beta+\alpha)y \in P_{y,x}(C)$. Since y is a grouplike element, this implies $\beta+\alpha=0$. Thus $c=\alpha(x-y)+{}^xc^y$. Obviously $\varepsilon({}^xc^y)=0$ since ${}^xc^y \in C_1 \cap P_{y,x}$, so $c \in k(x-y)+C_1 \cap ({}^xC^y)^+$, and equation (7.30) is proved. Then we have

$$C_1 = C_0 \oplus (\oplus_{x,y\in G}(C_1 \cap ({}^xC^y)^+)) = C_0 + \sum_{x,y\in G} P_{y,x}(C)$$

If $P_{g,h}(C) = k(g-h) \oplus P'_{g,h}(C)$, we have

$$C_1 = C_0 + \sum_{g,h\in G} (k(g-h) + P'_{g,h}(C)) = C_0 + \sum_{g,h\in G} P'_{g,h}(C)$$

We show that the sum $C_0 + \sum_{g,h\in G} P'_{g,h}(C)$ is direct. Indeed, let $c \in C_0$ and $d_{g,h} \in P'_{g,h}(C)$ for any $g,h \in G$, such that $c+\sum_{g,h\in G} d_{g,h}=0$. Since

$$P'_{g,h}(C) \subseteq P_{g,h}(C) = k(g-h) \oplus (C_1 \cap ({}^gC^h)^+)$$

we have $d_{g,h} = \alpha_{g,h}(g-h)+b_{g,h}$ with $b_{g,h} \in C_1 \cap ({}^gC^h)^+$ and $\alpha_{g,h} \in k$. Then we have

$$c + \sum_{g,h\in G} \alpha_{g,h}(g-h) + \sum_{g,h\in G} b_{g,h} = 0$$

and from the fact that $C_1 = C_0 \oplus (\oplus_{g,h\in G}(C_1 \cap ({}^gC^h)^+))$ we see that $b_{g,h}=0$ for any $g,h \in G$. Then we obtain $d_{g,h} = \alpha_{g,h}(g-h)$ and since $P'_{g,h}(C) \cap k(g-h) = 0$ we must have $d_{g,h}=0$ for any g,h. Hence $c=0$, so the sum is direct, and this ends the proof. ∎

Exercise 7.7.8 *Let H be a finite dimensional pointed Hopf algebra with $dim(H) > 1$. Show that $|G(H)| > 1$.*

The next exercise contains an application of the Taft-Wilson Theorem. Recall that if R is a subring of S, the extension $R \subset S$ is called a finite *subnormalizing* (or *triangular*) extension if there exist elements $x_1, \ldots, x_n \in S$ such that $S = \sum_{i=1}^{n} Rx_i$ and for any $1 \le j \le n$ we have $\sum_{i=1}^{j} Rx_i = \sum_{i=1}^{j} x_iR$ (see [241] or [121]). Then we have

Exercise 7.7.9 *Let H be a finite dimensional pointed Hopf algebra acting on the algebra A. Show that $A\#H$ is a finite subnormalizing extension of A.*

7.8 Pointed Hopf algebras of dimension p^n with large coradical

Let p be a prime integer and $n \ge 2$ an integer. Let G be a group of order p^{n-1}, $g \in Z(G)$ an element in the center of G, and assume that there exists a linear character α of G such that $\alpha(g)$ is a primitive p-th root of unity. The linear map $\phi : kG \to kG$ defined by $\phi(h) = \alpha(h)h$ for any $h \in G$, is an automorphism of the group algebra kG, thus we can form the Ore extension $kG[X,\phi]$, this is $Xh = \phi(h)X = \alpha(h)hX$ for any $h \in G$. Then using the universal property for Ore extensions (Lemma 5.6.4), the usual Hopf algebra structure of kG can be extended to a Hopf algebra structure of $kG[X,\phi]$ by setting

$$\Delta(X) = g \otimes X + X \otimes 1,\ \varepsilon(X) = 0$$

As $\alpha(g)^p = 1$, it is easy to see that the ideals (X^p) and $(X^p - g^p + 1)$ are Hopf ideals of $kG[X,\phi]$. Hence we define the factor Hopf algebras

$$H_1(G,g,\alpha) = kG[X,\phi]/(X^p) \text{ and } H_2(G,g,\alpha) = kG[X,\phi]/(X^p - g^p + 1)$$

As in Section 5.6, we see that $H_1(G,g,\alpha)$ is a pointed Hopf algebra of dimension p^n, with coradical kG. Also, if we require the extracondition that $\alpha^p = \varepsilon$, then $H_2(G,g,\alpha)$ is a pointed Hopf algebra of dimension p^n, with coradical kG (see Proposition 5.6.14). The Hopf algebra $H_1(G,g,\alpha)$ can be presented by generators x and the grouplike elements $h, h \in G$, subject to relations

$$x^p = 0,\ xh = \alpha(h)hx \text{ for any } h \in G$$

$$\Delta(x) = g \otimes x + x \otimes 1, \varepsilon(x) = 0$$

For the presentation of $H_2(G,g,\alpha)$ we just replace the relation $x^p = 0$ by $x^p = g^p - 1$. Obviously $H_1(G,g,\alpha) \simeq H_2(G,g,\alpha)$ in the case where $g^p = 1$. In both cases the coradical filtration is the degree filtration in x, and $P_{1,h}$ is not contained in kG if and only if $h = g$. The following result shows that the two types of Hopf algebras described above are essentially different.

Lemma 7.8.1 *Assume that $g'^p \neq 1$. Then the Hopf algebras $H_1(G,g,\alpha)$ and $H_2(G,g',\alpha')$ are not isomorphic.*

Proof: If the two Hopf algebras were isomorphic, let $f : H_2(G,g',\alpha') \to H_1(G,g,\alpha)$ be an isomorphism. Then $f(g')$ must be g, as the unique grouplike with non-trivial $P_{1,g}$. Then $f(x) \in P_{1,g}$, thus $f(x) = \gamma(g-1) + \delta x$ for some scalars γ and δ. Apply f to $xg' = \alpha'(g')g'x$, and find that γ must be 0. Then apply f to $x^p = g'^p - 1$, and find $\delta^p x^p = g^p - 1$. This shows that $g^p = 1$, and thus $g'^p = 1$, a contradiction. ∎

Theorem 7.8.2 *Let H be a pointed Hopf algebra of dimension p^n, p prime, such that $G(H) = G$ is a group of order p^{n-1}. Then there exist $g \in Z(g)$ and a linear character $\alpha \in G^*$ such that $\alpha(g)$ is a primitive p-th root of unity and $H \simeq H_1(G,g,\alpha)$ or $H \simeq H_2(G,g,\alpha)$ (for the second type the condition $\alpha^p = \varepsilon$ must be satisfied).*

Proof: The Taft-Wilson Theorem shows that there is a $g \in G$ such that $\dim(P_{1,g}) \geq 2$. Since $g^{p^{n-1}} = 1$, the conjugation by g is an endomorphism of $P_{1,g}$ whose minimal polynomial has distinct roots. Therefore it has a basis of eigenvectors, and moreover, we may assume that this basis contains $g-1$. Let x be another element of the basis, x an eigenvector corresponding to the eigenvalue λ. If $\lambda = 1$, then $xg = gx$ and $\Delta(x) = g \otimes x + x \otimes 1$, so then the subalgebra of H generated by g and x is a Hopf subalgebra, and this is commutative, hence cosemisimple. We find that $x \in Corad(H) = kG$, a contradiction. Thus we must have $\lambda \neq 1$, which implies that λ is a primitive root of 1 of order p^e, for some $e \geq 1$.

Now we prove by induction on $1 \leq a \leq p^e - 1$ that the set $S_a = \{ hx^i \mid h \in G, 0 \leq i \leq a \}$ is linearly independent. For $a = 1$, this follows from the Taft-Wilson Theorem. Assume that S_{a-1} is linearly independent, and say that

$$\sum_{\substack{h \in G \\ 0 \leq i \leq a}} \alpha_{h,i} h x^i = 0 \tag{7.31}$$

for some scalars $\alpha_{h,i}$. Since $\Delta(x) = g \otimes x + x \otimes 1$, and $(x \otimes 1)(g \otimes x) = \lambda(g \otimes x)(x \otimes 1)$, we can use the quantum binomial formula, and get

$$\Delta(x^i) = \sum_{0 \leq s \leq i} \binom{i}{s}_\lambda g^{i-s} x^s \otimes x^{i-s} \tag{7.32}$$

Apply Δ to (7.31), then using (7.32) we see that

$$\sum_{\substack{h \in G \\ 0 \leq i \leq a}} \sum_{0 \leq s \leq i} \binom{i}{s}_\lambda \alpha_{h,i} h g^{i-s} x^s \otimes h x^{i-s} = 0 \tag{7.33}$$

Fix some $h_0 \in H$. Since S_{a-1} is linearly independent, there exist $\phi, \psi \in H^*$ such that $\phi(h_0 g^{a-1} x) = 1$, $\phi(hx^i) = 0$ for any $(h,i) \neq (h_0 g^{a-1}, 1)$, $\psi(h_0 x^{a-1}) = 1$, and $\psi(hx^i) = 0$ for any $(h,i) \neq (h_0, a-1)$. Applying $\phi \otimes \psi$ to (7.33), we find that $\binom{a}{1}_\lambda \alpha_{h_0,a} = 0$. As $a \leq p^e - 1$, we have $\binom{a}{1}_\lambda \neq 0$, thus $\alpha_{h_0,a} = 0$. Now the induction hypothesis shows that all $\alpha_{h,i}$ are zero, therefore S_a is linearly independent.
But $|S_{p^e-1}| = p^{n-1+e}$ shows that e must be 1, and S_{p-1} is a basis of H.

We prove now that $H_1 = kG + \sum_{h \in G} P_{h,hg}$ and $P_{h,hg} = k(hg - h) + khx$ for any $h \in G$. Let $z = \sum_{\substack{h \in G \\ 0 \leq i \leq a}} \alpha_{h,i} h x^i \in H_1$. Then as in (7.33) we have

$$\sum_{\substack{h \in G \\ 0 \leq i \leq a}} \sum_{0 \leq s \leq i} \binom{i}{s}_\lambda \alpha_{h,i} h g^{i-s} x^s \otimes h x^{i-s} \in H_0 \otimes H + H \otimes H_0$$

Note that $(hg^{i-s}, s, h, i-s) = (h'g^{i'-s'}, s', h', i'-s')$ if and only if $s = s', i = i'$ and $h = h'$. Then for $i \geq 2$, take $s = 1$, and $hg^{i-s}x^s \otimes hx^{i-s}$ has the coefficient $\alpha_{h,i}\binom{i}{1}_\lambda$ in $\Delta(z)$. On the other hand, since $\Delta(z) \in H_0 \otimes H + H \otimes H_0$, this coefficient must be zero, thus $\alpha_{h,i} = 0$. Therefore $z \in kG + \sum_{h\in G} khx$, which is what we want.

In particular, the only $P_{u,v}$ not contained in kG are $P_{h,hg}$, $h \in G$. On the other hand, $xh \in P_{h,gh}$, thus $P_{h,gh}$ is not contained in kG. Thus we must have $gh = hg$ for any $h \in G$, i.e. $g \in Z(G)$. Also, $xh \in k(hg-h)+khx$. Thus there exist $\alpha(h) \in k^*, \beta(h) \in k$ such that $xh = \alpha(h)hx + \beta(h)(gh-h)$. We have that

$$\begin{aligned} xgh &= \lambda gxh \\ &= \lambda g(\alpha(h)hx + \beta(h)(gh-h)) \\ &= \lambda\alpha(h)ghx + \lambda\beta(h)g(gh-h) \end{aligned}$$

and

$$\begin{aligned} xhg &= (\alpha(h)hx + \beta(h)(gh-h))g \\ &= \alpha(h)\lambda hgx + \beta(h)(gh-h)g \end{aligned}$$

showing that $\beta(h) = 0$. Now $xh = \alpha(h)hx$ for any $h \in H$, thus α is a linear character of G.

Finally, taking the p^{th} powers in $\Delta(x) = g\otimes x + x\otimes 1$, we obtain $\Delta(x^p) = g^p \otimes x^p + x^p \otimes 1$. Since $g^p \neq g$, this implies that $x^p \in P_{1,g^p} = k(g^p - 1)$. If $x^p = 0$, then $H \simeq H_1(G, g, \alpha)$. If $x^p = \beta(g^p - 1)$ for some nonzero scalar β, then by the change of variables $y = \beta^{1/p}x$ (k is algebraically closed) we see that $H \simeq H_1(G, g, \alpha)$. ∎

Corollary 7.8.3 *Let k be an algebraically closed field of characteristic zero and p a prime number. Then a pointed Hopf algebra of dimension p^2 over k is isomorphic either to a group algebra or to a Taft algebra.* ∎

Let p be a prime. Then a group of order p or p^2 is abelian, therefore in order to find examples of non-cosemisimple pointed Hopf algebras of dimension p^n with non-abelian coradical, we need $n \geq 4$. We first investigate dimension p^4, and the possibility of the coradical to be the group algebra of a non-abelian group of order p^3.

Proposition 7.8.4 *Let H be a pointed Hopf algebra of dimension p^4, p prime. Then either H is a group algebra or $G(H)$ is abelian.*

Proof: It is enough to show that there do not exist Hopf algebras of dimension p^4 with coradical the group algebra of a non-abelian group of order p^3. If we assume that such a Hopf algebra H exists, then the structure result given in Theorem 7.8.2 shows that there exist $g \in Z(G(H))$ and a linear character α of $G(H)$ such that $\alpha(g)$ is a primitive p-th root of unity. There exist two types of non-abelian groups with p^3 elements. The first one is G_1, with generators a and b, subject to

$$a^{p^2} = 1,\ b^p = 1,\ bab^{-1} = a^{1+p}$$

In this case $Z(G_1) =< a^p >$, and if $\alpha \in G_1^*$, then the relation $bab^{-1} = a^{1+p}$ shows that $\alpha(a^p) = 1$, thus $\alpha(g) = 1$ for any $g \in Z(G_1)$.
The second type is G_2, which is generated by a, b, c, subject to

$$a^p = b^p = c^p = 1,\ ac = ca,\ bc = cb,\ ab = bac$$

Then $Z(G_2) =< c >$, and again the relation $ab = bac$ shows that $\alpha(c) = 1$ for any $\alpha \in G_2^*$. Thus $\alpha(g) = 1$ for any $g \in Z(G_2)$, which ends the proof. ∎

It is easy to see that there exist pointed Hopf algebras of dimension p^5 with non-commutative coradical of dimension p^4. We can take for example $H = kG_1 \otimes H_{p^2}$, where H_{p^2} is a Taft Hopf algebra, and G_1 is the first type of non-abelian group of order p^3. Then H is pointed with $G(H) = G_1 \times C_p$. We can also give examples of such Hopf algebras that are not obtained by tensor products as above.

Example 7.8.5 i) Let M be the group of order p^4 generated by a and b, subject to relations

$$a^{p^3} = 1,\ b^p = 1,\ ab = ba^{1+p^2}$$

Then $Z(M) =< a^p >$. Let λ be a primitive root of unity of order p^2. Then $\alpha(a) = \lambda$ and $\alpha(b) = 1$ define a linear character of M, and $\alpha(a^p)$ is a primitive root of unity of order p. We thus have a Hopf algebra $H(M, a^p, \alpha)$ with the required conditions.
ii) Let E be the group of order p^4 generated by a and b, subject to relations

$$a^{p^2} = b^{p^2} = 1,\ ab = ba^{1+p}$$

Then $Z(E) =< a^p, b^p >$. Take $\alpha \in E^*$ such that $\alpha(a) = 1$ and $\alpha(b)$ is a primitive root of unity of order p^2. Then $H(E, b^p, \alpha)$ is another example as we want.

Now we show that if $C = (C_p)^{n-1} =< c_1 > \times < c_2 > \times \ldots \times < c_{n-1} >$ then a result similar to Corollary 7.8.3 holds.

Proposition 7.8.6 *If $C = (C_p)^{n-1}$ and H is a pointed Hopf algebra of dimension p^n with $G(H) = C$, then $H \simeq k(C_p)^{n-2} \otimes T$ for some Taft Hopf algebra T. Moreover, there are exactly $p - 1$ isomorphism classes of such Hopf algebras.*

Proof: We know from Theorem 7.8.2 that $H \simeq H_1(C, g, \alpha)$ for some $g \in C$ and $\alpha \in C^*$ such that $\alpha(g) \neq 1$. Regard C as a $\mathbf{Z}_p$-vector space. Then there exists a basis $g_1 = g, g_2, \dots, g_{n-1}$ of C. Since $\alpha(g) \neq 1$ we can find a basis $c_1 = g, c_2, \dots, c_{n-1}$ of C such that $\alpha(c_2) = \dots = \alpha(c_{n-1}) = 1$. Then $xc_i = c_i x$ for any $2 \leq i \leq n-1$, the Hopf subalgebra T generated by g and x is a Taft algebra and we clearly have $H \simeq k(C_p)^{n-2} \otimes T$. The second part follows from Proposition 5.6.38. ∎

Exercise 7.8.7 *Let k be an algebraically closed field of characteristic zero. Show that there exist 3 isomorphism types of Hopf algebras of dimension 4 over k: the group algebras kC_4 and $k(C_2 \times C_2)$ and Sweedler's Hopf algebra H_4.*

7.9 Pointed Hopf algebras of dimension p^3

In this section we classify pointed Hopf algebras of dimension p^3, p prime, over an algebraically closed field k. The most difficult is the case where the coradical has dimension p, which we will treat first. So let H be a Hopf algebra of dimension p^3 with $Corad(H) = kC_p$.

Lemma 7.9.1 *There exist $c \in G(H)$, $x \in H$ and λ a primitive p-th root of 1 such that $xc = \lambda cx$ and $\Delta(x) = c \otimes x + x \otimes 1$. The Hopf subalgebra T generated by c and x is a Taft Hopf algebra.*

Proof: The Taft-Wilson theorem ensures the existence of some $c \in G(H)$ such that $P_{1,c} \neq k(1-c)$. If $\phi : P_{1,c} \to P_{1,c}$ is the map defined by $\phi(a) = c^{-1}ac$ for every $a \in H$, then $\phi^p = Id$, so $P_{1,c}$ has a basis of eigenvectors for ϕ. Let x be such an eigenvector which is not in $k(1-c)$, and λ the corresponding eigenvalue. If $\lambda = 1$, then the Hopf subalgebra T generated by c and x is commutative, and hence the square of its antipode is the identity. Now T is cosemisimple by Theorem 7.4.6, $dim(T) > p$ and $Corad(H) = kC_p$, a contradiction. We conclude that $\lambda \neq 1$, which ends the proof of the first statement.
Taking the p-th power of the relation $\Delta(x) = c \otimes x + x \otimes 1$, and using the quantum binomial formula, we find that x^p is $(1,1)$-primitive. Thus $x^p = 0$ by Exercise 4.2.16. This shows that T is a Taft Hopf algebra. ∎

From now on T will be the Hopf subalgebra generated by c and x. The $(n+1)$-th term T_n in the coradical filtration of T is the subspace spanned by all $c^i x^j$ with $j \leq n$. In particular $T_{p-1} = T$.
In the sequel, we will assume that the sum over an empty family is zero.

Lemma 7.9.2 *Let $a \in H$ be such that*

$$\Delta(a) = g \otimes a + a \otimes 1 + \sum_{i=0}^{p-1}\sum_{j=0}^{n-1} v_{i,j} \otimes c^i x^j \tag{7.34}$$

for some $g \in G(H), n \leq p$ and $v_{i,j} \in H$. Then

$$\Delta(a + v_{0,0}) = g \otimes (a + v_{0,0}) + (a + v_{0,0}) \otimes 1 + \sum_{j=1}^{n-1} v_{0,j} \otimes x^j \tag{7.35}$$

and for all $1 \leq r \leq n-1$

$$\Delta(v_{0,n-r}) = g \otimes v_{0,n-r} + v_{0,n-r} \otimes c^{n-r} + \sum_{i=1}^{r-1} \binom{n-r+i}{i}_\lambda v_{0,n-r+i} \otimes c^{n-r} x^i \tag{7.36}$$

Proof: We have that

$$\begin{aligned}(\Delta \otimes I)\Delta(a) &= g \otimes g \otimes a + g \otimes a \otimes 1 + a \otimes 1 \otimes 1 + \\ &+ \sum_{i=0}^{p-1}\sum_{j=0}^{n-1} v_{i,j} \otimes c^i x^j \otimes 1 + \sum_{i=0}^{p-1}\sum_{j=0}^{n-1} \Delta(v_{i,j}) \otimes c^i x^j\end{aligned}$$

and

$$(I \otimes \Delta)\Delta(a) = g \otimes g \otimes a + g \otimes a \otimes 1 + a \otimes 1 \otimes 1 + \sum_{i=0}^{p-1}\sum_{j=0}^{n-1} g \otimes v_{i,j} \otimes c^i x^j +$$

$$+ \sum_{i=0}^{p-1}\sum_{j=0}^{n-1}\sum_{s=0}^{j} \binom{j}{s}_\lambda v_{i,j} \otimes c^{i+j-s} x^s \otimes c^i x^{j-s}.$$

Looking at the terms with 1 on the third tensor position we find

$$\sum_{i=0}^{p-1}\sum_{j=0}^{n-1} v_{i,j} \otimes c^i x^j + \Delta(v_{0,0}) = g \otimes v_{0,0} + \sum_{j=1}^{n-1} v_{0,j} \otimes x^j + v_{0,0} \otimes 1,$$

and now we obtain (7.35) since $\sum_{i=0}^{p-1}\sum_{j=0}^{n-1} v_{i,j} \otimes c^i x^j = \Delta(a) - g \otimes a - a \otimes 1$.
Looking at the terms with x^{n-r} on the third position we find (7.36). ∎

The key step is to show that there exist $(1, g)$-primitives that are not in T.

Lemma 7.9.3 $\dim(H_1) > 2p$.

Proof: Suppose $\dim(H_1) \leq 2p$. Since $T_1 \subseteq H_1$, we have $H_1 = T_1$. In particular $\dim(P_{u,v}) = 2$ only for $v = cu$.

Step 1. We prove by induction on $n \leq p-1$ that $H_n = T_n$. Assume that $H_{n-1} = T_{n-1}$ and $H_n \neq T_n$, and pick some $h \in H_n - T_n$. Write $h = \sum_{u,v \in G(H)} h_{u,v}$ as in the Taft-Wilson Theorem and pick some $h_{u,v} \in H_n - T_n$.
Denoting $g = u^{-1}v$ we have that $a = u^{-1}h_{u,v} \in H_n - T_n$ and

$$\Delta(a) = g \otimes a + a \otimes 1 + \sum_{i=0}^{p-1}\sum_{j=0}^{n-1} v_{i,j} \otimes c^i x^j$$

with $v_{i,j} \in T_{n-1}$. Let $b = a + v_{0,0} \in H_n - T_n$. 7.9.2 shows that $\Delta(v_{0,n-1}) = g \otimes v_{0,n-1} + v_{0,n-1} \otimes c^{n-1}$. If $g \neq c^n$ we have $v_{0,n-1} \in H_0$, and then $\Delta(b) \in H_0 \otimes H + H \otimes H_{n-2}$, which is a contradiction since $b \notin H_{n-1}$. Hence $g = c^n$ and $v_{0,n-1} = \alpha(c^n - c^{n-1}) + \beta c^{n-1}x$ for some $\alpha, \beta \in k, \beta \neq 0$. We have that

$$\begin{aligned}\Delta(b) - c^n \otimes b - b \otimes 1 - \alpha(c^n \otimes x^{n-1} - c^{n-1} \otimes x^{n-1}) - \\ -\beta c^{n-1}x \otimes x^{n-1} \in H \otimes H_{n-2} + H_0 \otimes H. \qquad (7.37)\end{aligned}$$

Since $(\Delta(x^{n-1}) - c^n \otimes x^{n-1} - x^{n-1} \otimes 1) + (c^n \otimes x^{n-1} - c^{n-1} \otimes x^{n-1}) \in H \otimes H_{n-2} + H_0 \otimes H$ and $(\Delta(x^n) - c^n \otimes x^n - x^n \otimes 1) - \binom{n}{1}_\lambda c^{n-1}x \otimes x^{n-1} \in H \otimes H_{n-2}$, relation 7.37 implies that $b' = b + \alpha x^{n-1} - \binom{n}{1}_\lambda^{-1} \beta x^n$ satisfies $\Delta(b') - c^n \otimes b' - b' \otimes 1 \in H \otimes H_{n-2} + H_0 \otimes H$. Therefore $b' \in H_{n-1} = T_{n-1}$ and $b \in T \cap H_n = T_n$, providing a contradiction.

Step 2. We have from Step 1 that $H_{p-1} = T_{p-1} = T \neq H_p$. Using the Taft-Wilson Theorem and 7.9.2 as in Step 1, we find some $b \in H_p - T$ with $\Delta(b) = 1 \otimes b + b \otimes 1 + \sum_{j=1}^{p-1} v_j \otimes x^j$ for some $v_j \in T$ (note that we need here $c^p = 1$). We use induction to show that for any $1 \leq m \leq p$ there exists $b_m \in H_p - T$ such that

$$\Delta(b_m) = 1 \otimes b_m + b_m \otimes 1 + \sum_{j=1}^{p-m} w_j \otimes x^j + \sum_{j=p-m}^{p-1} \alpha_j c^j x^{p-j} \otimes x^j \qquad (7.38)$$

for some $w_j \in T, \alpha_j \in k$.
For $m = 1$, we see again as in Step 1 that $v_{p-1} = \alpha(1 - c^{p-1}) + \beta c^{p-1}x$ for some $\alpha, \beta \in k, \beta \neq 0$. Observe that

$$(1 - c^{p-1}) \otimes x^{p-1} + (\Delta(x^{p-1}) - 1 \otimes x^{p-1} - x^{p-1} \otimes 1) \in \sum_{j \leq p-2} T \otimes T_j,$$

Applying (7.9.2) to $a = b + \alpha x^{p-1}$ (in the case $n = p-1$),we obtain a b_1 as wanted.

Assume that we have found b_m for some $1 \le m \le p-1$ satisfying (7.38). Applying relation (7.36) to b_m and $r = m$ we obtain

$$\begin{aligned}
\Delta(v_{0,p-m}) &= \Delta(\alpha_{p-m}c^{p-m}x^m) \\
&= \alpha_{p-m}\sum_{i=0}^{m}\binom{m}{i}_\lambda c^{p-i}x^i \otimes c^{p-m}x^{m-i} \\
&= 1 \otimes \alpha_{p-m}c^{p-m}x^m + \alpha_{p-m}c^{p-m}x^m \otimes 1 \\
&+ \sum_{i=1}^{r-1}\binom{p-m+i}{i}_\lambda \alpha_{p-m+i}c^{p-m+i}c^{p-m+i}x^{m-i} \otimes c^{p-m}x^i
\end{aligned}$$

and

$$\sum_{i=1}^{m-1}\binom{m}{i}_\lambda \alpha_{p-m}c^{p-m+i}x^{m-i} \otimes c^{p-m}x^i =$$

$$= \sum_{i=1}^{m-1}\binom{p-m+i}{i}_\lambda \alpha_{p-m+i}c^{p-m+i}x^{m-i} \otimes c^{p-m}x^i,$$

which implies that

$$\binom{m}{i}_\lambda \alpha_{p-m} = \binom{p-m+i}{i}_\lambda \alpha_{p-m+i} \tag{7.39}$$

for every $1 \le i \le m-1$. For $r = m+1$ the relation (7.36) gives

$$\Delta(w_{p-m-1}) = 1 \otimes w_{p-m-1} + w_{p-m-1} \otimes c^{p-m-1} +$$

$$+ \sum_{i=1}^{m}\binom{p-m+i-1}{i}_\lambda \alpha_{p-m+i-1}c^{p-m+i-1}x^{m-i} \otimes c^{p-m-1}x^i.$$

On the other hand we have

$$\begin{aligned}
\Delta(c^{p-m-1}x^{m+1}) &= 1 \otimes c^{p-m-1}x^{m+1} + c^{p-m-1}x^{m+1} \otimes c^{p-m-1} \\
&+ \sum_{i=1}^{m}\binom{m+1}{i}_\lambda c^{p-m+i-1}x^{m-i} \otimes c^{p-m-1}x^i.
\end{aligned}$$

We obtain the following identities after we apply (7.39) with i replaced by $i-1$ (first equality) and some elementary computation with λ-factorials (second equality).

$$\binom{p-m+i-1}{i}_\lambda \alpha_{p-m+i-1} =$$
$$= \binom{p-m+i-1}{i}_\lambda \binom{m}{i-1}_\lambda \binom{p-m+i-1}{i-1}_\lambda^{-1} \alpha_{p-m}$$
$$= \binom{p-m}{1}_\lambda \binom{m+1}{1}_\lambda^{-1} \binom{m+1}{i}_\lambda \alpha_{p-m}$$

We obtain that

$$\Delta\left(w_{p-m-1} - \binom{p-m}{1}_\lambda \binom{m+1}{1}_\lambda^{-1} c^{p-m-1}\alpha_{p-m}x^{m+1} \right) \in P_{c^{p-m-1},1}.$$

As $c^{p-m} \neq 1$ we find

$$w_{p-m-1} - \binom{p-m}{1}_\lambda \binom{m+1}{1}_\lambda^{-1} c^{p-m-1}x^{m+1} = \alpha(1-c^{p-m-1})$$

for some $\alpha \in k$. Since

$$(1-c^{p-m-1}) \otimes x^{p-m-1} + (\Delta(x^{p-m-1}) - 1 \otimes x^{p-m-1} - x^{p-m-1} \otimes 1) \in$$
$$\in \sum_{j<p-m-1} T \otimes T_j,$$

we can apply (7.9.2) to $b_m + \alpha x^{p-m-1}$ and get a b_{m+1} satisfying (7.38).

Step 3. Take a $b = b_p$ satisfying (7.38):

$$\Delta(b) = 1 \otimes b + b \otimes 1 + \sum_{j=1}^{p-1} \alpha_j c^j x^{p-j} \otimes x^j \tag{7.40}$$

It follows easily that $\Delta(bc-cb) = c \otimes (bc-cb) + (bc-cb) \otimes c$, and $bc = cb$. Also

$$\Delta(bx-xb) + (\alpha_{p-2} + \lambda^{p-1}\alpha_{p-1} - \alpha_{p-1} - \lambda^2\alpha_{p-2})x^2 \otimes x^{p-1} \in H_0 \otimes H + H \otimes H_{p-2} \tag{7.41}$$

Applying (7.39) with $i = 1, m = 2$, we obtain

$$(\lambda+1)\alpha_{p-2} = \frac{\lambda^{p-1}-1}{\lambda-1}\alpha_{p-1}$$

and

$$(\lambda^2-1)\alpha_{p-2} - (\lambda^{p-1}-1)\alpha_{p-1} = 0$$

We see that the coefficient of $x^2 \otimes x^{p-1}$ is 0 in (7.41) and $bx - xb \in H_{p-1} = T$. Clearly $\delta = bx - xb \in T^+ = T \cap \mathrm{Ker}(\varepsilon)$. The relations $bc = cb, bx - xb = \delta$ and 7.40 show that the algebra generated by c, b and x is a Hopf subalgebra of H, so it is the whole of H by the Nichols-Zoeller Theorem. They also show that $T^+ H = HT^+$, which means that T is a normal Hopf subalgebra. Hence by Theorem 7.2.11 we have an isomorphism of algebras $H \simeq T\#_\sigma H/T^+H$ (a certain crossed product). But in H/T^+H we have $\hat{c} = \hat{1}, \hat{x} = 0$ and $\hat{b}$ is $(1,1)$-primitive, thus 0. We obtain $H/T^+H \simeq k$, and then $\dim(H) = \dim(T)$, which provides a final contradiction. ∎

At this point we know that there are two different cases: $3 \leq \dim(P_{1,c})$ or there exists $g \neq c$ such that $2 \leq \dim(P_{1,g})$. In the first case let us pick some $y \in P_{1,c} - kx$ such that $yc = \mu cy$ for some primitive p-th root μ of 1 (recall that $P_{1,c}$ has a basis of eigenvectors for the conjugation by c). In the second case pick $y \in P_{1,g}$ such that $yg = \mu gy$ for some $\mu \neq 1$. Write $g = c^d$ (in the first case we will take $d = 1$).

Lemma 7.9.4 *The set $\{c^q x^i y^j \mid 0 \leq q, i, j \leq p-1\}$ is a basis of H.*

Proof: We prove by induction on $1 \leq n \leq 2p-2$ that the set $B_n = \{c^q x^i y^j \mid 0 \leq q, i, j \leq p-1 \text{ and } i+j \leq n\}$ is linearly independent. For $n = 1$ this follows from the Taft-Wilson Theorem. Suppose that B_n is linearly independent and take $\sum_{q=0}^{p-1} \sum_{i+j \leq n+1} \alpha_{q,i,j} c^q x^i y^j = 0$. Applying Δ, we find

$$\sum_{q=0}^{p-1} \sum_{i+j \leq n+1} \sum_{s=0}^{i} \sum_{t=0}^{j} \alpha_{q,i,j} \binom{i}{s}_\lambda \binom{j}{t}_\mu \lambda^{sd(j-t)} c^{q+i-s+d(j-t)} x^s y^t \otimes$$

$$\otimes c^q x^{i-s} y^{j-t} = 0$$

Fix some triple (q_0, i_0, j_0) with $i_0 + j_0 = n+1$ and assume $i_0 \neq 0$ (otherwise $j_0 \neq 0$ and we proceed in a similar way). Take $\phi \in H^*$ mapping $c^{q_0+i_0-1+dj_0} x$ to 1 and any other element of B_n to 0, and $\psi \in H^*$ mapping $c^{q_0} x^{i_0-1} y^{j_0}$ to 1 and the rest of B_n to 0. Applying $\phi \otimes \psi$, we find that $\alpha_{q_0,i_0,j_0} = 0$. Now all the $\alpha_{q,i,j}$ are zero by the induction hypothesis. ∎

Corollary 7.9.5 *B_n spans H_n for every $0 \leq n \leq 2p-2$.*

Proof: We prove by induction on $1 \leq n \leq 2p-2$ that $B_n - B_{n-1} \subseteq H_n - H_{n-1}$. This is clear for $n = 1$. For the induction step, pick $x^i y^j \in B_{n+1} - B_n$. Then

$$\Delta(x^i y^j) = \sum_{s=0}^{i} \sum_{t=0}^{j} \binom{i}{s}_\lambda \binom{j}{t}_\mu \lambda^{sd(j-t)} c^{i-s+d(j-t)} x^s y^t \otimes x^{i-s} y^{j-t} \in$$

$$\in H_0 \otimes H + H \otimes H_n,$$

and $x^i y^j \in H_{n+1}$. Assuming again that $i \neq 0$, choose $\phi, \psi \in H^*$ such that $\phi(c^{i+dj-1}x) = \psi(x^{i-1}y^j) = 1$, $\phi(B_0) = 0$ and $\psi(B_{n-1}) = 0$. Then $(\phi \otimes \psi)(H_0 \otimes H + H \otimes H_{n-1}) = 0$, while $(\phi \otimes \psi)(\Delta(x^i y^j)) = \binom{i}{1}_\lambda \lambda^{dj} \neq 0$, and this shows that $x^i y^j \notin H_n$. ∎

We define now some Hopf algebras. If λ is a primitive p-th root of 1 and $1 \leq i \leq p-1$ an integer, we denote by $H(\lambda, i)$ the Hopf algebra with generators c, x, y defined by

$$c^p = 1, \quad x^p = y^p = 0, \quad xc = \lambda cx, \quad yc = \lambda^{-i} cy, \quad yx = \lambda^{-i} xy$$

$$\Delta(c) = c \otimes c, \quad \Delta(x) = c \otimes x + x \otimes 1, \quad \Delta(y) = c^i \otimes y + y \otimes 1.$$

We also denote by $H_\delta(\lambda)$ the Hopf algebra with generators c, x, y defined by

$$c^p = 1, \quad x^p = y^p = 0, \quad xc = \lambda cx, \quad yc = \lambda^{-1} cy, \quad yx = \lambda^{-1} xy + c^2 - 1$$

$$\Delta(c) = c \otimes c, \quad \Delta(x) = c \otimes x + x \otimes 1, \quad \Delta(y) = c \otimes y + y \otimes 1.$$

Note that for $p = 2$ the only Hopf algebra of the second type, $H_\delta(-1)$, is equal to $H(-1, 1)$.

Theorem 7.9.6 *Let H be a Hopf algebra of dimension p^3 with $Corad(H) = kC_p$. Then H is isomorphic either to some $H_\delta(\lambda)$ or to some $H(\lambda, i)$.*

Proof: We first consider an odd prime p. We distinguish the following cases.

Case 1. $x, y \in P_{1,c}$. Then $yx \in H_2$, and since B_2 spans H_2 we have

$$yx = \sum_{0 \leq i \leq n-1} (\alpha_i c^i x^2 + \beta_i c^i xy + \gamma_i c^i y^2) + \delta \tag{7.42}$$

for some $\alpha_i, \beta_i, \gamma_i \in k, \delta \in H_1$. Applying Δ and replacing everywhere yx by the right hand side in (7.42), we find

$$\sum_{0 \leq i \leq n-1} (\alpha_i c^2 \otimes c^i x^2 + \beta_i c^2 \otimes c^i xy + \gamma_i c^2 \otimes c^i y^2 + \alpha_i c^i x^2 \otimes 1 + \beta_i c^i xy \otimes 1 +$$

$$+\gamma_i c^i y^2 \otimes 1) + c^2 \otimes \delta + \delta \otimes 1 + \mu cy \otimes x + cx \otimes y$$

$$= \sum_{0 \leq i \leq n-1} \alpha_i (c^{i+2} \otimes c^i x^2 + c^i x^2 \otimes c^i + \binom{2}{1}_\lambda c^{i+1} x \otimes c^i x)$$

$$+ \sum_{0 \leq i \leq n-1} \gamma_i (c^{i+2} \otimes c^i y^2 + c^i y^2 \otimes c^i + \binom{2}{1}_\mu c^{i+1} y \otimes c^i y)$$

$$+\sum_{0\le i\le n-1}\beta_i(c^{i+2}\otimes c^ixy+c^ixy\otimes c^i+c^{i+1}y\otimes c^ix+\lambda c^{i+1}x\otimes c^iy)+\Delta(\delta)$$

Since B_2 is linearly independent we get $\alpha_i=\gamma_i=0$ for all i (looking at the coefficients of $c^{i+1}x\otimes c^ix$ and $c^{i+1}y\otimes c^iy$), $\beta_i=0$ for any $i\neq 0$ (looking at the coefficient of $c^{i+2}\otimes c^ixy$), $\beta_0\lambda=1$ (looking at the coefficient of $cx\otimes y$), $\mu=\beta_0$ (looking at the coefficient of $cy\otimes x$), and $\Delta(\delta)=c^2\otimes\delta+\delta\otimes 1$. Thus $\mu=\lambda^{-1}$ and $\delta\in P_{1,c^2}=k(c^2-1)$. If $\delta=0$, then $H\simeq H(\lambda,1)$. If $\delta\neq 0$, then $H\simeq H_\delta(i)$.

Case 2. $x\in P_{1,c}$, $y\in P_{1,g}$, where $g=c^d\neq c$. Writing again yx as in (7.42) and applying Δ, we find

$$\sum_{0\le i\le n-1}(\alpha_icg\otimes c^ix^2+\beta_icg\otimes c^ixy+\gamma_icg\otimes c^iy^2+\alpha_ic^ix^2\otimes 1+\beta_ic^ixy\otimes 1+$$

$$+\gamma_ic^iy^2\otimes 1)+cg\otimes\delta+\delta\otimes 1+\mu cy\otimes x+gx\otimes y$$

$$=\sum_{0\le i\le n-1}\alpha_i(c^{i+2}\otimes c^ix^2+c^ix^2\otimes c^i+\binom{2}{1}_\lambda c^{i+1}x\otimes c^ix)+$$

$$+\sum_{0\le i\le n-1}\gamma_i(c^ig^2\otimes c^iy^2+c^iy^2\otimes c^i+\binom{2}{1}_\mu c^igy\otimes c^iy)+$$

$$+\sum_{0\le i\le n-1}\beta_i(c^{i+1}g\otimes c^ixy+c^ixy\otimes c^i+c^{i+1}y\otimes c^ix+\lambda^dc^igx\otimes c^iy)+\Delta(\delta)$$

Since B_2 is linearly independent we obtain that $\alpha_i=\gamma_i=0$ for any i, $\beta_i=0$ for any $i\neq 0$,
$\beta_0=\mu$, $\lambda^d\beta_0=1$ and $\Delta(\delta)=\delta\otimes 1+cg\otimes\delta$. Thus $\mu=\lambda^{-d}$ and $\delta\in P_{1,c^{d+1}}=k(c^{d+1}-1)$.
If $\delta=0$, then $H\simeq H(\lambda,i)$. If $\delta\neq 0$, then

$$yxc=(\beta_0xy+\delta)c=\beta_0\mu xcy+\delta c=\lambda\beta_0\mu cxy+\delta c,$$

and

$$yxc=\lambda ycx=\lambda\mu cyx=\lambda\mu c(\beta_0xy+\delta)=\lambda\mu\beta_0cxy+\lambda\mu c\delta.$$

These show that $\lambda\mu=1$, and this implies $d=1$, which is impossible.
If $p=2$, then $x^2=y^2=0$ and $B_2=\{c^q,c^qx,c^qy,c^qxy|0\le q\le p-1\}$, so in the equation (7.42) we consider from the beginning that $\alpha_i=\gamma_i=0$, and the proof works with the same computations. ∎

The number of isomorphism types of Hopf algebras of the form $H_\delta(\lambda)$ and $H(\lambda,i)$ can be evaluated using the following.

Proposition 7.9.7
1) $H(\lambda, i) \simeq H(\mu, j)$ if and only if either $(\lambda, i) = (\mu, j)$ or $\mu = \lambda^{-i^2}$ and $ij \equiv 1 \pmod p$.
2) If p is odd, then $H_\delta(\lambda) \simeq H_\delta(\mu)$ if and only if $\lambda = \mu$.
3) If p is odd, then no one of the $H_\delta(\mu)$ is isomorphic to any $H(\lambda, i)$.

Proof: 1) We use the classification result given in Proposition 5.6.38, taking into account the fact that $H(\lambda, i) = H(C_p, (p,p), (c, c^i), (c^*, c^{*-i}))$ where $c^* \in C^*$ is such that $c^*(c) = \lambda$, while

$$H(\mu, j) = H(C_p, (p,p), (c, c^j), (d^*, d^{*-j}))$$

where $d^* \in C^*$ is such that $d^*(c) = \mu$. The permutation π as in Proposition 5.6.38 is either the identity or the transposition. In the first case, $H(\lambda, i) \simeq H(\mu, j)$ if and only if there exists h such that $c^h = c, c^{hi} = c^j$, $c^* = d^{*h}$ and $c^{*-i} = d^{*-hj}$. This implies that $h \equiv 1 (\mathrm{mod} p)$, and then $i = j$ and $\lambda = c^*(c) = d^*(c) = \mu$. In the second case $H(\lambda, i) \simeq H(\mu, j)$ if and only if there exists h such that $c^h = c^j, c^{hi} = c$, $c^* = d^{*-jh}$ and $c^{*-i} = d^{*h}$. Then h is the inverse of i modulo p, $j = h$, and $d^* = c^{*-i^2}$, and we obtain that $\mu = d^*(c) = c^{*-i^2}(c) = \lambda^{-i^2}$.
2) It follows immediately from Corollary 5.6.44.
3) It follows from Theorem 5.6.28. ∎

Corollary 7.9.8 *If p is odd, then there exist $(p-1)^2/2$ types of Hopf algebras of the form $H(\lambda, i)$ and $p-1$ types of the form $H_\delta(\lambda)$. If $p = 2$, then there is only one Hopf algebra of the form $H(\lambda, i)$, namely $H(-1, 1)$, and it is equal to $H_\delta(-1)$.*

Proof: Assume that p is odd. There exist $(p-1)^2$ Hopf algebras of the form $H(\lambda, i)$. The classification of these, given in the previous proposition, shows that any of them is isomorphic to precisely one other in this list. Indeed, if we take some $1 \le i \le p-1$ and some primitive p-th root of unity λ, then $H(\lambda, i) \simeq H(\mu, j)$ where j is the inverse of i modulo p and $\mu = \lambda^{-i^2}$. Then $(\lambda, i) \neq (\mu, j)$. Otherwise we would have that $i^2 \equiv 1 (\mathrm{mod} p)$, so then $\mu = \lambda^{-1} \neq \lambda$. We conclude that there exist $(p-1)^2/2$ isomorphism types of Hopf algebras of the form $H(\lambda, i)$. The rest is obvious. ∎

Let H be a pointed Hopf algebra of dimension p^3. We have seen (Exercise 7.7.8) that the coradical of H can not be of dimension 1. By the Nichols-Zoeller Theorem we have $\dim(Corad(H)) \in \{p, p^2, p^3\}$.

If $\dim(Corad(H)) = p$, then $Corad(H) = kC_p$, and this case was discussed.

If $\dim(Corad(H)) = p^2$, then $Corad(H) = kC_{p^2}$ or $Corad(H) = k(C_p \times C_p)$, and the classification in these cases was done in the previous section, where pointed Hopf algebras H of dimension p^n with $G(H)$ of order p^{n-1}

are classified. For every $\lambda \neq 1$ and i such that $\lambda^{p^2} = 1$ and λ^i is a primitive p-th root of 1, denote by $H_{p^2}(\lambda, i)$ is the Hopf algebra with generators c and x and

$$c^{p^2} = 1, \quad x^p = 0, \quad xc = \lambda cx$$
$$\Delta(c) = c \otimes c, \quad \Delta(x) = c^i \otimes x + x \otimes 1$$

By Proposition 5.6.38 two such Hopf algebras $H_{p^2}(\lambda, i)$ and $H_{p^2}(\mu, j)$ are isomorphic if and only if there exists h not divisible by p such that $\mu = \lambda^h$ and $i \equiv hj \pmod{p^2}$.
If λ is a primitive p-th root of 1, we denote by $\tilde{H}(\lambda)$ the Hopf algebra with generators c and x defined by

$$c^{p^2} = 1, \quad x^p = c^p - 1, \quad xc = \lambda cx$$

$$\Delta(c) = c \otimes c, \quad \Delta(x) = c \otimes x + x \otimes 1$$

Then using again Proposition 5.6.38, we see that $\tilde{H}(\lambda) \simeq \tilde{H}(\mu)$ if and only if $\lambda = \mu$. These facts imply the following.

Proposition 7.9.9 *Let H be a pointed Hopf algebra of dimension p^3 with $Corad(H) = kC_{p^2}$. Then H is isomorphic either to some $H_{p^2}(\lambda, i)$ or to a $\tilde{H}(\lambda)$, and there are $3(p-1)$ types of such Hopf algebras.* ∎

The case where $G(H) = C_p \times C_p$ follows from the more general Proposition 7.8.6.

Proposition 7.9.10 *Let H be a pointed Hopf algebra of dimension p^3 with $Corad(H) = k(C_p \times C_p)$. Then $H \simeq T_\lambda \otimes kC_p$, where T_λ is one of the Taft Hopf algebras, and there exist $p-1$ types of such Hopf algebras.* ∎

Finally, if $\dim(Corad(H)) = p^3$, then H is the group algebra of one of the following groups: $C_p \times C_p \times C_p, C_{p^2} \times C_p, C_{p^3}, G_1 = C_{p^2} \rtimes C_p, G_2 = C_p \rtimes C_{p^2}$, where G_1, G_2 are the two types of nontrivial semidirect products. We have now the complete classification of pointed Hopf algebras of dimension p^3.

Theorem 7.9.11 *Let H be a pointed Hopf algebra of dimension p^3. Then H is isomorphic to one of the following: $H_\delta(\lambda), H(\lambda, i), \tilde{H}(\lambda), T_\lambda \otimes kC_p$, where λ is a primitive p-th root of 1, $H_{p^2}(\lambda, i)$ for some $\lambda \neq 1$ and i such that $\lambda^{p^2} = 1$ and λ^i is a primitive p-th root of 1, $k(C_p \times C_p \times C_p)$, $k(C_{p^2} \times C_p)$, $k(C_{p^3})$, $k(G_1)$, $k(G_2)$.*
If p is odd, then there are $\frac{(p-1)(p+9)}{2} + 5$ such types. If $p = 2$, then there are 10 types. ∎

7.10 Solutions to exercises

Exercise 7.4.2 *Show that $l(p)^* = R(p)$ for any $p \in H^*$. In particular $Tr(l(p)) = Tr(R(p))$.*
Solution: If $q \in H^*$ and $a \in H$ we have

$$\begin{aligned}(l(p)^*(q))(a) &= (ql(p))(a)\\ &= \sum q(p(a_2)a_1)\\ &= (qp)(a)\\ &= (R(p)(q))(a)\end{aligned}$$

Exercise 7.4.3 *Show that if $S^2 = Id$ and H is cosemisimple, then x is a nonzero right integral in H.*
Solution: For any $p \in H^*$ we have

$$\begin{aligned}p(x) &= Tr(l(p))\\ &= Tr(l(1) \circ S^2 \circ l(p)) \ \ (\text{since } l(1) = S^2 = Id)\\ &= \lambda(1)p(\Lambda) \ \ (\text{by } (7.23))\\ &= p(\lambda(1)\Lambda)\end{aligned}$$

so $x = \lambda(1)\Lambda$. Since H is cosemisimple, $\lambda(1) \neq 0$, and then x is a nonzero right integral.

Exercise 7.4.7 *Let k be a field of characteristic zero and H a semisimple Hopf algebra over k. Show that a right (or left) integral t in H is cocommutative, i.e. $\sum t_1 \otimes t_2 = \sum t_2 \otimes t_1$.*
Solution: We know that H is cosemisimple and $S^2 = Id$, so the element $x \in H$ for which $p(x) = Tr(l(p))$ for any $p \in H^*$, is a right integral in H by Exercise 7.4.3. By Lemma 7.4.5, x is cocommutative.

Exercise 7.4.8 *Let k be a field of characteristic zero and H be a finite dimensional Hopf algebra over k. Show that:*
(i) If H is commutative, then $H \simeq (kG)^*$ for some finite group G.
(ii) If H is cocommutative, then $H \simeq kG$ for a finite group G.
Solution: If H is either commutative or cocommutative, then $S^2 = Id$, showing that H is semisimple and cosemisimple. For (i), if H is semisimple and commutative, then $H \simeq k \times k \times \ldots \times k$ as an algebra, and now $H \simeq (kG)^*$ for some finite group G by Exercise 4.3.8. For (ii), we apply (i) for H^*.

Exercise 7.4.9 *Let H be a finite dimensional Hopf algebra over a field of characteristic zero, and let S be the antipode of H. Show that S has odd order if and only if $H \simeq kG$, where $G = C_2 \times C_2 \times \ldots \times C_2$, and in this* *case $S = Id$, so the order of S is 1.*

Solution: We know that S is an antimorphism of coalgebras, so if it has odd order, we obtain that S is also an coalgebra morphism. Since S is bijective, this implies that H is cocommutative. Then necessarily $S^2 = Id$, and the odd order must be 1. Also, by Exercise 7.4.8 we have that $H \simeq kG$ for some group G. Since S has order 1, we must have that $g = g^{-1}$ for any $g \in G$, so then $G = C_2 \times C_2 \times \ldots \times C_2$.

Exercise 7.5.1 *Let $V, W \in_H \mathcal{M}$ be finite dimensional. Then $\chi(V \oplus W) = \chi(V) + \chi(W)$ and $\chi(V \otimes W) = \chi(V)\chi(W)$.*

Solution: If $(v_i)_{1\leq i\leq n}$ is a basis of V and $(w_j)_{1\leq j\leq m}$ is a basis of W, then we take as a basis for $V \oplus W$ the union of these two bases and obtain

$$\begin{aligned}
\chi(V \oplus W)(h) &= \sum_{1\leq i\leq n} v_i^*(hv_i) + \sum_{1\leq j\leq m} w_j^*(hw_j)\\
&= \chi(V)(h) + \chi(W)(h)
\end{aligned}$$

proving the first formula. In $V \otimes W$ we take the basis $(v_i \otimes w_j)_{i,j}$. The dual basis in $(V \otimes W)^*$ is $(v_i^* \otimes w_j^*)_{i,j}$, if we identify $(V \otimes W)^*$ with $V^* \otimes W^*$ via the natural isomorphism. Then

$$\begin{aligned}
\chi(V \otimes W)(h) &= \sum_{i,j} (v_i^* \otimes w_j^*)(h(v_i \otimes w_j))\\
&= \sum_{i,j} v_i^*(h_1 v_i) w_j^*(h_2 w_j)\\
&= \sum \chi(V)(h_1)\chi(W)(h_2)\\
&= (\chi(V)\chi(W))(h)
\end{aligned}$$

proving the second formula.

Exercise 7.5.2 *Show that for a finite dimensional $V \in_H \mathcal{M}$ we have $\chi(V^*) = S^*(\chi(V))$, where S^* is the dual map of S.*

Solution: If $(v_i)_{1\leq i\leq n}$ is a basis of V and the dual basis of V^* is $(v_i)^*_{1\leq i\leq n}$ then for any $h \in H$

$$\begin{aligned}
\chi(V^*)(h) &= \sum_i v_i^{**}(hv_i^*)\\
&= \sum_i (hv_i^*)(v_i)\\
&= \sum_i v_i^*(S(h)v_i)\\
&= \chi(V)(S(h))
\end{aligned}$$

$$\begin{aligned} &= (\chi(V) \circ S)(h) \\ &= S^*(\chi(V))(h) \end{aligned}$$

Exercise 7.5.13 *Let $C \simeq M^c(m,k)$ be a matrix coalgebra and $x \in C$ such that $\sum x_1 \otimes x_2 = \sum x_2 \otimes x_1$. Then there exists $\alpha \in k$ such that $x = \alpha\chi_C$.*
Solution: Let $(c_{ij})_{1\le i,j\le m}$ be a comatrix basis of C, and

$$x = \sum_{1\le i,j\le m} \alpha_{ij}c_{ij}$$

for some scalars α_{ij}. Then $\sum x_1 \otimes x_2 = \sum x_2 \otimes x_1$ is equivalent to

$$\sum_{1\le i,j,p\le m} \alpha_{ij}c_{ip} \otimes c_{pj} = \sum_{1\le i,j,p\le m} \alpha_{ij}c_{pj} \otimes c_{ip}$$

Looking at the coefficients of the elements of the basis $(c_{ij}\otimes c_{uv})_{1\le i,j,u,v\le m}$ of $C\otimes C$, we see that this is equivalent to $\alpha_{ij} = 0$ for any $i \ne j$ and $\alpha_{ii} = \alpha_{pp}$ for any $1 \le i,p \le m$. But this means that $x = \alpha_{11}\sum_{1\le i\le m} c_{ii} = \alpha_{11}\chi_C$.

Exercise 7.6.2 *Show that for any idempotent $e \in H^*$, $tr(e) = \dim(eH^*)$. This provides another way to see that $tr(e_{\alpha ii})$ is a positive integer.*
Solution: The endomorphism $u : H^* \to H^*$, $u(p) = ep$ for any $p \in H^*$, satisfies $Im(u) \subseteq eH^*$. This implies that $Tr(u) = Tr(u_{|eH^*})$. On the other hand, for any $p \in eH^*$ we see that $u(p) = ep = p$, thus $u_{|eH^*} = Id$, and then $Tr(u_{|eH^*}) = \dim(eH^*)$.

Exercise 7.6.6 *Let A be a k-subalgebra of the k-algebra B, and e, e' idempotents of A such that $eA \simeq e'A$ as right A-modules. Then $eB \simeq e'B$ as right B-modules.*
Solution: Let $f : eA \to e'A$ be an isomorphism of right A-modules with inverse f^{-1}. Note that $ex = x$ for any $x \in eA$, and $e'x' = x'$ for any $x' \in e'A$. Define $g : eB \to e'B$ by $g(eb) = f(e)b$ for any $b \in B$. This is correctly defined, since $eb_1 = eb_2$ implies that

$$f(e)b_1 = f(e^2)b_1 = f(e)eb_1 = f(e)eb_2 = f(e^2)b_2 = f(e)b_2$$

With the same argument we can define $g' : e'B \to eB$ by $g'(eb) = f^{-1}(e')b$ for any $b \in B$. Then

$$\begin{aligned} g'g(eb) &= g'(f(e)b) \\ &= g'(e'f(e)b) \\ &= f^{-1}(e')f(e)b \\ &= f^{-1}(e'f(e))b \\ &= f^{-1}(f(e))b \\ &= eb \end{aligned}$$

thus $g'g = Id$, and similarly $gg' = Id$. Then g provides an isomorphism of right B-modules.

Exercise 7.6.9 *Show that if the algebra A is commutative, then a twisted product of A and kC_p is commutative.*
Solution: If $A\#_\sigma H$ is a twisted product, the weak action of H on A is trivial, i.e. $h \cdot a = \varepsilon(h)a$ for any $h \in H, a \in A$. The normality condition tells us that $\sigma(1,g) = \sigma(g,1) = 1$ for any $g \in C_p$, and the cocycle condition tells that

$$\sigma(l,m)\sigma(h,lm) = \sigma(h,l)\sigma(hl,m)$$

for any $h, l, m \in C_p$. For $l = h^i$ and $m = h$, this equation becomes

$$\sigma(h^i,h)\sigma(h,h^{i+1}) = \sigma(h,h^i)\sigma(h^{i+1},h) \tag{7.43}$$

We prove by induction that $\sigma(h^i,h) = \sigma(h,h^i)$ for any i. This is clear for $i = 0$. Also, equation (7.43) shows that if $\sigma(h^i,h) = \sigma(h,h^i)$, then $\sigma(h,h^{i+1}) = \sigma(h^{i+1},h)$. Thus we have proved that $\sigma(h^i,h) = \sigma(h,h^i)$ for any $h \in C_p$ and $i \geq 0$. Since C_p is cyclic, this implies that $\sigma(g,h) = \sigma(h,g)$ for any $g, h \in C_p$. Then the multiplication of $A\#_\sigma kC_p$, given by

$$(a\#h)(b\#l) = ab\sigma(h,l)\#hl$$

for any $a, b \in A$ and $h, l \in C_p$, is commutative.

Exercise 7.7.8 *Let H be a finite dimensional pointed Hopf algebra with $dim(H) > 1$. Show that $|G(H)| > 1$.*
Solution: If $G(H)$ is trivial, then the Taft-Wilson Theorem and the fact that $P_{1,1}(H)$, the set of all primitive elements of H, consists only of 0 (by Exercise 4.2.16) show that $H_1 = H_0$. Then $H_n = H_0$ for any n, in particular $H = H_0$. Thus $H = kG(H)$, which has dimension 1, a contradiction.

Exercise 7.7.9 *Let H be a finite dimensional pointed Hopf algebra acting on the algebra A. Show that $A\#H$ is a finite subnormalizing extension of A.*
Solution: We construct by induction a basis $\{x_1, \ldots, x_n\}$ of H such that

$$\sum_{i=1}^{j} x_i A = \sum_{i=1}^{j} Ax_i$$

for $1 \leq j \leq n$ (we denote $ax = a\#x = (a\#1)(1\#x)$ and $xa = (1\#x)(a\#1)$). We put $G = G(H)$, and denote by

$$kG = C_0 \subset C_1 \subset \ldots \subset C_m = H$$

the coradical filtration on H.
Now the elements of G form a basis of C_0 and they clearly normalize A in $A\#H$. So we put $G = \{x_1, \dots, x_t\}$, and assume that a basis $\{x_1, \dots, x_r\}$ $(t \leq r)$ of C_{i-1} has been constructed such that $\sum_{i=1}^{j} x_i A = \sum_{i=1}^{j} Ax_i$, $1 \leq j \leq r$. Since $C_i = C_{i-1} \oplus \sum K_{i,\sigma,\tau}$, where

$$K_{i,\sigma,\tau} = \{x \in H \mid \Delta(x) = x \otimes \sigma + \tau \otimes x + \sum u_s \otimes v_s, \ \ u_s, v_s \in C_{i-1}\}.$$

Let $x \in K_{i,\sigma,\tau}$. By Lemma 6.1.8 we have $ah = \sum h_2(S^{-1}(h_1) \cdot a)$ for all $a \in A$, $h \in H$. So we get

$$ax = \sigma(S^{-1}(x) \cdot a) + x(\tau^{-1} \cdot a) + \sum v_s(S^{-1}(u_s) \cdot a).$$

On the other hand,

$$xa = (x \cdot a)\sigma + (\tau \cdot a)x + \sum (u_s \cdot a)v_s.$$

Thus if we put $x_{r+1} = x$, we have $Ax_{r+1} \in \sum_{j=1}^{r+1} x_j A$, and $x_{r+1}A \in \sum_{j=1}^{r+1} Ax_j$. If $C_i = C_{i-1} + kx_{r+1}$ we are done. If not, take $x_{r+2} \in K_{i,\sigma,\tau} \backslash (C_{i-1} + kx_{r+1})$, for some $\sigma, \tau \in G$, and continue as above. The process will stop when $dim(H)$ is reached.

Exercise 7.8.7 *Let k be an algebraically closed field of characteristic zero. Show that there exist 3 isomorphism types of Hopf algebras of dimension 4 over k: the group algebras kC_4 and $k(C_2 \times C_2)$ and Sweedler's Hopf algebra H_4.*
Solution: Let H be a Hopf algebra of dimension 4. If H has a simple subcoalgebra S of dimension greater than 1, then this must be a matrix coalgebra, so it has dimension at least 4. Thus $H = S$, and then the dual Hopf algebra H^* is isomorphic as an algebra to $M_2(k)$, and this is impossible by Exercise 4.1.9. We obtain that any simple subcoalgebra of H has dimension 1, i.e. H is pointed. We know from Exercise 7.7.8 that $G(H)$ is not trivial. Then $G(H)$ has order either 4, and in this case H is a group algebra, or 2, in in this case H is isomorphic to Sweedler's Hopf algebra by Corollary 7.8.3.

Bibliographical notes

The fact that the antipode of a finite dimensional Hopf algebra has finite order was proved by D. Radford [187]. E. Taft and R. Wilson gave in [225] examples of finite dimensional Hopf algebras over an arbitrary field with antipode having the order a given odd positive integer. The Nichols-Zoeller theorem was proved in [173], and answered a conjecture of I. Kaplansky [104] concerning the freeness of a finite dimensional Hopf algebra as a module over a Hopf subalgebra. Examples of an infinite Hopf algebra which is not free over a Hopf subalgebra were given by U. Oberst and H.-J. Schneider [176], H.-J. Schneider [201], and M. Takeuchi [230] (see also [149]). D. Radford proved in [188] that any pointed Hopf algebra is free over a Hopf subalgebra, and in [190] that commutative Hopf algebras are free over finite dimensional Hopf subalgebras. For the proof of Theorem 7.2.11, which is from A. Masuoka [133], we have used an old argument of Nakayama (see [149, 8.3.6, p. 136]), adapted as in [197]. In Section 7.3 we used the papers of W. Nichols [170] and R. Larson [115]. In Section 7.4 we used the papers [117, 118] of R. Larson and D. Radford, and the paper [170] of W. Nichols. The last ten years showed an increasing interest for classification problems for finite dimensional Hopf algebras over an algebraically closed field of characteristic zero. A very nice and complete survey on this is the paper [6] of N. Andruskiewitsch. Small dimensions (≤ 11) were classified by R. Williams [243] (see also D. Ştefan [214]). Dimension 12 was recently solved by S. Natale [167]. In prime dimension p, I. Kaplansky conjectured in [104] that any Hopf algebra is isomorphic to kC_p. This was proved by Y. Zhu in [247], using an argument of Kac [102]. Y. Zhu also proved a result, called the class equation (for another proof see M. Lorenz [126]), which is very useful for other classification problems. We present in Sections 7.5 and 7.6 the class equation, the classification in dimension p, and also the classification of semisimple Hopf algebras of dimension p^2. We have used the papers [102, 247], the lecture notes of H.-J. Schneider [207], and A. Masuoka's paper [139]. The problem of classifying all Hopf algebras of a given finite dimension is wide open. Apart from prime dimension and several small dimensions, no other general result is known. In dimension p^2, p prime, it is conjectured that any Hopf algebra is isomorphic either to a group algebra or to a Taft algebra (some partial answer is given by N. Andruskiewitsch and H.-J. Schneider in [12]). The classification efforts have focused on two important classes: semisimple Hopf algebras and pointed Hopf algebras. About these two classes, we should remark that the theory of semisimple Hopf algebras parallels in some sense the theory of finite groups, while pointed Hopf algebras have a geometric flavour. D. Ştefan proved that there are only finitely many isomorphism types of semisimple Hopf algebras of a given finite dimension [213], while we have seen in Section 5.6 that the number of types of pointed Hopf algebras of a given finite dimension may be infinite. Several results on the classification of semisimple Hopf algebras have been obtained by A. Masuoka [136, 137, 138, 139, 140], S. Gelaki and

S. Westreich [87], P. Etingof and S. Gelaki [81], S. Natale [165, 166], N. Fukuda [84] and Y. Kashina [105]. A survey paper is S. Montgomery [153]. For the classification of pointed Hopf algebras, a fundamental result is the Taft-Wilson theorem, given in [223]. We give the proof presented in S. Montgomery's book [149], which uses techniques of D. Radford [192, 193]. A new proof was given by N. Andruskiewitsch and H.-J. Schneider in [18]. Exercise 7.7.9 is taken from [64], and the solution was suggested by D. Quinn. In Section 7.8 we present the classification of pointed Hopf algebras of dimension p^n, p prime, with coradical of dimension p^{n-1}. We follow the paper [66] of S. Dăscălescu, with techniques similar to the one in M. Beattie, S. Dăscălescu, L, Grünenfelder [26]. The same result was proved by N. Andruskiewitsch and H.-J. Schneider in [15]. A more general result about pointed Hopf algebras with coradical of prime index was proved by M. Graña [91]. For the classification of pointed Hopf algebras of dimension p^3 we used the paper [45] of S. Caenepeel and S. Dăscălescu. The same result is proved in N. Andruskiewitsch, H.-J. Schneider [13], and D. Ştefan, F. Van Oystaeyen [215]. Other classification results in the pointed case have been given by N. Andruskiewitsch and H.-J. Schneider in [14, 15, 16], S. Caenepeel and S. Dăscălescu [46], S. Caenepeel, S. Dăscălescu and Ş. Raianu [47], M. Graña [89, 90], I. Musson [155], D. Ştefan [212], etc.
If the field is not algebraically closed, the classification of Hopf algebras is much more difficult. Even in dimension 3 (where for an algebraically closed field of characteristic zero the only isomorphism type is kC_3) it was shown in S. Caenepeel, S. Dăscălescu and L. le Bruyn [48] that there exist infinitely many isomorphism types of Hopf algebras of dimension 3 over certain fields of characteristic zero.
Finally, we mention two aspects which we did not include in this book, since it was not our aim to go too deep in classification problems for finite dimensional Hopf algebras. For the classification of semisimple Hopf algebras a central role is played by the theory of extensions of Hopf algebras. The reader is referred for this to [208], [5], [7], [98], [135], [130], [205]. Among the approaches to classification of pointed Hopf algebras, the technique which has proved to be the most powerful is the lifting method invented by N. Andruskiewitsch and H.-J. Schneider. However, we did not include it in this book since several technical concepts are necessary. We refer for this to the papers [6] and [17].

Appendix A

The category theory language

A.1 Categories, special objects and special morphisms

A category $\mathcal{C}$ consists of a *class* of objects (which we simply call the objects of $\mathcal{C}$; if A is an object of this class, we simply write $A \in \mathcal{C}$), such that:
for any pair (A, B) of objects of $\mathcal{C}$, a set $Hom_{\mathcal{C}}(A, B)$ is given (also denoted $Hom(A, B)$ if there is no danger of confusion), whose elements are called the *morphisms* from A to B,
for any $A \in \mathcal{C}$ there is a distinguished element 1_A (or I_A) of $Hom_{\mathcal{C}}(A, A)$, and for any $A, B, C \in \mathcal{C}$ there exists a map (composition)

$$Hom_{\mathcal{C}}(A, B) \times Hom_{\mathcal{C}}(B, C) \longrightarrow Hom_{\mathcal{C}}(A, C),$$

associating to the pair (f, g), where $f \in Hom_{\mathcal{C}}(A, B)$ and $g \in Hom_{\mathcal{C}}(B, C)$, an element of $Hom_{\mathcal{C}}(A, C)$, denoted by $g \circ f$, such that the following properties are satisfied.
i) Composition is associative, in the sense that if $f \in Hom_{\mathcal{C}}(A, B)$, $g \in Hom_{\mathcal{C}}(B, C)$ and $h \in Hom_{\mathcal{C}}(C, D)$, then $h \circ (g \circ f) = (h \circ g) \circ f$.
ii) $f \circ 1_A = f$ and $1_B \circ f = f$ for any $f \in Hom_{\mathcal{C}}(A, B)$.
iii) The sets $Hom_{\mathcal{C}}(A, B)$ and $Hom_{\mathcal{C}}(A', B')$ are disjoint whenever $(A, B) \neq (A', B')$.

We also write $f : A \to B$ instead of $f \in Hom_{\mathcal{C}}(A, B)$. The morphism 1_A is uniquely determined for a given A, and it is called the identity morphism of A.

Example A.1.1 *1) The category of sets, denoted by Set, whose class of objects is the class of all sets, and for any sets A and B, $Hom_{Set}(A, B)$ is the set of all maps from A to B. The composition is just the map composition, and 1_A is the usual identity map of a set A.*
2) The category of topological spaces, denoted by Top. The objects are all topological spaces, and for any topological spaces X and Y, $Hom_{Top}(X, Y)$ is the set of continuous functions from X to Y. The composition is again the map composition and the identity morphism is the usual identity map.
3) If R is a ring, then the category of left R-modules, denoted by ${}_R\mathcal{M}$, has the class of objects all left R-modules, and for any left R-modules M and N, $Hom_{{}_R\mathcal{M}}(M, N)$, which is usually denoted by $Hom_R(M, N)$, is the set of the morphisms of R-modules from M to N. The composition and the identity morphisms are as in Set. Similarly, one can define the category $\mathcal{M}_R$ of right R-modules. In particular, if k is a field, ${}_k\mathcal{M}$ is the category of k-vector spaces. Also, if $\mathbf{Z}$ is the ring of integers, then ${}_{\mathbf{Z}}\mathcal{M}$, the category of $\mathbf{Z}$-modules, is just the category of abelian groups, which is also denoted by Ab.
4) The category Gr of groups has as objects all the groups, and the morphisms are group morphisms.
5) The category Ring of rings, has as objects all the rings with identity, and the morphisms are ring morphisms which preserve the identity.

The dual category
Let $\mathcal{C}$ be an arbitrary category. We denote by $\mathcal{C}^0$ the category having the same class of objects as $\mathcal{C}$, and such that $Hom_{\mathcal{C}^0}(A, B) = Hom_{\mathcal{C}}(B, A)$ for any objects $A, B \in \mathcal{C}$. The composition of the morphisms $f \in Hom_{\mathcal{C}^0}(A, B)$ and $g \in Hom_{\mathcal{C}^0}(B, C)$ is defined to be $f \circ g \in Hom_{\mathcal{C}}(C, A) = Hom_{\mathcal{C}^0}(A, C)$. The category $\mathcal{C}^0$ is called the dual category of $\mathcal{C}$. Clearly $(\mathcal{C}^0)^0 = \mathcal{C}$. The introduction of the dual category is important since for any concept or statement in a category, there is a dual concept or statement, obtained by regarding the initial one in the dual category.

Subcategory
Let $\mathcal{C}$ be a category. By a subcategory $\mathcal{C}'$ of $\mathcal{C}$ we understand the following.
a) The class of objects of $\mathcal{C}'$ is a subclass of the class of objects of $\mathcal{C}$.
b) If $A, B \in \mathcal{C}'$, then $Hom_{\mathcal{C}'}(A, B) \subseteq Hom_{\mathcal{C}}(A, B)$.
c) The composition of morphisms in $\mathcal{C}'$ is the same as in $\mathcal{C}$.
d) 1_A is the same in $\mathcal{C}'$ as in $\mathcal{C}$ for any $A \in \mathcal{C}'$.

If furthermore $Hom_{\mathcal{C}'}(A, B) = Hom_{\mathcal{C}}(A, B)$ for any $A, B \in \mathcal{C}'$, then $\mathcal{C}'$ is called a full subcategory of $\mathcal{C}$.

Direct product of categories
Let $(\mathcal{C}_i)_{i \in I}$ be a family of categories indexed by a non-empty set I. We

define a new category $\mathcal{C}$ as follows. The objects of $\mathcal{C}$ are families $(M_i)_{i\in I}$ where $M_i \in \mathcal{C}_i$ for any $i \in I$. If $M = (M_i)_{i\in I}$ and $N = (N_i)_{i\in I}$ are two objects of $\mathcal{C}$, then

$$Hom_{\mathcal{C}}(M,N) = \{(u_i)_{i\in I} | u_i \in Hom_{\mathcal{C}_i}(M_i,N_i) \text{ for any } i \in I\}$$

If $M = (M_i)_{i\in I}$, $N = (N_i)_{i\in I}$ and $P = (P_i)_{i\in I}$ are three objects of $\mathcal{C}$, and $u = (u_i)_{i\in I} \in Hom_{\mathcal{C}}(M,N)$ and $v = (v_i)_{i\in I} \in Hom_{\mathcal{C}}(N,P)$, then the composition of u and v is defined by $v \circ u = (v_i \circ u_i)_{i\in I}$. The category $\mathcal{C}$ defined in this way is called the direct product of the family $(\mathcal{C}_i)_{i\in I}$, and it is usually denoted by $\mathcal{C} = \prod_{i\in I} \mathcal{C}_i$. If moreover we have $\mathcal{C}_i = \mathcal{D}$ for any $i \in I$, then $\prod_{i\in I} \mathcal{C}_i$ is also denoted by $\mathcal{D}^I$. If I is finite, say $I = \{1,2,\dots,n\}$, then instead of $\prod_{i\in I} \mathcal{C}_i$ we also write $\mathcal{C}_1 \times \mathcal{C}_2 \times \dots \times \mathcal{C}_n$.

Monomorphisms, epimorphisms and isomorphisms in a category
Let $\mathcal{C}$ be a category. A morphism $f : A \to B$ is called a *monomorphism* if for any object C and any morphisms $h, g \in Hom_{\mathcal{C}}(C,A)$ such that $f \circ h = f \circ g$, we have $g = h$. The morphism f is called an *epimorphism* if for any object D and any morphisms $k, l \in Hom_{\mathcal{C}}(B,D)$ such that $k \circ f = l \circ f$, we have $k = l$. The morphism f is called an *isomorphism* if there exists a morphism $g \in Hom_{\mathcal{C}}(B,A)$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$. It is easy to see that such a g is unique (when it exists), and it is called the inverse of f and denoted by $g = f^{-1}$. It is easy to check that any isomorphism is a monomorphism and an epimorphism. The converse is not true. Indeed, in the category of rings with identity the inclusion map $i : \mathbf{Z} \to \mathbf{Q}$ is a monomorphism and an epimorphism, but not an isomorphism.
The composition of any two monomorphisms (respectively epimorphisms, isomorphisms) is a monomorphism (respectively epimorphism, isomorphism). If $f : A \to B$ is a morphism in a category $\mathcal{C}$, then f is a monomorphism (epimorphism) in $\mathcal{C}$ if and only if f is an epimorphism (monomorphism) when regarded as a morphism from B to A in the dual category $\mathcal{C}^0$. Thus the notion of epimorphism is dual to the one of monomorphism.
Let us fix an object A of the category $\mathcal{C}$. If $\alpha_1 : A_1 \to A$ and $\alpha_2 : A_2 \to A$ are monomorphisms, we shall write $\alpha_1 \leq \alpha_2$ if there exists a morphism $\gamma : A_1 \to A_2$ such that $\alpha_2 \circ \gamma = \alpha_1$. Clearly, if such a γ exists, then it is unique, and it is also a monomorphism. If $\alpha_1 \leq \alpha_2$ and $\alpha_2 \leq \alpha_1$, then there exist morphisms γ and δ such that $\alpha_2 \circ \gamma = \alpha_1$ and $\alpha_1 \circ \delta = \alpha_2$, and this implies that $\delta \circ \gamma = 1_{A_1}$ and $\gamma \circ \delta = 1_{A_2}$, so γ and δ are invertible. The monomorphisms α_1 and α_2 are called equivalent if $\alpha_1 \leq \alpha_2$ and $\alpha_2 \leq \alpha_1$. The equivalence of monomorphisms is an equivalence relation, and by Zermelo's axiom we can choose a representant in any equivalence class. The resulting monomorphism is called a *subobject* of the object A. Similarly we can define the notion of a *quotient object* of A by using the concept of

epimorphism.

Initial and final object. Zero object.
If $\mathcal{C}$ is a category and I (respectively F) is an object with the property that $Hom_{\mathcal{C}}(I, A)$ (respectively $Hom_{\mathcal{C}}(A, F)$ is a set with only one element for any $A \in \mathcal{C}$, then I (respectively F) is called an initial (respectively final) object of $\mathcal{C}$. Clearly, any two initial (respectively final) objects are isomorphic.
An object $0 \in \mathcal{C}$ is called a *zero object* if it is an initial object and a final object. When exist, a zero object is unique up to an isomorphism. In this case we call a morphism $f : A \to B$ a zero morphism if it factors through 0. Each set $Hom_{\mathcal{C}}(A, B)$ has precisely one zero morphism, which we denote by 0_{AB} or simply by 0.

Equalizers
Let $\alpha, \beta : A \to B$ be two morphisms in a category C. We say that a morphism $u : K \to A$ is an *equalizer* for α and β if $\alpha \circ u = \beta \circ u$, and whenever $u' : K' \to A$ is a morphism such that $\alpha \circ u' = \beta \circ u'$, there exists a unique morphism $\gamma : K' \to K$ such that $u' = u \circ \gamma$. Clearly, if $u : K \to A$ is an equalizer for α and β then u is a monomorphism, and two equalizers of α and β are isomorphic subobjects of A. Dually, we can define the notion of *coequalizer* of two morphisms α and β, which is just the equalizer in the dual category $\mathcal{C}^0$.
Now assume that the category $\mathcal{C}^0$ has a zero object. If $\alpha : A \to B$ is a morphism in $\mathcal{C}^0$, then the equalizer (respectively the coequalizer) of α and 0 is called the *kernel* (respectively the *cokernel*) of α. The associated subobject (respectively quotient object) is denoted by $Ker(\alpha)$ (respectively $Coker(\alpha)$).
Let $\mathcal{C}$ be a category with zero object. Assume that for any morphism $\alpha : A \to B$ in $\mathcal{C}$ there exist the kernel and the cokernel of α, so we have the sequence of morphisms

$$Ker(\alpha) \xrightarrow{i} A \xrightarrow{\alpha} B \xrightarrow{\pi} Coker(\alpha)$$

where i and π are the natural morphisms. We have that i is a monomorphism and π is an epimorphism. If there exists a cokernel of i, then it is called the coimage of α, and it is denoted by $Coim(\alpha)$. Also, if a kernel of π exists, then it is called an image of α, and it is denoted by $Im(\alpha)$. By the universal properties of the kernel and cokernel, there exists a unique morphism $\overline{\alpha} : Coim(\alpha) \to Im(\alpha)$ such that $\alpha = \mu \circ \overline{\alpha} \circ \lambda$, where λ and μ are the natural morphisms.

Products and coproducts
Let $\mathcal{C}$ be a category and $(M_i)_{i \in I}$ be a family of objects of $\mathcal{C}$. A *product* of the

family is an object which we denote by $\prod_{i\in I} M_i$, together a family of morphisms $(\pi_i)_{i\in I}$, where $\pi_j : \prod_{i\in I} M_i \to M_j$ for any $j \in I$, such that for any object $M \in \mathcal{C}$, and any family of morphisms $(f_i)_{i\in I}$, where $f_j : M \to M_j$ for any $j \in I$, there exists a unique morphism $f : M \to \prod_{i\in I} M_i$ such that $\pi_i \circ f = f_i$ for any $i \in I$. If it exists, the product of the family is unique up to isomorphism. In the case where I is a finite set, say $I = \{1, 2, \ldots, n\}$, the product is also denoted by $M_1 \times M_2 \times \ldots \times M_n$. The categories *Set*, *Gr*, *Ring*, ${}_R\mathcal{M}$, *Top* have products. Dually, one defines the notion of *coproduct* of a family of objects $(M_i)_{i\in I}$, which (if it exists) is denoted by $\coprod_{i\in I} M_i$. This is exactly the product of the family in the dual category. In fact, the coproduct $\coprod_{i\in I} M_i$ is an object together with a family $(q_i)_{i\in I}$ of morphisms such that $q_j : M_j \to \coprod_{i\in I} M_i$ for any $j \in I$, and for any object M and any family $(f_i)_{i\in I}$ of morphisms with $f_i : M_i \to M$ for any i, there exists a unique morphism $f : \coprod_{i\in I} M_i \to M$ such that $f \circ q_i = f_i$ for any i. Again, in the case where I is finite, say $I = \{1, 2, \ldots, n\}$, the coproduct is also denoted by $M_1 \coprod M_2 \coprod \ldots \coprod M_n$, or $M_1 \oplus M_2 \oplus \ldots \oplus M_n$.

Fiber products
Let S be an object of a category $\mathcal{C}$. We define the category $\mathcal{C}/S$ in the following way:
- the objects are pairs (A, α), where $\alpha : A \to S$ is a morphism in $\mathcal{C}$.
- If (A, α) and (B, β) are objects of $\mathcal{C}/S$, then a morphism between (A, α) and (B, β) is a morphism $f : A \to B$ in $\mathcal{C}$ such that $\beta \circ f = \alpha$.

If (A, α) and (B, β) are two objects of $\mathcal{C}/S$, the product of these two objects in the category $\mathcal{C}/S$ is called the *fiber product*(or pull-back) of the two objects, and it is denoted by $A \prod_S B$ or $A \times_S B$. The dual notion of fibred product is called a pushout.

A.2 Functors and functorial morphisms

Functors
Let $\mathcal{C}$ and $\mathcal{D}$ be two categories. We say that we give a *covariant functor* (or simply a functor) from $\mathcal{C}$ to $\mathcal{D}$ if to any object $A \in \mathcal{C}$ we associate an object $F(A) \in \mathcal{D}$, and to any morphism $f \in Hom_{\mathcal{C}}(A, B)$ we associate a morphism $F(f) \in Hom_{\mathcal{D}}(F(A), F(B))$ such that $F(1_A) = 1_{F(A)}$ for any object $A \in \mathcal{C}$, and $F(g \circ f) = F(g) \circ F(f)$ for any morphisms f and g in $\mathcal{C}$ for which it makes sense the composition $g \circ f$.
A covariant functor from the dual category $\mathcal{C}^0$ to $\mathcal{D}$ (or from $\mathcal{C}$ to $\mathcal{D}^0$) is called a *contravariant functor* from $\mathcal{C}$ to $\mathcal{D}$.
If $F : \mathcal{C} \to \mathcal{D}$ is a covariant functor, then for any objects $A, B \in \mathcal{C}$ we have a map $Hom_{\mathcal{C}}(A, B) \longrightarrow Hom_{\mathcal{D}}(F(A), F(B))$ defined by $f \mapsto F(f)$. If this map is injective (surjective, bijective), then the functor F is called *faithful*

(*full*, *full and faithful*).
If $\mathcal{C}$ is a category, then the identity functor $1_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$ is defined by $1_{\mathcal{C}}(A) = A$ for any object A, and $1_{\mathcal{C}}(f) = f$ for any morphism f.

Functorial morphisms (natural transformations)
Let $F, G : \mathcal{C} \to \mathcal{D}$ be two functors. A *functorial morphism* ϕ from F to G, denoted by $\phi : F \to G$, is a family $\{\phi(A) | A \in \mathcal{C}\}$ of morphisms, such that $\phi(A) : F(A) \to G(A)$ for any $A \in \mathcal{C}$, and for any morphism $f : A \to B$ in $\mathcal{C}$ we have that $\phi(B) \circ F(f) = G(f) \circ \phi(A)$. If moreover $\phi(A)$ is an isomorphism for any $A \in \mathcal{C}$, then ϕ is called a functorial isomorphism. If there exists such a functorial isomorphism we write $F \simeq G$.
Clearly if $\phi : F \to G$ and $\psi : G \to H$ are two functorial morphisms, we can define the composition $\psi \circ \phi : F \to H$ by $(\psi \circ \phi)(A) = \psi(A) \circ \phi(A)$ for any object A. We denote by $Hom(F, G)$ the class of all functorial morphisms from F to G. If the category $\mathcal{C}$ is small, i.e. its class of objects is a set, then $Hom(F, G)$ is also a set.
For every functor F we can define the functorial morphism $1_F : F \to F$ by $1_F(A) = 1_{F(A)}$ for any $A \in \mathcal{C}$. This is called the identity functorial morphism.

Equivalence of categories
Let $\mathcal{C}$ and $\mathcal{D}$ be two categories. A covariant functor $F : \mathcal{C} \to \mathcal{D}$ is called an *equivalence of categories* if there exists a covariant functor $G : \mathcal{D} \to \mathcal{C}$ such that $G \circ F \simeq 1_{\mathcal{C}}$ and $F \circ G \simeq 1_{\mathcal{D}}$. If moreover $G \circ F = 1_{\mathcal{C}}$ and $F \circ G = 1_{\mathcal{D}}$, then F is called an *isomorphism of categories*, and $\mathcal{C}$ and $\mathcal{D}$ are called isomorphic categories. An equivalence of categories is characterized by the following.

Theorem A.2.1 *If $F : \mathcal{C} \to \mathcal{D}$ is a covariant functor, then F is an equivalence of categories if and only if the following conditions are satisfied.*
(i) F is a full and faithful functor.
(ii) For any object $Y \in \mathcal{D}$ there exists an object $X \in \mathcal{C}$ such that $Y \simeq F(X)$.

A contravariant functor $F : \mathcal{C} \to \mathcal{D}$ such that F is an equivalence between $\mathcal{C}^0$ and $\mathcal{D}$ (or $\mathcal{C}$ and $\mathcal{D}^0$) is called a *duality*.

Yoneda's Lemma
Let $\mathcal{C}$ be a category and $A \in \mathcal{C}$. We can define the covariant functor $h^A : \mathcal{C} \to Set$ as follows: if $X \in \mathcal{C}$, then $h^A(X) = Hom_{\mathcal{C}}(A, X)$, and if $u : X \to Y$ is a morphism in $\mathcal{C}$, then $h^A(u) : h^A(X) \to h^A(Y)$ is defined by $h^A(u)(\xi) = h \circ \xi$ for any $\xi \in h^A(X)$. Similarly, we can define a contravariant functor $h_A : \mathcal{C} \to Set$ as follows: if $X \in \mathcal{C}$, then $h_A(X) = Hom_{\mathcal{C}}(X, A)$, and if $u : X \to Y$ is a morphism in $\mathcal{C}$, then $h_A(u) : h_A(Y) \to h_A(X)$ is

defined by $h_A(u)(\eta) = \eta \circ u$ for any $\eta \in h_A(Y)$.

Theorem A.2.2 *(Yoneda's Lemma) Let $F : \mathcal{C} \to Set$ be a contravariant functor and $A \in \mathcal{C}$. Then the natural map*

$$\alpha : Hom(h_A, F) \to F(A),\ \alpha(\phi) = \phi(A)(1_A)$$

is a bijection.

We indicate the construction of the inverse of α. We define the map $\beta : F(A) \to Hom(h_A, F)$ as follows. If $\xi \in F(A)$, then for $X \in \mathcal{C}$ we consider the map

$$\psi(X) : h_A(X) \to F(X),\ \psi(X)(f) = F(f)(\xi)$$

Note that since the functor F is contravariant we have that $F(f) : F(A) \to F(X)$. It is easy to check that the family of morphisms $\{\psi(X) | X \in \mathcal{C}\}$ defines a functorial morphism $\psi : h_A \to F$. We define then $\beta(\xi) = \psi$.
One consequence of Yoneda's Lemma is that the class $Hom(h_A, F)$ is a set. We also have the following important consequence.

Corollary A.2.3 *If A and B are two objects of $\mathcal{C}$, then $A \simeq B$ if and only if $h_A \simeq h_B$.*

A contravariant functor $F : \mathcal{C} \to Set$ is called *representable* if there exists an object $A \in \mathcal{C}$ such that $F \simeq h_A$. By the above Corollary we see that if such an object A exists, then it is unique up to an isomorphism.

A.3 Abelian categories

Preadditive categories
A category $\mathcal{C}$ is called *preadditive* if it satisfies the following conditions.
a) For any objects $A, B \in \mathcal{C}$, the set $Hom_{\mathcal{C}}(A, B)$ has a structure of an abelian group, with the operation denoted by $+$. The neutral (zero) element of the group $(Hom_{\mathcal{C}}(A, B), +)$ is denoted by $0_{A,B}$, or shortly by 0, and it is called the zero morphism.
b) If A, B, C are arbitrary objects of $\mathcal{C}$, then for any $u, u_1, u_2 \in Hom_{\mathcal{C}}(A, B)$ and $v, v_1, v_2 \in Hom_{\mathcal{C}}(B, C)$, we have that $v \circ (u_1 + u_2) = v \circ u_1 + v \circ u_2$ and $(v_1 + v_2) \circ u = v_1 \circ u + v_2 \circ u$.
c) There exists an object $X \in \mathcal{C}$ such that $1_X = 0$.

If $A \in \mathcal{C}$ and $f \in Hom_{\mathcal{C}}(A, X)$, then by conditions b) and c) we have that $f = 1_X \circ f = 0 \circ f = 0$. Also, if $g \in Hom_{calC}(X, A)$, we have that $g = 0$. Therefore the object X is a zero object in the sense given in Section

1 of the Appendix. Since the zero object is unique up to an isomorphism, we denote it by the symbol 0. If A is any object, we denote by $0 \rightarrow A$ (respectively $A \rightarrow 0$) the unique morphism from 0 to A (respectively from A to 0). Clearly $0 \rightarrow A$ is a monomorphism and $A \rightarrow 0$ is an epimorphism. Clearly if a category $\mathcal{C}$ is preadditive, then so is the dual category $\mathcal{C}^0$. If $\mathcal{C}$ and $\mathcal{D}$ are two preadditive categories, then a functor $F : \mathcal{C} \rightarrow \mathcal{D}$ is called additive if for any two objects $A, B \in \mathcal{C}$ and any $f, g \in Hom_{\mathcal{C}}(A, B)$ we have that $F(f + g) = F(f) + F(g)$. Clearly, if F is an additive functor and 0 is the zero object of $\mathcal{C}$, then $F(0)$ is the zero object of $\mathcal{D}$. As in Section 1, in any preadditive category $\mathcal{C}$ we can define for any morphism $f : A \rightarrow B$ the notions of $Ker(f), Coker(f), Im(f)$ and $Coim(f)$. We say that a preadditive category $\mathcal{C}$ satisfies the axiom $(AB1)$ if for any morphism $f : A \rightarrow B$ there exist a kernel and a cokernel of f. In this case, we have a decomposition

$$\begin{tikzcd}
Ker(f) \arrow[r, "i"] & A \arrow[r, "f"] \arrow[d, "\lambda"'] & B \arrow[r, "\pi"] & Coker(f) \\
& Coim(f) \arrow[r, "\overline{f}"] & Im(f) \arrow[u, "\mu"'] &
\end{tikzcd}$$

where $f = \mu \circ \overline{f} \circ \lambda$, and i, μ are monomorphisms, and λ, π are epimorphisms. using the above decomposition of f, we say that the category $\mathcal{C}$ satisfies the axiom $(AB2)$ if $\overline{f}$ is an isomorphism for any morphism f in $\mathcal{C}$. Clearly, if $\mathcal{C}$ verifies $(AB2)$, then a morphism $f : A \rightarrow B$ is an isomorphism if and only if f is a monomorphism and an epimorphism.

Assume that $\mathcal{C}$ is a preadditive category which satisfies the axioms $(AB1)$ and $(AB2)$. Then a sequence of morphisms

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is called exact if $Im\ f = Ker\ g$ as subobjects of B. An arbitrary sequence of morphisms is called exact if every subsequence of two consecutive morphisms is exact.

If $\mathcal{C}$ and $\mathcal{D}$ are two preadditive categories satisfying the axioms $(AB1)$ and $(AB2)$, then an additive functor $F : \mathcal{C} \rightarrow \mathcal{D}$ is called left (respectively right) exact if for any exact sequence of the form

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

we have an exact sequence

$$0 \longrightarrow F(A) \stackrel{F(f)}{\longrightarrow} F(B) \stackrel{F(g)}{\longrightarrow} F(C)$$

respectively

$$F(A) \stackrel{F(f)}{\longrightarrow} F(B) \stackrel{F(g)}{\longrightarrow} F(C) \longrightarrow 0$$

A functor is called exact if it is left and right exact.

Additive and abelian categories

A preadditive category $\mathcal{C}$ with the property that there exists a coproduct (direct sum) of any two objects is called an *additive category.* An additive category which satisfies the axioms $(AB1)$ and $(AB2)$ is called an *abelian category.*

If $\mathcal{C}$ is an additive category and $A_1, A_2 \in \mathcal{C}$, let $A_1 \oplus A_2$ be a coproduct of the two objects. Bytheuniversal property we have natural morphisms $i_k : A_k \to A_1 \oplus A_2$ and $\pi_k : A_1 \oplus A_2 \to A_k$ for $k = 1, 2$, such that $\pi_k \circ i_k = 1_{A_k}$ for $k = 1, 2$, $\pi_l \circ i_k = 0$ for $k \neq l$, and $i_1 \circ \pi_1 + i_2 \circ \pi_2 = 1_{A_1 \oplus A_2}$. These relations show that $(A_1 \oplus A_2, \pi_1, \pi_2)$ is a product (also called direct product) of the objects A_1 and A_2. Therefore if $\mathcal{C}$ is an additive (respectively preabelian, abelian) category, then so is the dual category $\mathcal{C}^0$. Also, a functor $F : \mathcal{C} \to \mathcal{D}$ between two additive categories is additive if and only if F commutes with finite coproducts.

Grothendieck categories

In the famous paper *"Sur quelques points d'algèbre homologique* (Tohôku Math. J. **9**(1957), 119-221), A. Grothendieck introduced the following axioms for an abelian category $\mathcal{C}$.

$(AB3)$ $\mathcal{C}$ has coproducts, i.e. for any family of objects $(A_i)_{i \in I}$ there exists a coproduct of the family in $\mathcal{C}$.

$(AB3)^*$ $\mathcal{C}$ has products, i.e. for any family of objects $(A_i)_{i \in I}$ there exists a product of the family in $\mathcal{C}$.

Assume that the category $\mathcal{C}$ satisfies the axiom $(AB3)$. Then for any non-empty set I we can define a functor $\oplus_{i \in I} : \mathcal{C}^{(I)} \to \mathcal{C}$, by associating to any family of objects indexed by I the coproduct (direct sum) of the family. This functor is always right exact. We formulate a new axiom.

$(AB4)$ For any non-empty set I, the functor $\oplus_{i \in I}$ is exact.

We also have the dual axiom for a category which satisfies $(AB3)^*$.

$(AB4)^*$ For any non-empty set I, the direct product functor $\prod_{i \in I}$ is exact.

Assume now that $\mathcal{C}$ is an abelian category satisfying the axiom $(AB3)$. If $A \in \mathcal{C}$ and $(A_i)_{i \in I}$ is a family of subobjects of A, then by using $(AB3)$ we see that there exists a smallest subobject $\sum_{i \in I} A_i$ of A such that all A_i's are subobjects of $\sum_{i \in I} A_i$. The subobject $\sum_{i \in I} A_i$ is called the sum of the family $(A_i)_{i \in I}$. The dual situation is when $\mathcal{C}$ is an abelian category satisfying the axiom $(AB3)^*$. Then for $A \in \mathcal{C}$ and $(A_i)_{i\in I}$ a family of subobjects of A, then there exists a largest subobject $\cap_{i\in I} A_i$ of A, which is a subobject of each A_i. The subobject $\cap_{i\in I} A_i$ is called the intersection of the family $(A_i)_{i\in I}$.

If $\mathcal{C}$ is an abelian category, since $\mathcal{C}$ has finite products, then for any subobjects B, C of an object A, there exists the intersection of the family of two subobjects. This is denoted by $B \cap C$ and is called the intersection of the subobjects B and C. We can introduce now a new axiom.

$(AB5)$ Let $\mathcal{C}$ be a category satisfying $(AB3)$. If A is an object of $\mathcal{C}$, and $(A_i)_{i\in I}$ and B are subobjects of A such that the family $(A_i)_{i\in I}$ is right filtered, then $(\sum_{i\in I} A_i) \cap B = \sum_{i\in I}(A_i \cap B)$.

The dual of this axiom is called $(AB5)^*$. It is easy to see that a a category satisfying $(AB5)$ also satisfies $(AB4)$.

Let $\mathcal{C}$ be an abelian category. A family $(U_i)_{i\in I}$ of objects of $\mathcal{C}$ is called a *family of generators* of $\mathcal{C}$ if for any object $A \in \mathcal{C}$ and any subobject B of A such that $B \neq A$ (as a subobject), there exist some $i \in I$ and a morphism $\alpha : U_i \rightarrow A$ such that $Im(\alpha)$ is not a subobject of B. We say that an object U of $\mathcal{C}$ is a *generator* if the singleton family $\{U\}$ is a family of generators. In the case where $\mathcal{C}$ is an abelian category with $(AB3)$, then a family $(U_i)_{i\in I}$ of objects of $\mathcal{C}$ is a family of generators if and only if the direct sum $\oplus_{i\in I} U_i$ of the family is a generator of $\mathcal{C}$. An abelian category $\mathcal{C}$ which verifies the axiom $(AB5)$ and has a generator (or equivalently a family of generators) is called a *Grothendieck category*. In the same cited paper of Grothendieck it is proved that an abelian category which verifies both $(AB5)$ and $(AB5)^*$ must be the zero category. In particular we see that if $\mathcal{C}$ is a non-zero Grothendieck category, then the dual category $\mathcal{C}^0$ is not a Grothendieck category.

A.4 Adjoint functors

Let $\mathcal{C}$ and $\mathcal{D}$ be two categories and $F : \mathcal{C} \rightarrow \mathcal{D}$, $G : \mathcal{D} \rightarrow \mathcal{C}$ be two functors. The functor F is called a *left adjoint* of G (or G is called a *right adjoint* of F) if there exists a functorial morphism

$$\phi : Hom_{\mathcal{D}}(F, -) \longrightarrow Hom_{\mathcal{C}}(-, G)$$

where $Hom_{\mathcal{D}}(F, -) : \mathcal{C}^0 \times \mathcal{D} \rightarrow Set$ is the functor associating to the pair of objects (A, B) the set $Hom_{\mathcal{D}}(F(A), B)$, and $Hom_{\mathcal{C}}(-, G) : \mathcal{C}^0 \times \mathcal{D} \rightarrow Set$ is the functor associating to (A, B) the set $Hom_{\mathcal{C}}(A, G(B))$.

In the case where $\mathcal{C}$ and $\mathcal{D}$ are preadditive categories, and F and G are two additive functors, then we assume that $\phi(A, B)$ is an isomorphism of abelian groups for any $A \in \mathcal{C}$ and $B \in \mathcal{D}$. We give now the main properties of adjoint functors.

Theorem A.4.1 *With the above notation, assume that F is a left adjoint of G. Then the following assertions hold.*
1) The functor F commutes with coproducts and the functor G commutes with products.
2) If $\mathcal{C}$ and $\mathcal{D}$ are abelian categories and the functors F and G are additive, then F is right exact and G is left exact.
3) Assume that the category $\mathcal{D}$ has enough injective objects, i.e. for any $B \in \mathcal{D}$ there exist an injective object $Q \in \mathcal{D}$ and a monomorphism $0 \to B \to Q$ in $\mathcal{D}$. Then F is exact if and only if G commutes with injective objects (i.e. for any injective object $Q \in \mathcal{D}$, the object $G(Q)$ is injective in $\mathcal{C}$.
4) Assume that $\mathcal{C}$ has enough projective objects, i.e. for any $A \in \mathcal{C}$ there exist a projective object $P \in \mathcal{C}$ and an epimorphism $P \to A \to 0$ in $\mathcal{C}$. Then G is exact if and only if F commutes with projective objects.

The concept of adjoint functor is fundamental in mathematics, since many properties are in fact adjointness properties. A standard example of an adjoint pair of functors is provided by the Hom and $\otimes$ functors, more precisely, if $M \in {}_R\mathcal{M}_S$, then $M \otimes_R - : {}_S\mathcal{M} \to {}_R\mathcal{M}$ is a left adjoint of $Hom_R(M, -) : {}_R\mathcal{M} \to {}_S\mathcal{M}$.

Appendix B

$\mathcal{C}$-groups and $\mathcal{C}$-cogroups

B.1 Definitions

Let $\mathcal{C}$ be a category and $A \in \mathcal{C}$. We say that we have an *internal composition* on the object A if for any object $X \in \mathcal{C}$ there exists an binary operation on the set $h_A(X) = Hom_{\mathcal{C}}(X, A)$ such that for any morphism $u : Y \to X$ in $\mathcal{C}$ the map $h_A(u) : h_A(X) \to h_A(Y)$ is a morphism for the operations on the two sets. This means that for any $X \in \mathcal{C}$ there is a map "$*_X$" (or simply "$*$"): $h_A(X) \times h_A(X) \to h_A(X)$ such that for any morphism $u : Y \to X$ the diagram

$$\begin{tikzcd}
h_A(X) \times h_A(X) \arrow[r, "h_A(u) \times h_A(u)"] \arrow[d, "*_X"'] & h_A(Y) \times h_A(Y) \arrow[d, "*_Y"] \\
h_A(X) \arrow[r, "h_A(u)"] & h_A(Y)
\end{tikzcd}$$

is commutative, i.e.

$$(f \ *_X \ g) \circ u = (f \circ u) \ *_Y \ (g \circ u) \tag{B.1}$$

for any $f, g \in h_A(X)$.

In case $*_X$ turns $h_A(X)$ into a group (abelian group, resp.) for any $A \in \mathcal{C}$, then A is called a $\mathcal{C}$-*group* ($\mathcal{C}$-*abelian group*, resp.). If A is a $\mathcal{C}^\circ$-group ($\mathcal{C}^\circ$-abelian group, resp.), then A is called a $\mathcal{C}$-*cogroup* ($\mathcal{C}$-*abelian cogroup*, resp.).

If $A, B \in \mathcal{C}$ are two $\mathcal{C}$-groups, and $u : A \to B$ a morphism in $\mathcal{C}$ such that for any $X \in \mathcal{C}$ the map $h_A(u) : h_A(X) \to h_A(Y)$ is a morphism of groups, i.e.

$$u \circ (f \ *_X \ g) = (u \circ f) \ *_Y \ (u \circ g) \tag{B.2}$$

then u is called a morphism of $\mathcal{C}$-groups.

It is clear that the class of all $\mathcal{C}$-groups defines a category, denoted by $Gr(\mathcal{C})$. Similarly, the class of all $\mathcal{C}$-abelian groups defines a category, denoted by $Ab(\mathcal{C})$.

Remark B.1.1 *If the category $\mathcal{C}$ has a "zero" object, then for any objects X and Y we have the zero morphism from Y to X. Then, putting $u = 0$ in equality (B.1), we have in that*

$$0 = 0 \ *_Y 0 \tag{B.3}$$

in $Hom_{\mathcal{C}}(Y, A)$.
If A is a $\mathcal{C}$-group, then from (B.3) it follows that $0 = e$, where e is the unit element of the group $Hom_{\mathcal{C}}(Y, A)$ for any $Y \in \mathcal{C}$. ∎

We assume now that $\mathcal{C}$ has finite direct products, and a final object, denoted by F.
If $A \in \mathcal{C}$ is a $\mathcal{C}$-group, we denote by $\eta_A \in Hom_{\mathcal{C}}(F, A)$ the unit element of this group. Then for any $X \in \mathcal{C}$, the element

$$\eta_A \circ \varepsilon_X : X \xrightarrow{\varepsilon_X} F \xrightarrow{\eta_A} A,$$

where ε_X is the unique element of $Hom_{\mathcal{C}}(X, F)$, is the unit element of the group $Hom_{\mathcal{C}}(X, A)$. Indeed, from (B.1) we have

$$(\eta_A * \eta_A) \circ \varepsilon_X = (\eta_A \circ \varepsilon_X) * (\eta_A \circ \varepsilon_X),$$

so

$$\eta_A \circ \varepsilon_X = (\eta_A \circ \varepsilon_X) * (\eta_A \circ \varepsilon_X),$$

and since $Hom_{\mathcal{C}}(X, A)$ is a group, it follows that $\eta_A \circ \varepsilon_X$ is its unit element.

Now since $\mathcal{C}$ has finite direct products, we have the direct products $A \times A$ and $A \times A \times A$. By the Yoneda Lemma, the maps $*_X$, $X \in \mathcal{C}$, yield a morphism $m : A \times A \to A$. Then the associativity and the existence of the unit element imply the commutativity of the following diagrams

$$\begin{tikzcd} A\times A\times A \arrow[r, "I\times m"] \arrow[d, "m\times I"'] & A\times A \arrow[d, "m"] \\ A\times A \arrow[r, "m"] & A \end{tikzcd} \tag{B.4}$$

$$\begin{tikzcd} & A\times A \arrow[dd, "m"] & \\ F\times A \arrow[ur, "\eta_A\times I"] \arrow[dr, "\sim"'] & & A\times F \arrow[ul, "I\times\eta_A"'] \arrow[dl, "\sim"] \\ & A & \end{tikzcd} \tag{B.5}$$

where I is the identity morphism, and since F is a final object, we have the canonical isomorphisms $A \times F \simeq A$ and $F \times A \simeq A$.
In the same way, the existence of the inverse shows that there exists an $S \in Hom_C(A, A)$ making the following diagram commutative

$$\begin{tikzcd} A \arrow[r, "\binom{I}{S}"] \arrow[d, "\varepsilon_A"] & A\times A \arrow[d, "m"] & A \arrow[l, "\binom{S}{I}"'] \arrow[d, "\varepsilon_A"] \\ F \arrow[r] & A & F \arrow[l] \end{tikzcd} \tag{B.6}$$

Here $\binom{I}{S}$ and $\binom{S}{I}$ denote the canonical morphisms defined by the universal property of the direct product using the morphisms $I : A \to A$ and $S : A \to A$.

Example B.1.2 *1. If $C = Set$ (the category of sets), then it has arbitrary direct products and a final object. In this case we have that $Gr(Set)$ is just the category of groups.*
2. If $C = Top$ (the category of topological spaces), then $Gr(Top)$ is the

category of topological groups.
3. Assume that $\mathcal{C}$ is an additive category. Let $A \in \mathcal{C}$, and consider the canonical morphisms $i_j : A \to A \times A$, and $\pi_j : A \times A \to A$, $j = 1, 2$, such that $\pi_j \circ i_l = \delta_{jl} I_A$. In fact, $i_1 = \binom{I}{0}$ and $i_2 = \binom{0}{I}$. By the commutativity of the diagram (B.4), it follows that $m \circ i_1 = m \circ i_2 = I_A$. On the other hand, let $f, g \in Hom_{\mathcal{C}}(X, A)$. We denote by $\nabla : A \times A \to A$ the canonical morphism with the property that $\nabla \circ i_1 = \nabla \circ i_2 = I_A$ (we used the fact that $A \times A$ is also a coproduct). The morphisms f and g also define a canonical morphism $\binom{f}{g} : X \to A \times A$, such that $\pi_1 \circ \binom{f}{g} = f$ and $\pi_2 \circ \binom{f}{g} = g$. Since $i_1 \circ \pi_1 + i_2 \circ \pi_2 = I_{A \times A}$, we have

$$\nabla \circ (i_1 \circ \pi_1) \circ \begin{pmatrix} f \\ g \end{pmatrix} = \nabla \circ i_1 \circ f = f,$$

and

$$\nabla \circ (i_2 \circ \pi_2) \circ \begin{pmatrix} f \\ g \end{pmatrix} = \nabla \circ i_2 \circ g = g,$$

and therefore $\nabla \circ \binom{f}{g} = f + g$.
Since $m \circ i_1 = m \circ i_2 = I_A$, we get by uniqueness that $m = \nabla$, so $m \circ \binom{f}{g} = f + g$. But $m \circ \binom{f}{g} = f \ast_X g$, so $f \ast_X g = f + g$.
In conclusion, if $\mathcal{C}$ is an additive category, we have that every object $A \in \mathcal{C}$ is an abelian $\mathcal{C}$-group, with the multiplication of $Hom_{\mathcal{C}}(X, A)$ the sum of morphisms. So $Gr(\mathcal{C}) = Ab(\mathcal{C})$ is isomorphic to the category $\mathcal{C}$.
Since $\mathcal{C}^\circ$ is also an additive category, it follows that every object $A \in \mathcal{C}$ is also an abelian $\mathcal{C}$-cogroup. ∎

B.2 General properties of $\mathcal{C}$-groups

Proposition B.2.1 *Assume that $\mathcal{C}$ is a ctegory which has finite direct products, and a final object. Then the following assertion hold:*
i) $Gr(\mathcal{C})$ has direct products.
ii) $Ab(\mathcal{C})$ is an abelian category.
iii) If $\mathcal{C}$ also has fiber products (pull-backs), then in the category $Ab(\mathcal{C})$ every morphism has a kernel.

Proof: i) If $A, B \in Gr(\mathcal{C})$, since we have

$$Hom_{\mathcal{C}}(X, A \times B) \simeq Hom_{\mathcal{C}}(X, A) \times Hom_{\mathcal{C}}(X, B),$$

it follows that $A \times B$ is also a $\mathcal{C}$-group.
ii) Assume that $A, B \in Ab(\mathcal{C})$. Then we consider the operation "$*$" on $Hom_{Ab(\mathcal{C})}(A, B)$ as in the first section. From (B.1) and (B.2) we get the

distributivity of the composition "$\circ$" with respect to "$*$".
Now if F denotes the final object of $\mathcal{C}$, then F is the zero object of $Ab(\mathcal{C})$, and from i) we get that $Ab(\mathcal{C})$ is an abelian category.
iii) Let $f : A \to B$ be a morphism in the category $Ab(\mathcal{C})$. If F is the final object and, and $\eta : F \to B$ is the unit element of the group $Hom_{\mathcal{C}}(F, B)$, then for $X \in \mathcal{C}$ and $\varepsilon : X \to F$ the unique morphism, we saw that $\eta \circ \varepsilon$ is the unit element of the group $Hom_{\mathcal{C}}(X, B)$. We denote by $A \times_B F$ the fiber product associated to the diagram

$$\begin{tikzcd} A \arrow[dr, "f"] & \\ & F \\ F \arrow[ur, "\eta"] & \end{tikzcd}$$

Then by the definition of the fiber product we have that $Hom_{\mathcal{C}}(X, A \times_B F)$ is identified to the set of all elements $u \in Hom_{\mathcal{C}}(X, A)$ such that $f \circ u = \eta \circ \varepsilon$. Since $Hom_{\mathcal{C}}(X, A)$ is an abelian group, and $f : A \to B$ is a morphism of groups, then $Hom_{\mathcal{C}}(X, A \times_B F)$ is a subgroup of $Hom_{\mathcal{C}}(X, A)$. So $A \times_B F$ is a $\mathcal{C}$-abelian group. It is easy to see that $A \times_B F$ is the kernel of f in the category $Ab(\mathcal{C})$. ∎

Remark B.2.2 *A category $\mathcal{C}$ with finite direct products and final object is a braided monoidal category (even symmetric), where the "tensor product" functor is the direct product.* ∎

B.3 Formal groups and affine groups

Let k be a field. We consider two categories: $k - CCog$, i.e. the category of all cocommutative k-coalgebras, and the dual $(k - CAlg)^\circ$, where $k - CAlg$ is the category of commutative k-algebras. These categories have finite direct products and final objects (the final object is in both cases the field k, regarded as a coalgebra or an algebra). It is easy to see that $Gr(k - CCog)$ is exactly the category of cocommutative Hopf algebras over k. An object in this category is called a *formal group*.
Similarly, $Gr((k - CAlg)^\circ)$ is exactly the category of commutative Hopf algebras over k. In fact, the objects of this category are cogroups in the category $k - CAlg$. When we consider only the category of all affine k-algebras (i.e. commutative k-algebras which are finitely generated as k-

algebras), then a group object in the dual of this category is called an *affine group*.

We remark that $Ab(k{-}CCog) = Ab(k{-}CAlg)$. The following important result concerns this category.

Theorem B.3.1 *$Ab(k - CCog)$ is a Grothendieck category.*

Proof: We will give a sketch of proof. To simplify the notation, put $\mathcal{A} = Ab(k - CCog)$. The main steps of the proof are the following:
Step 1. If $H, K \in \mathcal{A}$, then $Hom_{\mathcal{A}}(H, K)$ is the set of all Hopf algebra maps. Now if $f, g \in Hom_{\mathcal{A}}(H, K)$, then the multiplication of f and g is given by the convolution product $f * g$. Since H and K are commutative and cocommutative, then $f * g$ is also a Hopf algebra morphism. It is easy to see that $\eta \circ \varepsilon$ is the unit element, where $\varepsilon : H \to k$ and $\eta : k \to K$ are the canonical maps. Moreover, the inverse of f is given by $S_K \circ f = f \circ S_H$. Hence $Hom_{\mathcal{A}}(H, K)$ is an abelian group. It is also easy to see that

$$(f * g) \circ u = (f \circ u) * (g \circ u) \text{ and } v \circ (f * g) = (v \circ f) * (v \circ g).$$

Step 2. We know from Proposition B.2.1 that $\mathcal{A}$ is an additive category. If $H, K \in \mathcal{A}$, then $H \otimes K$ is a commutative and cocommutative Hopf algebra. It is easy to see that $H \otimes K$ is the coproduct and the product of H and K in the category $\mathcal{A}$. The zero object in $\mathcal{A}$ is k.
Step 3. $\mathcal{A}$ verifies the axiom AB1). Let $f : H \to K$ be a morphism in the category $\mathcal{A}$. By Proposition B.2.1, f has a kernel. In fact, the kernel is exactly $H \times_K k = H \square_K k$ (see Exercise 2.3.11). On the other hand, if we put $L = Im(f)$, then L is a Hopf subalgebra of K, and $I = L^+K$ is a Hopf ideal (recall that $L^+ = Ker(\varepsilon_L)$. Then it is easy to see that K/I, together with the canonical projection $\pi : K \to K/I$, is a cokernel of f.
Step 4. $\mathcal{A}$ verifies the axiom AB2). This is the main step, and it follows from the following result: if H is a commutative and cocommutative Hopf algebra, the map $K \mapsto K^+H$ establishes a bijective correpondence between the Hopf subalgebras of H and the Hopf ideals of H. A proof of a more general version of this result may be found in M. Takeuchi [228], A. Heller [94], or more recently in H.-J. Schneider [203].
Step 5. $\mathcal{A}$ verifies the axioms AB3) and AB5). Let $(H_i)_{i \in I}$ be a family of objects in $\mathcal{A}$. Consider the infinite tensor product $\bigotimes_{i \in I} H_i$, which is a k-algebra, and the subalgebra, denoted by $\overline{\bigotimes_{i \in I}} H_i$, generated by all images of morphisms $\alpha_i : H_i \to \bigotimes_{j \in I} H_j$, $\alpha_i(x) = \bigotimes_{j \in I} x_j$, where $x_i = x$, and $x_j = 1$ for $j \neq i$. It is easy to see that $\overline{\bigotimes_{i \in I}} H_i$ is also a Hopf algebra, and it is the direct sum of the family $(H_i)_{i \in I}$ in the category $\mathcal{A}$. Now by Step 4, if

$f : H \to K$ is a morphism in $\mathcal{A}$, then f is a monomorphism in this category if and only if $Ker(f) = k$ (k is the zero object in $\mathcal{A}$), if and only if f is injective (since the Hopf ideal associated to the Hopf subalgebra k is zero as a vector space). So the subobjects of K are all Hopf subalgebras. From this it follows that $\mathcal{A}$ satisfies AB5).
Step 6. $\mathcal{A}$ has a family of generators. Indeed, if we consider the category $k - CCog$, the forgetful functor

$$U : Ab(k - CCog) \longrightarrow k - CCog$$

has a left adjoint, denoted by

$$F : k - CCog \longrightarrow Ab(k - CCog).$$

Then if we consider the set of all finite dimensional cocommutative coalgebras $(C_i)_{i \in I}$, from the above it follows that the family $(F(C_i))_{i \in I}$ is a family of generators for $\mathcal{A}$. ∎

Bibliography

[1] E. Abe, Hopf Algebras, Cambridge Univ. Press, 1977.

[2] H. Allen, D. Trushin, Coproper coalgebras, J. Algebra 54 (1978), 203-215.

[3] F.W. Anderson, K.R. Fuller, Rings and Categories of Modules, GTM 13, 2-nd edition, Springer-Verlag, 1992.

[4] N. Andruskiewitsch, Compact involutions on semisimple quantum groups, Czechoslovak J. Phys. 44 (1994), 963-972.

[5] N. Andruskiewitsch, Notes on extensions of Hopf algebras, Canad. J. Math. 48 (1996), 3-42.

[6] N. Andruskiewitsch, About finite dimensional Hopf algebras, to appear in Contemp. Math.

[7] N. Andruskiewitsch, J. Devoto, Extensions of Hopf algebra, Algebra i Analiz 7 (1995), 17-52.

[8] N. Andruskiewitsch, M. Graña, Braided Hopf algebras over non-abelian groups, Bol. Acad. Ciencias (Córdoba) 63 (1999), 45-78.

[9] N. Andruskiewitsch, S. Natale, Plancherel identity for semisimple Hopf algebras, Comm. Algebra 25 (1997), 3239-3254.

[10] N. Andruskiewitsch, S. Natale, Examples of selfdual Hopf algebras, J. Math. Sci. Univ. Tokyo 6 (1999), 181-215.

[11] N. Andruskiewitsch, S. Natale, Counting arguments for Hopf algebras of low dimension, to appear in Tsukuba J. Math.

[12] N. Andruskiewitsch, H.-J. Schneider, Hopf algebras of order p^2 and braided Hopf algebras of order p, J. Algebra 199 (1998), 430-454.

[13] N. Andruskiewitsch, H.-J. Schneider, Lifting of quantum linear spaces and pointed Hopf algebras of order p^3, J. Algebra 209 (1998), 658-691.

[14] N. Andruskiewitsch, H.-J. Schneider, Liftings of Nichols algebras of type A_2 and pointed Hopf algebras of order p^4, in Hopf algebras and quantum groups, Proc. of the Colloquium in Brussels 1998, 1-18.

[15] N. Andruskiewitsch, H.-J. Schneider, Finite quantum groups and Cartan matrices, to appear in Adv. in Math.

[16] N. Andruskiewitsch, H.-J. Schneider, Finite quantum groups over abelian groups of prime exponent, preprint.

[17] N. Andruskiewitsch, H.-J. Schneider, Pointed Hopf algebras, to appear in "Recent developments in Hopf algebras", Cambridge Univ. Press.

[18] N. Andruskiewitsch, H.-J. Schneider, On the coradical filtration of Hopf algebras whose coradical is a Hopf subalgebra, to appear in Bol. Acad. Ciencias (Córdoba).

[19] V. A. Artamonov, Invariants of Hopf algebras, Vestnik Moskovskogo Universiteta. Matematika. Mekhanika 4 (1996), 45-49 (in Russian).

[20] H. Bass, Algebraic K-Theory, W. A. Benjamin, Inc., 1968.

[21] M. Beattie, A generalization of the smash product of a graded ring, J. Pure Appl. Algebra 52 (1988), 219-226.

[22] M. Beattie, Duality theorems for rings with actions or coactions, J. Algebra 115 (1988), 303-312.

[23] M. Beattie, Strongly inner actions, coactions, and duality theorems, Tsukuba J. Math., 16 (1992), 279-293.

[24] M. Beattie, An isomorphism theorem for Ore extension Hopf algebras, Comm. Algebra 28 (2000), 569-584.

[25] M. Beattie, S. Dăscălescu, L. Grünenfelder, On the number of types of finite dimensional Hopf algebras, Invent. Math. 136 (1999), 1-7.

[26] M. Beattie, S. Dăscălescu, L. Grünenfelder, On pointed Hopf algebras of dimension p^n, Proc. Amer. Math. Soc. 128 (2000), 361-367.

[27] M. Beattie, S. Dăscălescu, L. Grünenfelder, Constructing pointed Hopf algebras by Ore extensions, J. Algebra 225 (2000), 743-770.

[28] M. Beattie, S. Dăscălescu, L. Grünenfelder, C. Năstăsescu, Finiteness Conditions, Co-Frobenius Hopf Algebras and Quantum Groups, J. Algebra 200 (1998), 312-333.

[29] M. Beattie, S. Dăscălescu, Ş. Raianu, Galois Extensions for Co-Frobenius Hopf Algebras, J. Algebra, 198 (1997), 164-183.

[30] M. Beattie, S. Dăscălescu, Ş. Raianu, A co-Frobenius Hopf algebra with a separable Galois extension is finite, to appear in Proc. Amer. Math. Soc.

[31] M. Beattie, K. H. Ulbrich, A Skolem-Noether theorem for Hopf algebra actions, Comm. Algebra 18 (1990), 3713-3724.

[32] J. Bergen, M. Cohen, Actions of commutative Hopf algebras, Bull. London. math. Soc. 18 (1986), 159-164.

[33] J. Bergen, S. Montgomery, Ideals and quotients in crossed products of Hopf algebras, J. Algebra 151 (1992), 374-396.

[34] J. Bergen, S. Montgomery, eds, Advances in Hopf algebras, Marcel Dekker Lecture Notes in Pure and Appl. Math., vol. 158 (1994).

[35] R. Blattner, S. Montgomery, A duality theorem for Hopf module algebras, J. Algebra 95 (1985), 153-172.

[36] R. Blattner, S. Montgomery, Crossed products and Galois extensions of Hopf algebras, Pacific J. Math 137 (1989), 37-54.

[37] R. Blattner, M. Cohen, S. Montgomery, Crossed Products and Inner Actions of Hopf Algebras, Trans. of the AMS, 298 (1986), 671-711.

[38] T. Brzeziński, On modules associated to coalgebra Galois extensions, J. Algebra 215 (1999), 290-317.

[39] T. Brzeziński, The structure of corings: Induction functors, Maschke-type theorem, and Frobenius and Galois-type properties, preprint, (http://xxx.lanl.gov).

[40] T. Brzeziński, S. Caenepeel, G. Militaru, S. Zhu, Frobenius and Maschke-type theorems for Doi-Hopf modules and entwined modules revisited: a unified approach, arXiv:math.RA/0003198.

[41] D. Bulacu, Injective modules graded by G-sets, Comm. Algebra 27 (1999), 3537-3543.

[42] C. Cai, H. Chen, Coactions, smash products, and Hopf modules, J. Algebra 167 (1994), 85-99.

[43] S. Caenepeel, Ş. Raianu, B. Zhou, The coinduced functor for infinite dimensional Hopf algebras, J. Pure Appl. Algebra, 107 (1996), 141-151.

[44] S. Caenepeel, Ş. Raianu, Induction functors for the Doi-Koppinen unified Hopf modules, in Abelian groups and modules, Proceedings of the Padova Conference, Padova, Italy, June 23-July 1, 1994, Kluwer, 1995, eds. A. Facchini and C. Menini, p. 73-94.

[45] S. Caenepeel, S. Dăscălescu, Pointed Hopf algebras of dimension p^3, J. Algebra 209 (1998), 622-634.

[46] S. Caenepeel, S. Dăscălescu, On pointed Hopf algebras of dimension 2^n, Bull. London. Math. Soc. 31 (1999), 17-24.

[47] S. Caenepeel, S. Dăscălescu, Ş. Raianu, Classifying pointed Hopf algebras of dimension 16, Comm. Algebra 28 (2000), 541-568.

[48] S. Caenepeel, S. Dăscălescu, L. Le Bruyn, Forms of pointed Hopf algebras, Manuscripta Math. 100 (1999), 35-53.

[49] S. Caenepeel, G. Militaru, S. Zhu, A Maschke type theorem for Doi-Hopf modules and applications, J. Algebra 187 (1997), 388-412.

[50] S. Caenepeel, G. Militaru, S. Zhu, Doi-Hopf modules, Yetter-Drinfel'd modules and Frobenius type properties, Trans. Amer. Math. Soc. 349 (1997), 4311-4342.

[51] S. Caenepeel, G. Militaru, S. Zhu, Generalized Hopf Modules and Non-Linear Equations, in preparation.

[52] C. Călinescu, Dissertation, University of Bucharest, 1998.

[53] S. U. Chase, M. E. Sweedler, Hopf algebras and Galois theory, Lecture Notes in Math. 97 (1969), Springer Verlag.

[54] H. Chen, C. Cai, Hopf algebra coactions, Comm. Algebra 22 (1994), 253-267.

[55] L. Childs, On the Hopf Galois theory for separable field extensions, Comm. Algebra 17 (1989), 809-825.

[56] W. Chin, Spectra of smash products, Israel J. Math. 72 (1990), 84-98.

[57] W. Chin, Crossed products of semisimple cocommutative Hopf algebras, proc. Amer. Math. Soc. 116 (1992), 321-327.

[58] M. Cohen, Smash products, inner actions and quotient rings, Pacific J. Math., 125 (1986), 45-66.

[59] M. Cohen, Hopf algebra actions-revisited, Contemp. Math. 134 (1992), 1-18.

[60] M. Cohen, S. Montgomery, Group-graded rings, smash products, and group actions, Trans. Amer. Math. Soc. 282 (1984), 237-258.

[61] M. Cohen, D. Fischman and S. Montgomery, Hopf Galois Extensions, Smash Products and Morita Equivalences, J. Algebra 133 (1992), 251-272.

[62] M. Cohen, D. Fischman, Hoph algebra actions, J. Algebra 100 (1986), 363-379.

[63] M. Cohen and D. Fischman, Semisimple extensions and elements of trace 1, J. Algebra 149 (1992), 419-437.

[64] M. Cohen, Ş. Raianu, S. Westreich, Semiinvariants for Hopf algebra actions, Israel J. Math. 88 (1994), 279-306.

[65] C. W. Curtis and I. Reiner, Representation theory of finite groups and associative algebras, Interscience, New York, 1962.

[66] S. Dăscălescu, Pointed Hopf algebras with large coradical, Comm. Algebra 27 (1999), 4821-4826.

[67] S. Dăscălescu, A. Kelarev, B. Torrecillas, FBN Hopf module algebras, Comm. Algebra 25 (1997), 3521-3529.

[68] S. Dăscălescu, C. Năstăsescu, B. Torrecillas, Co-Frobenius Hopf Algebras: Integrals, Doi-Koppinen Modules and Injective Objects, J. Algebra 220 (1999), 542-560.

[69] S. Dăscălescu, C. Năstăsescu, B. Torrecillas, Homological dimension of coalgebras and crossed coproducts, preprint.

[70] S. Dăscălescu, Ş. Raianu, F. Van Oystaeyen, Some Remarks on a Theorem of H.-J. Schneider, Comm. Algebra 24 (1996), 4477-4493.

[71] S. Dăscălescu, C. Năstăsescu, F. Van Oystaeyen and B. Torrecillas, Duality theorems for graded algebras and coalgebras, J. Algebra 192 (1997), 261-276.

[72] Y. Doi, Homological coalgebra, J. Math. Soc. Japan 33 (1981), 31-50.

[73] Y. Doi, On the structure of relative Hopf modules, Comm. Algebra 11 (1983), 243-255.

[74] Y. Doi, Cleft comodule algebras and Hopf modules, Comm. Algebra 12 (1984), 1155-1169.

[75] Y. Doi, Algebras with total integrals, Comm. Algebra 13 (1985), 2137-2159.

[76] Y. Doi, Unifying Hopf Modules, J. Algebra, 153 (1992), 373-385.

[77] Y. Doi, Generalized smash products and Morita contexts for arbitrary Hopf algebras, in Advances in Hopf Algebras, edited by J. Bergen and S. Montgomery, Marcel Dekker Lecture Notes in Pure and Appl. Math., vol. 158 (1994), 39-54.

[78] Y. Doi, M. Takeuchi, Cleft comodule algebras for a bialgebra, Comm. Algebra 14 (1986), 801-817.

[79] Y. Doi, M. Takeuchi, Hopf-Galois extensions of algebras, the Miyashita-Ulbrich action and Azumaya algebras, J. Algebra 121 (1989), 488-516.

[80] V. Drinfeld, Quantum groups, proceedings of the ICM Berkeley 1986, A.M.S.

[81] P. Etingof, S. Gelaki, Semisimple Hopf algebras of dimension pq are trivial, J. Algebra 210 (1998), 664-669.

[82] P. Etingof, S. Gelaki, On finite dimensional semisimple and cosemisimple Hopf algebras in positive characteristic, Int. Math. Res. Notices 16 (1998), 851-864.

[83] W. R. Ferrer Santos, Finite generation of the invariants of finite dimensional Hopf algebras, J. Algebra 165 (1994), 543-549.

[84] N. Fukuda, Semisimple Hopf algebras of dimension 12, Tsukuba J. Math. 21 (1997), 43-54.

[85] P. Gabriel, Des catégories abeliennes, Bull. Soc. Math. France 90 (1962), 323-448.

[86] S. Gelaki, Pointed Hopf algebras and Kaplansky's 10th conjecture, J. Algebra 209 (1998), 635-657.

[87] S. Gelaki, S. Westreich, On semisimple Hopf algebras of dimension pq, Proc. Amer. Math. Soc. 128 (2000), 39-47.

[88] J. Gomez Torrecillas, Coalgebras and comodules over a commutative ring, Rev. Roumaine Math. Pures. Appl. 43 (1998), 591-603.

[89] M. Graña, Pointed Hopf algebras of dimension 32, to appear in Comm. Algebra.

[90] M. Graña, On pointed Hopf algebras of dimension p^5, to appear in Glasgow Math. J.

[91] M. Graña, A freeness theorem for Nichols algebras, to appear in J. Algebra.

[92] C. Greither, B. Pareigis, Hopf Galois theory for separable field extensions, J. Algebra 106 (1987), 239-258.

[93] R. Haggenmüller, B. Pareigis, Hopf algebra forms of the multiplicative group and other groups, Manuscripta Math. 55 (1986), 121-136.

[94] A. Heller, Principal bundles and group of extensions with applications to Hopf algebras, J. Pure Appl. Algebra 3 (1973), 219-250.

[95] R. G. Heyneman, D.E. Radford, Reflexivity and coalgebras of finite type, J. Algebra 28 (1974), 215-246.

[96] R. G. Heyneman, M. E. Sweedler, Affine Hopf algebras I, J. Algebra 13 (1969), 192-241.

[97] R. G. Heyneman, M. E. Sweedler, Affine Hopf algebras II, J. Algebra 16 (1970), 271-297. 192-241.

[98] I. Hofstetter, Extensions of Hopf algebras and their cohomological description, J. Algebra 164 (1994), 264-298.

[99] N. Jacobson, Basic Algebra I, San Francisco: W.H. Freeman and Comp. XVI, 1974.

[100] N. Jacobson, Structure of rings, Amer. Math. Soc. Colloquium Publications, vol. 37, 1956.

[101] G.I. Kac, Extensions of groups to ring groups, Math. USSR Sbornik 5 (1968), 451-474.

[102] G.I. Kac, Certain arithmetic properties of ring groups, Funct. Anal. Appl. 6 (1972), 158-160.

[103] G.I. Kac, V. G. Paljutkin, Finite group rings, Trans. Moscow Math. Soc. 15 (1966), 251-294.

[104] I. Kaplansky, Bialgebras, Lecture Notes in Mathematics, University of Chicago, 1975.

[105] Y. Kashina, Semisimple Hopf algebras of dimension 16, preprint.

[106] C. Kassel, *Quantum Groups*, Graduate Texts in Mathematics **155** (1995), Springer Verlag.

[107] M. Koppinen, Variations on the smash product with applications to group-graded rings, J. Pure Appl. Algebra 104 (1995), 61-80.

[108] M. Koppinen, A duality theorem for crossed products of Hopf algebras, J. Algebra 146 (1992), 153-174.

[109] M. Koppinen, Coideal subalgebras in Hopf algebras: freeness, integrals, smash products, Comm. Algebra 21 (1993), 427-444.

[110] H. F. Kreimer, M. Takeuchi, Hopf algebras and Galois extensions of an algebra, Indiana univ. Math. J. 30 (1981), 675-692.

[111] H. F. Kreimer, P. M. Cook II, Galois theories and normal bases, J. Algebra 43 (1976), 115-121.

[112] T.Y. Lam, A First Course in Noncommutative Rings, GTM 131, Springer-Verlag, 1991.

[113] L.A. Lambe, D.E. Radford, Introduction to the quantum Yang-Baxter equation and quantum groups: an algebraic approach, Math. and its Appl., Dordrecht: Kluwer Academic Publishers, 1997.

[114] R. G. Larson, The order of the antipode of a Hopf algebra, Proc. Amer. Math. Soc. 21 (1969), 167-170.

[115] R. G. Larson, Characters of Hopf algebras, J. Algebra 17 (1971), 352-368.

[116] R. G. Larson, Coseparable Hopf algebras, J. Pure Appl. Algebra 3 (1973), 261-267.

[117] R. G. Larson, D. E. Radford, Semisimple cosemisimple Hopf algebras, Am. J. Math. 110 (1988), 187-195.

[118] R. G. Larson, D. E. Radford, Finite dimensional cosemisimple Hopf algebras in characteristic zero are semisimple, J. Algebra 117 (1988), 267-289.

[119] R. G. Larson, D. E. Radford, Semisimple Hopf algebras, J. Algebra 171 (1995), 5-35.

[120] R. G. Larson, M. E. Sweedler, An associative orthogonal form for Hopf algebras, Amer. J. Math. 91 (1969), 75-93.

[121] B. Lemonnier, Dimension de Krull et dualité de Morita dans les extensions triangulaires, Comm. Algebra 12 (1984), 3071-3110.

[122] B.I.-P. Lin, Products of torsion theories and applications to coalgebras, Osaka J. Math. 12 (1975), 433-439.

[123] B.I.-P. Lin, Semiperfect coalgebras, J. Algebra 49 (1977), 357-373.

[124] F.W. Long, The Brauer group of dimodule algebras, J. Algebra **30** (1974), 559-601.

[125] M. Lorenz, Representations of finite-dimensional Hopf algebras, J. Algebra 188 (1997), 476-505.

[126] M. Lorenz, On the class equation for Hopf algebras, Proc. Amer. Math. Soc. 126 (1998), 2841-2844.

[127] M. E. Lorenz, M. Lorenz, On crossed products of Hopf algebras, Proc. Amer. Math. Soc. 123 (1995), 33-38.

[128] G. Lusztig, Introduction to quantum groups, Birkhäuser, 1993.

[129] S. Majid, Crossed products by braided groups and bosonization, J. Algebra 163 (1994), 165-190.

[130] S. Majid, Foundations of quantum group theory, Cambridge Univ. Press, 1995.

[131] S. Majid, Y. Soibelman, Bicrossproduct structure of the quantum Weyl group, J. Algebra 163 (1994), 68-87.

[132] A. Masuoka, On Hopf algebras with commutative coradicals, J. Algebra 144 (1991), 415-466.

[133] A. Masuoka, Freeness of Hopf algebras over coideal subalgebras, Comm. Algebra 20 (1992), 1353-1373.

[134] A. Masuoka, Coideal subalgebras in finite Hopf algebras, J. Algebra 163 (1994), 819-831.

[135] A. Masuoka, Quotient theory of Hopf algebras, Advances in Hopf algebras, 107-133, Lecture Notes in Pure and Appl. Math. 158, M. Dekker, 1994.

[136] A. Masuoka, Semisimple Hopf algebras of dimension 6, 8, Israel J. Math. 92 (1995), 361-373.

[137] A. Masuoka, Semisimple Hopf algebras of dimension $2p$, Comm. Algebra 23 (1995), 1931-1940.

[138] A. Masuoka, Semisimple Hopf algebras of dimension p^3 obtained by an extension, J. Algebra 178 (1995), 791-806.

[139] A. Masuoka, The p^n-theorem for semisimple Hopf algebras, Proc. Amer. Math. Soc. 124 (1996), 735-737.

[140] A. Masuoka, Some further classification results on semisimple Hopf algebras, Comm. Algebra 24 (1996), 307-329.

[141] A. Masuoka, Y. Doi, Generalization of cleft comodule algebras, Comm. Algebra 20 (1992), 3703-3721.

[142] J. McConnell, M. E. Sweedler, Simplicity of smash products, Proc. London Math. Soc. 23 (1971), 251-266.

[143] C. Menini, M. Zuccoli, Equivalence theorems and Hopf-Galois extensions, J. Algebra 194 (1997), 245-274.

[144] C. Menini, Ş. Raianu, Morphisms of relative Hopf modules, smash products and duality, J. Algebra 219 (1999), 547-570.

[145] C. Menini, B. Torrecillas, R. Wisbauer, Strongly regular comodules and semiperfect Hopf algebras over QF rings, to appear in J. Pure Appl. Algebra.

[146] J. W. Milnor, J. C. Moore, On the structure of Hopf algebras, Annals of Math. 81 (1965), 211-264.

[147] R.K. Molnar, Semi-Direct Products of Hopf Algebras, J. Algebra, 47 (1977), 29-51.

[148] B. Mitchell, Theory of categories, Academic Press, New York, 1965.

[149] S. Montgomery, Hopf algebras and their actions on rings, CBMS Reg. Conf. Series 82, Providence, R.I., 1993.

[150] S. Montgomery, Hopf Galois extensions, AMS Contemp. Math. 124 (1992), 129-140.

[151] S. Montgomery, Some remarks on filtrations of Hopf algebras, Comm. Algebra 21 (1993), 999-1007.

[152] S. Montgomery, Indecomposable coalgebras, simple comodules and pointed Hopf algebras, Proc. Amer. Math. Soc. 123 (1995), 2343-2351.

[153] S. Montgomery, Classifying finite-dimensional semisimple Hopf algebras, A.M.S. Contemp. Math., 229 (1998), 265-279.

[154] E. Müller, Finite subgroups of the quantum general linear group, to appear in Proc. London Math. Soc.

[155] I. M. Musson, Finite quantum groups and pointed Hopf algebras, preprint.

[156] A. Nakajima, Cosemisimple coalgebras and coseparable coalgebras over coalgebras, Math. J. Okayama Univ. 21 (1979), 125-140.

[157] T. Nakayama, On Frobenius algebras I, Ann.of Math 40 (1939), 611-633.

[158] T. Nakayama, On Frobenius algebras II, Ann.of Math 42 (1941), 1-21.

[159] C. Năstăsescu, B. Torrecillas, Torsion theories for coalgebras, J. Pure Appl. Algebra 97 (1994), 203-220.

[160] C. Năstăsescu, B. Torrecillas, Colocalization on Grothendieck categories with applications to coalgebras, J. Algebra 185 (1996), 108-124.

[161] C. Năstăsescu, B. Torrecillas, Y. Zhang, Hereditary coalgebras, Comm. Algebra 24 (1996), 1521-1528.

[162] C. Năstăsescu, J. Gomez Torrecillas, Quasi-co-Frobenius coalgebras, J. Algebra 174 (1995), 909-923.

[163] C. Năstăsescu, F. Van Oystaeyen, Graded Ring Theory, North-Holland, 1982.

[164] C. Năstăsescu, F. Panaite, F. Van Oystaeyen, External homogenization for Hopf algebras: applications to Maschke's theorem, Algebr. Represent. Theory 2 (1999), 211-226.

[165] S. Natale, On semisimple Hopf algebras of dimension pq^2, J. Algebra 221 (1999), 242-278.

[166] S. Natale, On semisimple Hopf algebras of dimension pq^2.II, to appear in Algebr. Represent. Theory.

[167] S. Natale, Hopf algebras of dimension 12, preprint.

[168] K. Newman, A correspondence between bi-ideals and sub-Hopf algebras in cocommutative Hopf algebras, J. Algebra 36 (1975), 1-15.

[169] W. D. Nichols, Bialgebras of type one, Comm. Algebra 6 (1978), 1521-1552.

[170] W. D. Nichols, Cosemisimple Hopf algebras, in Advances in Hopf Algebras, edited by J. Bergen and S. Montgomery, Marcel Dekker Lecture Notes in Pure and Appl. Math., vol. 158 (1994), 135-151.

[171] W. D. Nichols, M. B. Zoeller, Finite dimensional Hopf algebras are free over grouplike subalgebras, J. Pure Appl. Algebra 56 (1989), 51-57.

[172] W. D. Nichols, M. B. Zoeller, Freeness of infinite dimensional Hopf algebras over grouplike subalgebras, Comm. Algebra 17 (1989), 413-424.

[173] W. D. Nichols, M. B. Zoeller, A Hopf algebra freeness theorem, Amer. J. Math. 111 (1989), 381-385.

[174] W. D. Nichols, M. B. Richmond, Freeness of infinite dimensional Hopf algebras, Comm. Algebra 26 (1998), 1081-1095.

[175] U. Oberst, H.-J. Schneider, Über Untergruppen endlicher algebraischer Gruppen, Manuscripta Math. 8 (1973), 217-241.

[176] U. Oberst, H.-J. Schneider, Untergruppen formeller Gruppen von endlichem Index, J. Algebra 31 (1974), 10-44.

[177] J. Osterburg, D. Quinn, Cocommutative Hopf algebra actions and the Connes spectrum, J. Algebra 165 (1994), 465-475.

[178] B. Pareigis, When Hopf algebras are Frobenius algebras, J. Algebra, 18 (1971), 588-596.

[179] B. Pareigis, Four lectures on Hopf algebras, Centre de Recerca Matematica, Insitut d'Estudis Catalans, No. 6, 1984.

[180] D. S. Passman, Infinite crossed products, Academic Press., New York, 1989.

[181] D. Passman, D. Quinn, Burnside's theorem for Hopf algebras, Proc. Amer. Math. Soc. 123 (1995), 327-333.

[182] D. Passman, D. Quinn, Trans. Amer. Math. Soc. 347 (1995), 327-333.

[183] Richard S. Pierce, Associative algebras, Springer G.T.M., Springer Verlag, 1982.

[184] D. Quinn, Group-graded rings and duality, Trans. Amer. Math. Soc. 292 (1985), 155-167.

[185] D. E. Radford, Coreflexive coalgebras, J. Algebra 26 (1973), 512-535.

[186] D. E. Radford, On the structure of ideals of the dual algebra of a coalgebra, Trans. Amer. Math. Soc. 198 (1974), 123-137.

[187] D. Radford, The order of the antipode of a finite dimensional Hopf algebra is finite, Amer. J. Math. 98 (1976), 333-355.

[188] D. E. Radford, Pointed Hopf algebras are free over Hopf subalgebras, J. Algebra 45 (1977), 266-273.

[189] D. Radford, Finiteness conditions for a Hopf algebra with a nonzero integral, J. Algebra 46 (1977), 189-195.

[190] D. E. Radford, Freeness (projectivity) criteria for Hopf algebras over Hopf subalgebras, J. Pure Appl. Algebra 11 (1977), 15-28.

[191] D. E. Radford, Operators on Hopf algebras, Am. J. Math. 99 (1977), 139-158.

[192] D. E. Radford, On the structure of cocommutative pointed Hopf algebras, J. Algebra 50 (1978), 284-296.

[193] D. E. Radford, On the structure of pointed coalgebras, J. Algebra 77 (1982), 1-14.

[194] D. E. Radford, On the antipode of a cosemisimple Hopf algebra, J. Algebra 88 (1984), 68-88.

[195] D. E. Radford, The structure of Hopf algebras with a projection, J. Algebra 92 (1985), 322-347.

[196] D. E. Radford, The group of autpmorphisms of a semisimple Hopf algebra over a field of characteristic 0 is finite, Am. J. Math. 112 (1990), 331-357.

[197] Ş. Raianu, M. Saorín, Hopf-Galois extensions equivalent to crossed products, preprint.

[198] Ş. Raianu, An easy proof for the uniqueness of integrals, to appear in the Proceedings of the Brussels Conference 1998, M. Dekker.

[199] W. Rudin, Real and complex analysis, 3rd edition, New York, McGraw-Hill, 1987.

[200] P. Schauenburg, Hopf modules and Yetter-Drinfel'd modules, J. Algebra, 169 (1994), 874-890.

[201] H.-J. Schneider, Zerlegbare Untergruppen affiner Gruppen, Math. Ann. 255 (1981), 139-158.

[202] H.-J. Schneider, Representation Theory of Hopf Galois Extensions, Israel J. Math., 72 (1990), 196-231.

[203] H.-J. Schneider, Principal homogeneous spaces for arbitrary Hopf algebras, Israel J. Math. 72 (1990), 167-195.

[204] H.-J. Schneider, Normal basis and transitivity of crossed products for Hopf algebras, J. Algebra 152 (1992), 289-312.

[205] H. -J. Schneider, Some remarks on exact sequences of quantum groups, Comm. Algebra 21 (1993), 3337-3357.

[206] H.-J. Schneider, Hopf Galois extensions, crossed products and Clifford Theory, in Advances in Hopf Algebras, edited by J. Bergen and S. Montgomery, Marcel Dekker Lecture Notes in Pure and Appl. Math., vol. 158 (1994), 267-298.

[207] H.-J. Schneider, Lectures on Hopf algebras, Trabajos de Matematica, Córdoba, 31 (1995).

[208] W. Singer, Extension theory for connected Hopf algebras, J. Algebra 21 (1972), 1-16.

[209] Y. Sommerhäuser, On Kaplansky's fifth conjecture, J. Algebra 204 (1998), 202-224.

[210] Y. Sommerhäuser, On Kaplansky's conjectures, preprint, University of Munich, 1998.

[211] D.Ştefan, The uniqueness of integrals. A homological approach, Comm. Algebra 23 (1995), 1657-1662.

[212] D.Ştefan, Hopf subalgebras of pointed Hopf algebras and applications, Proc. Amer. Math. Soc. 125 91997), 3191-3193.

[213] D.Ştefan, The set of types of n-dimensional semisimple and cosemisimple Hopf algebras is finite, J. Algebra 193 (1997), 571-580.

[214] D.Ştefan, Hopf algebras of low dimension, J. Algebra 211 (1999), 343-361.

[215] D.Ştefan, F. Van Oystaeyen, Hochschild cohomology and the coradical filtration of pointed coalgebras: applications, J. Algebra 210 (1998), 535-556.

[216] B. Stenström, Rings of quotients, Springer, Berlin, 1975.

[217] J.B. Sullivan, The Uniqueness of Integrals for Hopf Algebras and Some Existence Theorems of Integrals for Commutative Hopf Algebras, J. Algebra, 19 (1971), 426-440.

[218] M.E. Sweedler, Hopf Algebras, Benjamin New York, 1969.

[219] M.E. Sweedler, Integrals for Hopf algebras, Ann. of Math. 89 (1969), 323-335.

[220] E. J. Taft, The order of the antipode of finite-dimensional Hopf algebra, Proc. Natl. Acad. Sci. USA 68 (1971), 2631-2633.

[221] E. J. Taft, Reflexivity of algebras and coalgebras, Amer. J. Math. 94 (1972), 1111-1130.

[222] E. J. Taft, Reflexivity of algebras and coalgebras II, Comm. Algebra 5 (1977), 1549-1560.

[223] E. J. Taft, R. L. Wilson, On antipodes in pointed Hopf algebras, J. Algebra 29 (1974), 27-32.

[224] E. J. Taft, R. L. Wilson, Hopf algebras with non-semisimple antipode, Proc. Amer. Math. Soc. 49 (1975), 269-276.

[225] E. J. Taft, R. L. Wilson, There exist finite dimensional Hopf algebras with antipodes of arbitrary even order, J. Algebra 62 (1980), 283-291.

[226] M. Takeuchi, On the dimension of the space of integrals of Hopf algebras, J. Algebra 21 (1972), 174-177.

[227] M. Takeuchi, There exists a Hopf algebra whose antipode is not injective, Sci. papers College general Educ., univ. Tokyo 21 (1971), 127-130.

[228] M. Takeuchi, A correspondence between Hopf ideals and sub-Hopf algebras, Manuscr. Math. 7 (1972), 251-270.

[229] M. Takeuchi, Morita Theorems for Categories of Comodules, J. Fac. of Sci. Univ. Tokyo, 24 (1977), 629-644.

[230] M. Takeuchi, Relative Hopf modules- equivalences and freeness criteria, J. Algebra 60 (1979), 452-471.

[231] A. A. Totok, On invariants of finite dimensional Hopf algebras, Vestnik Moskovskogo Universiteta. Matematika, Mekhanika 3 (1997), 31-34 (in Russian).

[232] A. A. Totok, Actions of Hopf algebras, Matematichesky Sbornik 189 (1998), 149-160 (in Russian).

[233] K.-H. Ulbrich, Smash products and comodules of linear maps, Tsukuba J. Math. 14 (1990), 371-378.

[234] K.-H. Ulbrich, Vollgraduierte Algebren, Abh. Math. Sem. Univ. Hamburg 51 (1981), 136-148.

[235] M. Van den Bergh, A duality theorem for Hopf algebras, in Methods in Ring Theory, NATO ASI Series vol. 129, Reidel, Dordrecht, 1984, 517-522.

[236] A. Van Daele, An algebraic framework for group duality, Adv. Math. 140 (1998), 323-366.

[237] A. Van Daele, Y. Zhang, Galois Theory for Multiplier Hopf Algebras with Integrals, Algebra Representation Theory 2 (1999), 83-106.

[238] F. Van Oystaeyen, Y.H. Zhang, H-module endomorphism rings, J. Pure and Appl. Algebra, 102 (1995), 207-219.

[239] R. B. Warfield, A Krull-Schmidt theorem for infinite sums of modules, Proc. Amer. Math. Soc. 22 (1969), 460-465.

[240] W. C. Waterhouse, Introduction to affine group schemes, Springer Verlag, Berlin, 1979.

[241] E.A. Whelan, Finite subnormalizing extensions of rings, J. Algebra 99 (1986), 418-432.

[242] D. Wigner, Lecture at UIA Antwerp, 1996.

[243] R. Williams, Ph. D. thesis, Florida State University, 1988.

[244] R. Wisbauer, Introduction to coalgebras and comodules, Universität Düsseldorf, 1996.

[245] S. L. Woronowicz, Differential calculus on compact matrix pseudogroups (quantum groups), Comm. Math. Phys., 122 (1989), 125-170.

[246] S. Zhu, Integrality of module algebras over its invariants, J. Algebra 180 (1996), 187-205.

[247] Y. Zhu, Hopf algebras of prime dimension, Internat. Math. Res. Notices 1 (1994), 53-59.

Index