volume 158

lecture notes in pure and applied mathematics

advances in Hopf algebras

edited by
Jeffrey Bergen
Susan Montgomery

advances in Hopf algebras

LECTURE NOTES IN PURE AND APPLIED MATHEMATICS

1. *N. Jacobson,* Exceptional Lie Algebras
2. *L.-Å. Lindahl and F. Poulsen,* Thin Sets in Harmonic Analysis
3. *I. Satake,* Classification Theory of Semi-Simple Algebraic Groups
4. *F. Hirzebruch, W. D. Newmann, and S. S. Koh, Differentiable Manifolds and Quadratic Forms*
5. *I. Chavel,* Riemannian Symmetric Spaces of Rank One
6. *R. B. Burckel,* Characterization of C(X) Among Its Subalgebras
7. *B. R. McDonald, A. R. Magid, and K. C. Smith,* Ring Theory: Proceedings of the Oklahoma Conference
8. *Y.-T. Siu,* Techniques of Extension on Analytic Objects
9. *S. R. Caradus, W. E. Pfaffenberger, and B. Yood,* Calkin Algebras and Algebras of Operators on Banach Spaces
10. *E. O. Roxin, P.-T. Liu, and R. L. Sternberg,* Differential Games and Control Theory
11. *M. Orzech and C. Small,* The Brauer Group of Commutative Rings
12. *S. Thomier,* Topology and Its Applications
13. *J. M. Lopez and K. A. Ross,* Sidon Sets
14. *W. W. Comfort and S. Negrepontis,* Continuous Pseudometrics
15. *K. McKennon and J. M. Robertson,* Locally Convex Spaces
16. *M. Carmeli and S. Malin,* Representations of the Rotation and Lorentz Groups: An Introduction
17. *G. B. Seligman,* Rational Methods in Lie Algebras
18. *D. G. de Figueiredo,* Functional Analysis: Proceedings of the Brazilian Mathematical Society Symposium
19. *L. Cesari, R. Kannan, and J. D. Schuur,* Nonlinear Functional Analysis and Differential Equations: Proceedings of the Michigan State University Conference
20. *J. J. Schäffer,* Geometry of Spheres in Normed Spaces
21. *K. Yano and M. Kon,* Anti-Invariant Submanifolds
22. *W. V. Vasconcelos,* The Rings of Dimension Two
23. *R. E. Chandler,* Hausdorff Compactifications
24. *S. P. Franklin and B. V. S. Thomas,* Topology: Proceedings of the Memphis State University Conference
25. *S. K. Jain,* Ring Theory: Proceedings of the Ohio University Conference
26. *B. R. McDonald and R. A. Morris,* Ring Theory II: Proceedings of the Second Oklahoma Conference
27. *R. B. Mura and A. Rhemtulla,* Orderable Groups
28. *J. R. Graef,* Stability of Dynamical Systems: Theory and Applications
29. *H.-C. Wang,* Homogeneous Branch Algebras
30. *E. O. Roxin, P.-T. Liu, and R. L. Sternberg,* Differential Games and Control Theory II
31. *R. D. Porter,* Introduction to Fibre Bundles
32. *M. Altman,* Contractors and Contractor Directions Theory and Applications
33. *J. S. Golan,* Decomposition and Dimension in Module Categories
34. *G. Fairweather,* Finite Element Galerkin Methods for Differential Equations
35. *J. D. Sally,* Numbers of Generators of Ideals in Local Rings
36. *S. S. Miller,* Complex Analysis: Proceedings of the S.U.N.Y. Brockport Conference
37. *R. Gordon,* Representation Theory of Algebras: Proceedings of the Philadelphia Conference
38. *M. Goto and F. D. Grosshans,* Semisimple Lie Algebras
39. *A. I. Arruda, N. C. A. da Costa, and R. Chuaqui,* Mathematical Logic: Proceedings of the First Brazilian Conference
40. *F. Van Oystaeyen,* Ring Theory: Proceedings of the 1977 Antwerp Conference
41. *F. Van Oystaeyen and A. Verschoren,* Reflectors and Localization: Application to Sheaf Theory
42. *M. Satyanarayana,* Positively Ordered Semigroups
43. *D. L Russell,* Mathematics of Finite-Dimensional Control Systems
44. *P.-T. Liu and E. Roxin,* Differential Games and Control Theory III: Proceedings of the Third Kingston Conference, Part A
45. *A. Geramita and J. Seberry,* Orthogonal Designs: Quadratic Forms and Hadamard Matrices
46. *J. Cigler, V. Losert, and P. Michor,* Banach Modules and Functors on Categories of Banach Spaces

47. *P.-T. Liu and J. G. Sutinen,* Control Theory in Mathematical Economics: Proceedings of the Third Kingston Conference, Part B
48. *C. Byrnes,* Partial Differential Equations and Geometry
49. *G. Klambauer,* Problems and Propositions in Analysis
50. *J. Knopfmacher,* Analytic Arithmetic of Algebraic Function Fields
51. *F. Van Oystaeyen,* Ring Theory: Proceedings of the 1978 Antwerp Conference
52. *B. Kadem,* Binary Time Series
53. *J. Barros-Neto and R. A. Artino,* Hypoelliptic Boundary-Value Problems
54. *R. L. Sternberg, A. J. Kalinowski, and J. S. Papadakis,* Nonlinear Partial Differential Equations in Engineering and Applied Science
55. *B. R. McDonald,* Ring Theory and Algebra III: Proceedngs of the Third Oklahoma Conference
56. *J. S. Golan,* Structure Sheaves Over a Noncommutative Ring
57. *T. V. Narayana, J. G. Williams, and R. M. Mathsen,* Combinatorics, Representation Theory and Statistical Methods in Groups: YOUNG DAY Proceedings
58. *T. A. Burton,* Modeling and Differential Equations in Biology
59. *K. H. Kim and F. W. Roush,* Introduction to Mathematical Consensus Theory
60. *J. Banas and K. Goebel,* Measures of Noncompactness in Banach Spaces
61. *O. A. Nielson,* Direct Integral Theory
62. *J. E. Smith, G. O. Kenny, and R. N. Ball,* Ordered Groups: Proceedings of the Boise State Conference
63. *J. Cronin,* Mathematics of Cell Electrophysiology
64. *J. W. Brewer,* Power Series Over Commutative Rings
65. *P. K. Kamthan and M. Gupta,* Sequence Spaces and Series
66. *T. G. McLaughlin,* Regressive Sets and the Theory of Isols
67. *T. L. Herdman, S. M. Rankin III, and H. W. Stech,* Integral and Functional Differential Equations
68. *R. Draper,* Commutative Algebra: Analytic Methods
69. *W. G. McKay and J. Patera,* Tables of Dimensions, Indices, and Branching Rules for Representations of Simple Lie Algebras
70. *R. L. Devaney and Z. H. Nitecki,* Classical Mechanics and Dynamical Systems
71. *J. Van Geel,* Places and Valuations in Noncommutative Ring Theory
72. *C. Faith,* Injective Modules and Injective Quotient Rings
73. *A. Fiacco,* Mathematical Programming with Data Perturbations I
74. *P. Schultz, C. Praeger, and R. Sullivan,* Algebraic Structures and Applications: Proceedings of the First Western Australian Conference on Algebra
75. *L Bican, T. Kepka, and P. Nemec,* Rings, Modules, and Preradicals
76. *D. C. Kay and M. Breen,* Convexity and Related Combinatorial Geometry: Proceedings of the Second University of Oklahoma Conference
77. *P. Fletcher and W. F. Lindgren,* Quasi-Uniform Spaces
78. *C.-C. Yang,* Factorization Theory of Meromorphic Functions
79. *O. Taussky,* Ternary Quadratic Forms and Norms
80. *S. P. Singh and J. H. Burry,* Nonlinear Analysis and Applications
81. *K. B. Hannsgen, T. L. Herdman, H. W. Stech, and R. L. Wheeler,* Volterra and Functional Differential Equations
82. *N. L. Johnson, M. J. Kallaher, and C. T. Long,* Finite Geometries: Proceedings of a Conference in Honor of T. G. Ostrom
83. *G. I. Zapata,* Functional Analysis, Holomorphy, and Approximation Theory
84. *S. Greco and G. Valla,* Commutative Algebra: Proceedings of the Trento Conference
85. *A. V. Fiacco,* Mathematical Programming with Data Perturbations II
86. *J.-B. Hiriart-Urruty, W. Oettli, and J. Stoer,* Optimization: Theory and Algorithms
87. *A. Figa Talamanca and M. A. Picardello,* Harmonic Analysis on Free Groups
88. *M. Harada,* Factor Categories with Applications to Direct Decomposition of Modules
89. *V. I. Istrăţescu,* Strict Convexity and Complex Strict Convexity
90. *V. Lakshmikantham,* Trends in Theory and Practice of Nonlinear Differential Equations
91. *H. L. Manocha and J. B. Srivastava,* Algebra and Its Applications
92. *D. V. Chudnovsky and G. V. Chudnovsky,* Classical and Quantum Models and Arithmetic Problems
93. *J. W. Longley,* Least Squares Computations Using Orthogonalization Methods
94. *L. P. de Alcantara,* Mathematical Logic and Formal Systems
95. *C. E. Aull,* Rings of Continuous Functions
96. *R. Chuaqui,* Analysis, Geometry, and Probability
97. *L. Fuchs and L. Salce,* Modules Over Valuation Domains

98. *P. Fischer and W. R. Smith,* Chaos, Fractals, and Dynamics
99. *W. B. Powell and C. Tsinakis,* Ordered Algebraic Structures
100. *G. M. Rassias and T. M. Rassias,* Differential Geometry, Calculus of Variations, and Their Applications
101. *R.-E. Hoffmann and K. H. Hofmann,* Continuous Lattices and Their Applications
102. *J. H. Lightbourne III and S. M. Rankin III,* Physical Mathematics and Nonlinear Partial Differential Equations
103. *C. A. Baker and L, M. Batten,* Finite Geometrics
104. *J. W. Brewer, J. W. Bunce, and F. S. Van Vleck,* Linear Systems Over Commutative Rings
105. *C. McCrory and T. Shifrin,* Geometry and Topology: Manifolds, Varieties, and Knots
106. *D. W. Kueker, E. G. K. Lopez-Escobar, and C. H. Smith,* Mathematical Logic and Theoretical Computer Science
107. *B.-L. Lin and S. Simons,* Nonlinear and Convex Analysis: Proceedings in Honor of Ky Fan
108. *S. J. Lee,* Operator Methods for Optimal Control Problems
109. *V. Lakshmikantham,* Nonlinear Analysis and Applications
110. *S. F. McCormick,* Multigrid Methods: Theory, Applications, and Supercomputing
111. *M. C. Tangora,* Computers in Algebra
112. *D. V. Chudnovsky and G. V. Chudnovsky,* Search Theory: Some Recent Developments
113. *D. V. Chudnovsky and R. D. Jenks,* Computer Algebra
114. *M. C. Tangora,* Computers in Geometry and Topology
115. *P. Nelson, V. Faber, T. A. Manteuffel, D. L. Seth, and A. B. White, Jr.,* Transport Theory, Invariant Imbedding, and Integral Equations: Proceedings in Honor of G. M. Wing's 65th Birthday
116. *P. Clément, S. Invernizzi, E. Mitidieri, and I. I. Vrabie,* Semigroup Theory and Applications
117. *J. Vinuesa,* Orthogonal Polynomials and Their Applications: Proceedings of the International Congress
118. *C. M. Dafermos, G. Ladas, and G. Papanicolaou,* Differential Equations: Proceedings of the EQUADIFF Conference
119. *E. O. Roxin,* Modern Optimal Control: A Conference in Honor of Solomon Lefschetz and Joseph P. Lasalle
120. *J. C. Díaz,* Mathematics for Large Scale Computing
121. *P. S. Milojević,* Nonlinear Functional Analysis
122. *C. Sadosky,* Analysis and Partial Differential Equations: A Collection of Papers Dedicated to Mischa Cotlar
123. *R. M. Shortt,* General Topology and Applications: Proceedings of the 1988 Northeast Conference
124. *R. Wong,* Asymptotic and Computational Analysis: Conference in Honor of Frank W. J. Olver's 65th Birthday
125. *D. V. Chudnovsky and R. D. Jenks,* Computers in Mathematics
126. *W. D. Wallis, H. Shen, W. Wei, and L. Zhu,* Combinatorial Designs and Applications
127. *S. Elaydi,* Differential Equations: Stability and Control
128. *G. Chen, E. B. Lee, W. Littman, and L. Markus,* Distributed Parameter Control Systems: New Trends and Applications
129. *W. N. Everitt,* Inequalities: Fifty Years On from Hardy, Littlewood and Pólya
130. *H. G. Kaper and M. Garbey,* Asymptotic Analysis and the Numerical Solution of Partial Differential Equations
131. *O. Arino, D. E. Axelrod, and M. Kimmel,* Mathematical Population Dynamics: Proceedings of the Second International Conference
132. *S. Coen,* Geometry and Complex Variables
133. *J. A. Goldstein, F. Kappel, and W. Schappacher,* Differential Equations with Applications in Biology, Physics, and Engineering
134. *S. J. Andima, R. Kopperman, P. R. Misra, J. Z. Reichman, and A. R. Todd,* General Topology and Applications
135. *P Clément, E. Mitidieri, B. de Pagter,* Semigroup Theory and Evolution Equations: The Second International Conference
136. *K. Jarosz,* Function Spaces
137. *J. M. Bayod, N. De Grande-De Kimpe, and J. Martínez-Maurica,* *p*-adic Functional Analysis
138. *G. A. Anastassiou,* Approximation Theory: Proceedings of the Sixth Southeastern Approximation Theorists Annual Conference
139. *R. S. Rees,* Graphs, Matrices, and Designs: Festschrift in Honor of Norman J. Pullman
140. *G. Abrams, J. Haefner, and K. M. Rangaswamy,* Methods in Module Theory

141. *G. L. Mullen and P. J.-S. Shiue*, Finite Fields, Coding Theory, and Advances in Communications and Computing
142. *M. C. Joshi and A. V. Balakrishnan*, Mathematical Theory of Control: Proceedings of the International Conference
143. *G. Komatsu and Y. Sakane*, Complex Geometry: Proceedings of the Osaka International Conference
144. *I. J. Bakelman*, Geometric Analysis and Nonlinear Partial Differential Equations
145. *T. Mabuchi and S. Mukai*, Einstein Metrics and Yang–Mills Connections: Proceedings of the 27th Taniguchi International Symposium
146. *L. Fuchs and R. Göbel*, Abelian Groups: Proceedings of the 1991 Curaçao Conference
147. *A. D. Pollington and W. Moran*, Number Theory with an Emphasis on the Markoff Spectrum
148. *G. Dore, A. Favini, E. Obrecht, and A. Venni*, Differential Equations in Banach Spaces
149. *T. West*, Continuum Theory and Dynamical Systems
150. *K. D. Bierstedt, A. Pietsch, W. Ruess, and D. Vogt*, Functional Analysis
151. *K. G. Fischer, P. Loustaunau, J. Shapiro, E. L. Green, and D. Farkas*, Computational Algebra
152. *K. D. Elworthy, W. N. Everitt, and E. B. Lee*, Differential Equations, Dynamical Systems, and Control Science
153. *P.-J. Cahen, D. L. Costa, M. Fontana, and S.-E. Kabbaj*, Commutative Ring Theory
154. *S. C. Cooper and W. J. Thron*, Continued Fractions and Orthogonal Functions: Theory and Applications
155. *P. Clément and G. Lumer*, Evolution Equations, Control Theory, and Biomathematics
156. *M. Gyllenberg and L. Persson*, Analysis, Algebra, and Computers in Mathematical Research: Proceedings of the Twenty-First Nordic Congress of Mathematicians
157. *W. O. Bray, P. S. Milojević, and Č. V. Stanojević*, Fourrier Analysis: Analytic and Geometric Aspects
158. *J. Bergen and S. Montgomery*, Advances in Hopf Algebras

Additional Volumes in Preparation

advances in Hopf algebras

edited by

Jeffrey Bergen
DePaul University
Chicago, Illinois

Susan Montgomery
University of Southern California
Los Angeles, California

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

First published 1994 by Marcel Dekker

Published 2018 by CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

First issued in hardback 2018

ISBN 13: 978-1-138-40180-8 (hbk)
ISBN 13: 978-0-8247-9065-3 (pbk)

Library of Congress Cataloging-in-Publication Data

Advances in Hopf algebras / edited by Jeffrey Bergen, Susan Montgomery.
p. cm. -- (Lecture notes in pure and applied mathematics ; v. 158)
Lectures from a conference held Aug. 10-14, 1992 at DePaul University in Chicago.
Includes bibliographical references
ISBN 0—8247—9065—0 (acid-free)
1. Hopf algebras--Congresses. I. Bergen, Jeffrey. II. Montgomery, Susan. III. Series.
QA613.8.A38 1994
510'.55--dc20 94-804
CIP

DOI: 10.1201/9781003419792

Preface

The NSF-CBMS conference Hopf Algebras and Their Actions on Rings was held at DePaul University in Chicago, Illinois. The conference featured a series of ten lectures by Susan Montgomery as well as nine supporting lectures by Miriam Cohen, Yukio Doi, Warren Nichols, Bodo Pareigis, Donald Passman, David Radford, Hans-Jurgen Schneider, Earl Taft, and Mitsuhiro Takeuchi. The conference, which served as a "summer school" for both experts and nonexperts in the field, attracted approximately 90 participants representing 11 countries.

This volume contains the expository lectures by the nine supporting lecturers as well as invited expository papers by Lindsay Childs and David Moss, Shahn Majid, and Akira Masuoka. The lectures by Susan Montgomery appear in the Conference Board of the Mathematical Sciences series published by the American Mathematical Society.

We would like to thank the National Science Foundation and the University Research Council at DePaul University for their financial support of this conference. We would also like to thank Maria Allegra of Marcel Dekker, Inc., for her assistance in putting this volume together. Finally, we thank all of our anonymous referees.

Jeffrey Bergen
Susan Montgomery

Contents

Contributors

LINDSAY CHILDS State University of New York, Albany, New York

M. COHEN Ben Gurion University, Beer Sheva, Israel

YUKIO DOI Fukui University, Fukui, Japan

SHAHN MAJID Cambridge University, Cambridge, England

AKIRA MASUOKA Shimane University, Matsue, Shimane, Japan

DAVID J. MOSS State University of New York, Albany, New York

WARREN D. NICHOLS Florida State University, Tallahassee, Florida

BODO PAREIGIS University of Munich, Munich, Germany

D. S. PASSMAN University of Wisconsin, Madison, Wisconsin

DAVID E. RADFORD University of Illinois—Chicago, Chicago, Illinois

H.-J. SCHNEIDER University of Munich, Munich, Germany

EARL J. TAFT Rutgers University, New Brunswick, New Jersey

MITSUHIRO TAKEUCHI University of Tsukuba, Tsukuba, Ibaraki, Japan

Hopf Algebras and Local Galois Module Theory

LINDSAY CHILDS State University of New York, Albany, New York
DAVID J. MOSS State University of New York, Albany, New York

Let $L \supset K$ be a finite Galois extension of algebraic number fields with Galois group G, and with rings of integers $S \supset R$. Galois module theory seeks to understand S as an RG-module. If L/K is tamely ramified, then S is a locally free RG-module by a classical theorem of E. Noether, and a rich theory has been developed to understand the obstructions to freeness: see, for example [$F83$] or a forthcoming book by B. Erez. However, if L/K is wildly ramified the situation is much less well-understood, for the local structure is unclear.

In 1959 Leopoldt [$L59$] showed that a useful approach to wild extensions is to view S as a module, not over RG, but over the larger order

$$\mathcal{A}(S) = \{\alpha \in KG | \alpha S \subseteq S\}.$$

He showed that if $K = \mathbf{Q}$ and G is abelian, then S is free over $\mathcal{A}(S)$. However, Leopoldt's theorem does not extend beyond $K = \mathbf{Q}$ and G abelian, and since the appearance of Leopoldt's paper, positive results on local freeness over the Leopoldt order have been scarce.

One of the first general positive results was in [$C87$], where it was shown that if G is abelian and $\mathcal{A}(S)$ is a Hopf order in KG, then S is locally free as an $\mathcal{A}(S)$-module. This introduced the theme of "taming wild extensions with Hopf algebras".

The purpose of this paper is to offer further positive results on local freeness, built around the Hopf algebra theme. We note that this theme, when it applies, opens the possibility of extending the global theory of tame extensions to certain classes of wild extensions. Such a program has been pursued in recent work of M. Taylor and his collaborators ([$ST90$], [$T88$], [$T90a$], [$T90b$]), and is nicely described in a recent survey paper by Taylor and Byott [$TB92$].

Taylor and Byott almost always assume that L/K is a Galois extension with group G; however, in view of the work of Greither and Pareigis [$GP87$], as well as the examples of section 3, below, it will be useful to assume only that L/K is a Hopf Galois extension.

For the remainder of this introduction, assume K is a local field, a finite extension of $\mathbf{Q}_p$, with valuation ring R.

 DOI: 10.1201/9781003419792-1

In section 1, using a previously overlooked theorem of H.-J. Schneider, we show that with an appropriate notion of tameness Noether's theorem cited above generalizes to Hopf Galois extensions L/K with Hopf algebra A, where A is any finite dimensional cocommutative K-Hopf algebra. In particular, commutativity of A is not needed.

Let L/K be a Hopf Galois extension with Hopf algebra A. For an order S_0 over R in L (not necessarily the full integral closure of R in L), call

$$\mathcal{A}(S_0) = \{\alpha \text{ in } A | \alpha S_0 \subseteq S_0\}$$

the Leopoldt order of S_0. In section 2 we show that if $\mathcal{A}(S_0)$ is a Hopf order in A, then every Hopf order H over R in A containing $\mathcal{A}(S_0)$ is the Leopoldt order for some order S in L such that S is free over H.

In sections 3 and 4 we study Kummer extensions with respect to a formal group of dimension one. This is a class of extensions $S \supseteq R$ which are orders in Hopf Galois extensions $L \supseteq K$ and which are free over their Leopoldt orders. These extensions were introduced by Taylor [$T86$] and studied in special cases in [$T85$] and [$T87$]. They include a large collection of wildly ramified local Galois extensions L/K such that the Leopoldt order $\mathcal{A}(S)$ of the valuation ring S is Hopf and hence S is free over $\mathcal{A}(S)$. The freeness of S over $\mathcal{A}(S)$ follows from the fact that the algebras S under consideration are H-Galois objects (or in the terminology of [$TB92$], H-principal homogeneous spaces) where H is the representing Hopf algebra for a finite subgroup of the formal group. Then $\mathcal{A}(S)$ will be the dual of H; the main technical difficulty then becomes describing that dual, which we study in section 4, adapting techniques of Taylor.

In a brief final section we introduce the following question. Let L/K be an A-Hopf Galois extension, with valuation rings $S \supseteq R$. Let $\mathcal{A}(A, S)$ be the Leopoldt order of S. Does the structure of $\mathcal{A}(A, S)$ depend on A? This question is meaningful because, as Greither and Pareigis have shown ([$GP87$], c.f. [$C89$] and [$P90$]), a given extension L/K may be A-Hopf Galois for more than one Hopf algebra A. We give an example of an extension of degree 4 which is Hopf Galois for two Hopf algebras A_1 and A_2, such that only one of the corresponding Leopoldt orders of S is Hopf.

1. NOETHER'S THEOREM

The cornerstone of Galois module theory is Noether's theorem. Let L/K be a Galois extension of number fields with rings of integers S, R, respectively and Galois group G. Viewing S as an RG-module, we may ask if S is free over RG. This is the same as asking if S has a normal basis as a free R-module (or that L/K has a normal integral basis). Noether's theorem asserts that S is locally free over RG (where "local" means at the completion at any finite place of R) iff L/K is tamely ramified ("tame", for short), i.e. the ramification index of any non-zero prime ideal p of R is relatively prime to the characteristic of R/p.

Noether's theorem implies, in particular, that when L/K is wildly ramified (= "wild", i.e. not tame) there is no hope that S could be free over RG. To deal with this situation, Leopoldt introduced the idea of viewing S over the ring

$$\mathcal{A}(S) = \{\alpha \text{ in } KG | \alpha s \in S \text{ for all } s \text{ in } S\},$$

an order over R in KG which contains RG, and which we will call the Leopoldt order of S. Leopoldt [$Le59$] showed that if $K = \mathbf{Q}$ and G is abelian, then S is always free over $\mathcal{A}(S)$. However, subsequent examples showed that S need not be locally free over $\mathcal{A}(S)$ if $K \neq \mathbf{Q}$ or G is not abelian. See [$BF72a$].

In [$CH87$] (c.f. also [$W88$]), S. Hurley and the first author defined the notion of tame extension with respect to a Hopf algebra. Let S be a commutative R-algebra and an H-module algebra, where H is an R-Hopf algebra. Suppose S and H are both finitely generated projective R-modules of the same rank, and the fixed ring $S^H = R$. If I is the space of left integrals of H, then IS is contained in $S^H = R$. We called S/R tame if $IS = R$.

Assuming that H is commutative and cocommutative, we showed in [$CH86$] that S is locally isomorphic to H as an H-module if S is a tame H-extension of R.

This applies in the case where K is a number field with ring of integers R, L is a finite extension of K, S is an order contained in the ring of integers of L, and S is an H-module algebra, where H is a cocommutative R-Hopf algebra, finitely generated and projective as an R-module. If $A = K \otimes_R H$ and L is an A-Hopf Galois extension of K, then S is an H-tame extension of R if $IS = R$, where I is the space of left integrals of H. The result of [$CH86$] showed that, assuming H is also commutative, then S is locally free over H.

It turns out that the assumption of commutativity on H is not necessary, thanks to a deep result of H.-J. Schneider. In fact:

THEOREM 1.1. Let R be a complete discrete valuation ring of characteristic zero, with quotient field K. Let A be a cocommutative K-Hopf algebra, of finite rank as a K-module. Let L be a K-algebra which is a Hopf Galois extension of K with Hopf algebra A. Let H be an order over R in A with module of left integrals I and S be an order over R in L, such that S is an H- module algebra. If $IS = R$ (that is, the H-extension S/R is tame), then $S \cong H$ as left H-modules.

The proof of this is a matter of putting together two results.

One, found as Theorem 5.1 of [CH86], is that if $IS = R$ then S is H-projective. To sketch this generalization of a well-known result in representation theory of finite groups (c.f. [S77], Lemma 20, page 118): let ϑ generate the free rank one R-module I. Since $IS = R$, there is some z in S so that $\vartheta z = 1$. Now S is a free R- module, so $H \otimes_R S$, viewed as a left H-module via the H-action on H, is a projective left H-module, and the scalar multiplication map $\mu : H \otimes_R S \to S$ is a left H–module homomorphism. To show that S is H- projective, we find a left H-module splitting map ν for μ, namely $\nu : S \to H \otimes_R S$ by

$$\nu(s) = \sum_{(\vartheta)} \vartheta_{(1)} \otimes z \cdot (\vartheta^{\lambda}_{(2)} s)$$

(usual Sweedler notation, and with λ as the antipode of H). It is a technical exercise to verify that $\mu \circ \nu$ is the identity on S. One uses the fact that if ϑ is a left integral then for all h in H,

$$\sum_{(\vartheta)} h\vartheta_{(1)} \otimes \vartheta^{\lambda}_{(2)} = \sum_{(\vartheta)} \vartheta_{(1)} \otimes \vartheta^{\lambda}_{(2)} h$$

to verify that ν is a left H-module homomorphism. Technical details may be found in Theorem 5.1 of [CH86].

The other result is Schneider's. We have $K \otimes_R S \cong L$ and $K \otimes_R H \cong A$. Now L is an A-Hopf Galois extension of K, so by a result of Kreimer and Cook [KC76], $L \cong A$ as left A-modules. Hence S and H are two projective left H-modules so that $K \otimes_R S \cong K \otimes_R H$ as left $K \otimes_R H$-modules. But then Theorem 4.1 of [Sch77] applies to yield that $S \cong H$ as left H-modules. ∎

Theorem 1.1 extends Noether's theorem. For if L/K is a Galois extension of number fields with group G, and S is the integral closure of R in L, then S is tamely ramified iff the trace map $tr : S \to R$, $tr(s) = \sum_{\sigma \in G} \sigma(s)$, is onto. But $\sum_{\sigma \in G} \sigma$ generates the module of integrals I of RG. So L/K tame is equivalent to the condition $IS = R$. Schneider's theorem then plays the same role in Theorem 1.1 as Swan's theorem ([Sw60], Corollary 6.4, which Schneider's theorem extends) does in the proof of Noether's theorem (see [CF67], page 22).

This extension of Noether's theorem to Hopf orders has a nice interpretation involving the Leopoldt order. Note that S is any order over R in L, not necessarily the maximal order:

COROLLARY 1.2. With K, R, L, S and A as in Theorem 1.1, suppose the Leopoldt order $\mathcal{A}(S)$ of S in A, namely, $\mathcal{A}(S) = \{\alpha \text{ in } A | \alpha s \in S \text{ for all } s \text{ in } S\}$, is an R-Hopf algebra order in A. Then S is a free $\mathcal{A}(S)$-module.

PROOF. (c.f. [C87], Theorem 2.1). Since L/K is A-Galois, the fixed ring $L^A = \{s \text{ in } L | \text{ as} = \epsilon(a)s \text{ for all a in } A\} = K$. We have easily that $IS \subseteq S^H \subseteq L^A \cap S = R$, where I is the module of left integrals of H. Let ϕ be a generator of the one-dimensional K-space of left integrals of A. Since L is an A-Hopf Galois extension of K, $\phi L = K$ and ϕS is a fractional ideal of K. Thus $\phi S = aR$ for some a in K. But then $\vartheta = \phi/a$ is a left integral of A which maps S onto $R \subseteq S$. By definition of $H = \mathcal{A}(S)$, ϑ is in H, so is in I, and $IS = R$. The result then follows from Theorem 1.1. ∎

This result raises the question, given a Hopf Galois extension L/K of number fields with Hopf algebra A, under what conditions is the Leopoldt order

$$\mathcal{A}(S) = \{\alpha \text{ in } A | \alpha s \in S \text{ for all } s \text{ in } S\},$$

of the ring of integers S of L a Hopf order in A? This question was considered in [C87] for abelian extensions of $\mathbf{Q}$(i.e. $A = \mathbf{Q}G, G$ abelian) and for Kummer extensions of prime order.

Over $\mathbf{Q}$, it turns out that $\mathcal{A}(S)$ is Hopf iff the extension $L/\mathbf{Q}$ is tamely ramified at all odd primes, and the ramification group for $L/\mathbf{Q}$ at the prime 2 has order at most 2 ([C87], Theorem 5.1). By contrast, Leopoldt's main result in [Le59] is that S is free over $\mathcal{A}(S)$ for $A = \mathbf{Q}G$, G any finite abelian group.

In the case of Kummer extensions of a local field K of prime order p with ramification number t, $\mathcal{A}(S)$ is a Hopf order iff $t \equiv -1(\text{mod} p)$; if $t < pe_0/(p-1) - 1$, where e_0 is the ramification index of K over $\mathbf{Q}_p$, then S is free over $\mathcal{A}(S)$ iff

$t \equiv a(\text{mod} p)$ and a divides $p-1$. The first result is a reformulation by Greither [Gr92] of the main result of [C87]; the second is due to Bertrandias and Ferton [$BF72a$]; c.f. [$BF72b$] for the case $t \geq pe_0/(p-1)-1$. Greither's reformulation, with a suitably generalized ramification number, holds for any totally ramified Hopf Galois extension L/K of order p ([Gr92], Theorem 2.7).

Greither also has necessary conditions on the ramification numbers of a cyclic Galois extension L/K of degree p^2 in order that $\mathcal{A}(S)$ be Hopf (see [Gr92], Theorem 3.2).

2. ORDERING ORDERS

Rather than starting with a wildly ramified Galois extension of number fields and asking if the Leopoldt order of its ring of integers is Hopf, a relatively successful strategy has been to begin with a number field K with ring of integers R and a finite abelian group G, consider all the Hopf algebra orders over R in KG, and, for a wild extension L/K with group G, see if any Hopf algebra order is the Leopoldt order of the ring of integers of L. This was essentially the strategy of [Ch87] and [Gr92]. The basic approach is that starting from a Hopf algebra order one can construct an order over R in L. More precisely, let L be a Hopf Galois extension of K, a local number field, with Hopf algebra A. Let R be the valuation ring of K, let S be the integral closure of R in L (we do not assume L is a field) and let H be a Hopf order over R in A. Then

$$\tilde{\mathcal{O}}(H) = \{s \text{ in } L | hs \in S \text{ for all } h \text{ in } H\}$$

is a lattice in L (i.e. an R-finitely generated submodule of L which contains a K-basis of L). Taylor has observed:

PROPOSITION 2.1. $\tilde{\mathcal{O}}(H)$ is an order over R in L.

PROOF. ([T87], Lemma 3.1). To see that $\tilde{\mathcal{O}}(H)$ is an R-lattice in L, observe that since 1 is in H, $\tilde{\mathcal{O}}(H) \subseteq S$; on the other hand, if $\{h_i\}$ is an R-basis of H and $\{s_j\}$ is an R-basis of S (for $i,j = 1,\ldots,n$), then there is some r in R so that $r(h_i s_j)$ is in S for all i and j. So $rS \subseteq \tilde{\mathcal{O}}(H)$ and $\tilde{\mathcal{O}}(H)$ is a lattice. Now 1 is in $\tilde{\mathcal{O}}(H)$ because for all h in $H, h \cdot 1 = \epsilon(h) \cdot 1$ and $\epsilon(h)$ is in R, hence $h \cdot 1$ is in S for all h in H. If s,t are in $\tilde{\mathcal{O}}(H)$, then, for all h in $H, h(st) = \sum_{(h)} h_{(1)}(s) \cdot h_{(2)}(t)$ is in S. So st is in $\tilde{\mathcal{O}}(H)$. Thus $\tilde{\mathcal{O}}(H)$ is an order in L. ∎

Thus given a Hopf Galois extension L/K of number fields with Hopf algebra A, we have the map $\mathcal{A}$, from orders over R in L to orders over R in A, and the map $\tilde{\mathcal{O}}$, from orders over R in A to lattices over R in L. For an order S over R in L, sometimes $\mathcal{A}(S)$ is a Hopf order in A; if H is a Hopf order over R in A, $\tilde{\mathcal{O}}(H)$ is an order over R in L. It is not the case that $\tilde{\mathcal{O}}$ and $\mathcal{A}$ are always inverses of each other. The simplest example is to take a wildly ramified abelian extension $L/\mathbf{Q}$, with ring of integers S and Galois group G; then $\mathbf{Z}G$ acts on S, so, since S is the maximal order of L, $\tilde{\mathcal{O}}(\mathbf{Z}G) = S$. But $\mathcal{A}(S)$ is necessarily larger than $\mathbf{Z}G$, for since $L/\mathbf{Q}$ is wildly ramified, S cannot be projective over $\mathbf{Z}G$ by Noether's theorem, but Leopoldt's main theorem [Le59] is that S is free over $\mathcal{A}(S)$. Thus $\mathcal{A}\tilde{\mathcal{O}}(\mathbf{Z}G)$ is strictly larger than ZG.

The following results bear on the question of when $\mathcal{A}$ and $\tilde{\mathcal{O}}$ are inverses of each other.

PROPOSITION 2.2. Let K be a local field with valuation ring R. Let H be a commutative, cocommutative R-Hopf algebra, finitely generated and free as R-module, and $A = K \otimes_R H$. Let L be an A-Hopf Galois extension of K. Let S be an order over R in L such that S/R is a tame H-extension. Then S is a free rank one H-module and $H = \mathcal{A}(S)$. If S is an H-Galois extension of R or H is a local ring, then $S = \tilde{\mathcal{O}}(H)$, hence $H = \mathcal{A}(\tilde{\mathcal{O}}(H))$ and S is the unique order over R in L which is a tame H-extension.

The hypothesis that S is H-tame reflects a strategy often used in the theory: start with H, construct an S so that S is H-tame (a trace condition if A is a group ring), then apply this result.

PROOF. Since S/R is H-tame, by the extension of Noether's theorem, S is free of rank one.

To show $H = \mathcal{A}(S)$, first observe that since $\mathcal{A}(S) = \{a \text{ in } A \mid aS \subseteq S\}$, we have $H \subseteq \mathcal{A}(S)$. Let $S = Hw$, the free rank one H-module with basis w. Then $L = Aw$. If a is in $\mathcal{A}(S)$, then $aw \in S$, so $aw = hw$ for some h in $H \subseteq A$. But since L is A-free on w, $a = h$ in H. Hence $\mathcal{A}(S) \subseteq H$.

To show $S = \tilde{\mathcal{O}}(H)$, recall that

$$\tilde{\mathcal{O}}(H) = \{s \text{ in } L | Hs \subseteq \mathcal{O}_L\}$$

where $\mathcal{O}_L$ is the integral closure of R in L, and $HS \subseteq S \subseteq \mathcal{O}_L$, so $S \subseteq \tilde{\mathcal{O}}(H)$. First assume S is an H-Galois extension of R. The inclusion $S \subseteq \tilde{\mathcal{O}}(H)$ is an R-algebra, H-module homomorphism, hence induces an $S\#H$-module structure on $\tilde{\mathcal{O}}(H)$. But $S\#H \cong \mathrm{End}_R(S)$ since S is H- Galois, and we therefore have a Morita isomorphism $\tilde{\mathcal{O}}(H) \cong S \otimes_R \tilde{\mathcal{O}}(H)^H$ given by multiplication in $\tilde{\mathcal{O}}(H)$. But

$R \subseteq \tilde{\mathcal{O}}(H)^H \subseteq \tilde{\mathcal{O}}(H) \cap L^A \subseteq \mathcal{O}_L \cap K = R$, hence $\tilde{\mathcal{O}}(H)^H = R$ and $S = \tilde{\mathcal{O}}(H)$. Uniqueness of S follows.

If H is a local ring and $S \cong H$ as left H-module, then S is an H-Galois extension of R by [W92]. ∎

The following result says that if you find one Hopf order which is the Leopoldt order of some order in L, then the same is true for any larger Hopf order.

THEOREM 2.3. Let L/K be an A-Galois extension of local fields, and R be the valuation ring of K. Let H_0 be a Hopf order in A so that $\tilde{\mathcal{O}}(H_0)$ is H_0-tame. Then $H_0 = \mathcal{A}\tilde{\mathcal{O}}(H_0))$. If H is any Hopf order in A containing H_0, then $\tilde{\mathcal{O}}(H)$ is free over H and $\mathcal{A}\tilde{\mathcal{O}}(H)) = H$.

PROOF. That $H_0 = \mathcal{A}(\tilde{\mathcal{O}}(H_0))$ follows from Proposition 2.2.

Let ϑ_0 generate the module of left integrals of H_0. Since $S_0 = \tilde{\mathcal{O}}(H_0)$ is H_0-tame, there is a z_0 in S_0 so that $\vartheta_0 z_0 = 1$. Let ϑ generate the module of left integrals of H, then $\vartheta_0 = r\vartheta$ for some r in R, since $H_0 \subseteq H$. Let $z = rz_0$. Claim:

1) z is in $\tilde{\mathcal{O}}(H) = S$

2) $\vartheta z = 1$, hence S is H-tame.

Claim 2) is obvious: $\vartheta z = (\vartheta_0/r)(rz_0) = \vartheta_0 z_0 = 1$. To prove claim 1), first note that since $H_0 \subseteq H$, $H^* \subseteq H_0^*$ (linear duals over R). We have $H = H^* \cdot \vartheta$, so for any ξ in H, there exists f in H^* with $\xi = f \cdot \vartheta$. To show z is in S, we need to show that for any ξ in H, ξz is in $\mathcal{O}_L$, the valuation ring of L. But $\xi z = (f \cdot \vartheta)z = (f \cdot (\vartheta_0/r))(rz_0) = (f \cdot \vartheta_0)z_0$. Now since f is in $H^* \subseteq H_0^*$, $f \cdot \vartheta_0$ is in H_0, and since z_0 is in $\tilde{\mathcal{O}}(H_0)$, $(f \cdot \vartheta_0)z_0$ is in $\mathcal{O}_L$. Thus ξz is in $\mathcal{O}_L$, and z is in $\tilde{\mathcal{O}}(H)$. ∎

COROLLARY 2.4. If L/K is a Galois extension of local fields with Galois group G and L/K is tamely ramified, then for every Hopf order H in KG, $\tilde{\mathcal{O}}(H)$ is free over H and $H = \mathcal{A}(\tilde{\mathcal{O}}(H))$.

This follows immediately from Theorem 2.3 and the fact that any Hopf order in KG contains RG (because the dual of any Hopf order in KG is contained in the maximal order of KG^*, namely RG^*). ∎

3. KUMMER THEORY OF FORMAL GROUPS

In this section we describe a large class of extensions of a local field K which have orders whose Leopoldt orders are Hopf.

The extensions are called Kummer extensions with respect to a formal group. Classical cyclic Kummer extensions of prime power order may be described from this point of view, as we will show.

Fix a prime p, and let K be a local field, a finite extension of $\mathbf{Q}_p$. Let R be the valuation ring of K, with maximal ideal m generated by π. Let $\bar{K}$ be an algebraic closure of K, and let $\bar{R}$ be the integral closure of R in $\bar{K}$, with maximal ideal $\overline{m}$. A formal group $F = F(x,y)$ of dimension one defined over R is a power series in two variables with coefficients in R so that the operation $\alpha +_F \beta = F(\alpha, \beta)$ for any α, β in $\overline{m}$ makes $\overline{m}$ into an abelian group with identity element 0. A homomorphism $f : F \to G$ from one formal group of dimension one to another is a power series $f = f(x)$ in $R[[x]]$ so that for any α, β in $\overline{m}$, $f(\alpha +_F \beta) = f(\alpha) +_G f(\beta)$. We denote $\overline{m}$ with operation $+_F$ by $F(\bar{K})$. For any extension L of K contained in $\bar{K}$, $F(L)$ is defined similarly.

Unreferenced notation and facts about formal groups are from Fröhlich [F68].

There is a map $[\ ] = [\ ]_F : \mathbf{Z} \to \mathrm{End(F)}$ given by $[0] = 0$, $[1](x) = x$, $[-1](x)$ is defined by $F(x, [-1](x)) = 0$, and for any n,

$$[n+1](x) = F([n](x), x) \qquad (n > 0)$$

$$[n-1](x) = F([n](x), [-1](x)) \qquad (n < 0).$$

The formal group F has finite height if the power series $[p](x)$ is non-zero modulo m.

Given formal groups F and G of dimension one and finite height defined over R, and a homomorphism $f : F \to G$, we may define an R- Hopf algebra H by $H = R[[x]]/(f(x))$. Here the counit map ϵ is the algebra homomorphism induced by sending x to 0; the antipode is the algebra homomorphism induced by sending x to $[-1]_F(x)$, and the comultiplication map Δ is the algebra map from H to $H \otimes_R H$ induced by sending x to $F(x \otimes 1,\ 1 \otimes x)$.

To see that Δ is well-defined, we define Δ in the same way from $R[[x]]$ to $R[[x]]\hat{\otimes}R[[x]]$ and show that $(f(x))$ is mapped to $(f(x)) \otimes R[[x]] + R[[x]] \otimes (f(x))$ (that is, $(f(x))$ is a coideal). Thus it suffices to show that $\Delta(f(x))$ is in the ideal generated by $f(x) \otimes 1 = f(x \otimes 1)$ and $1 \otimes f(x) = f(1 \otimes x)$. But if we write $x \otimes 1$ as y and $1 \otimes x$ as z, then $R[[x]]\hat{\otimes}R[[x]] \cong R[[y,z]$, and $\Delta(x) = F(y,z)$. We then have

$$\Delta(f(x)) = f(F(y,z)) = G(f(y), f(z)).$$

Since $G(y,z)$ has no constant term, $G(f(y), f(z))$ is in the ideal generated by $f(y)$ and $f(z)$, as we wished to show.

Let $A = K \otimes_R H$.

If f has height h, that is, Weierstrass degree $q = p^h$, then by the Weierstrass preparation theorem, $f = f_0 \cdot u$, where f_0 is a Weierstrass polynomial of degree q and u is an invertible power series. Then, since f has no multiple roots, ([F68], p.107-8) $H \cong R[x]/(f_0(x))$ is a free R-module of rank q and Γ, the set of roots of f_0 in $\overline{m}$, is a subgroup of $F(\bar{K})$ of order q.

Following Taylor [T86], we define the Kummer order

$$S_c = R[[z]]/(f(z) - c)$$

for any c in m . As with H, S_c is a free R-module of rank q. We make S_c into an H-comodule algebra by defining the R-algebra homomorphism

$$\alpha : S_c \to S_c \otimes H \cong R[[z, x]]/(f(z) - c, f(x))$$

to be the homomorphism induced by sending z to $F(z, x)$. Then α is well-defined, since

$$\alpha(f(z)) = f(F(z, x)) = G(f(z), f(x)) = G(c, 0) = c = \alpha(c).$$

THEOREM 3.1. For any c in m , S_c is an H-Galois object.

PROOF. It suffices to show that $T \otimes_R S_c$ is a $T \otimes_R H$-Galois object for some faithfully flat R-algebra T. For that, it suffices to find a faithfully flat R-algebra T so that $T \otimes_R S_c$ is isomorphic to $T \otimes_R H$ as $T \otimes_R H$-comodule algebras, for then $T \otimes_R S_c$ will be isomorphic as Galois object to the trivial $T \otimes_R H$-Galois object.

Let a in $\bar{K}$ be a root of $f(x) - c$, and let $L = K[a]$, T the valuation ring of L with maximal ideal m_T generated by π_T. Define an algebra homomorphism γ from $T \otimes_R H \cong T[[x]]/(f(x))$ to $T \otimes_R S_c \cong T[[t]]/(f(t) - c)$ induced by sending x to $t -_F a$. Then $0 = f(x)$ is sent by γ to

$$\begin{aligned} f(t -_F a) &= f(F(t, [-1]_F(a)) \\ &= G(f(t), [-1]_G(f(a)) \\ &= G(c, [-1]_G(c)) \\ &= 0. \end{aligned}$$

Thus γ is a well-defined T-algebra homomorphism. To show that γ is a $T \otimes H$-comodule homomorphism, we show $\alpha \circ \gamma = (\gamma \otimes 1) \circ \Delta$ as maps from $T \otimes_R H$

to $(T \otimes S_c) \otimes_T (T \otimes H)$. We write $T \otimes H$ as the image of $T[[x]]$ and $(T \otimes S_c) \otimes_T (T \otimes H)$ as the image of $T[[t,x]]$. Now

$$\alpha \circ \gamma(x) = \alpha(t -_F a) = \alpha(F(t, [-1]_F(a)))$$

$$= F(\alpha(t), [-1]_F(a))$$

$$= F(F(t,x), [-1]_F(a)),$$

while

$(\gamma \otimes 1) \circ \Delta(x) = (\gamma \otimes 1)F(x \otimes 1,\ 1 \otimes x)$ in $(\gamma \otimes 1)(R[[x \otimes 1,\ 1 \otimes x]])$. Now $(\gamma \otimes 1)(x \otimes 1)$ is the image in $(T \otimes S_c) \otimes_T (T \otimes H)$ of $t -_F a$ in $T[[t,x]$, and $(\gamma \otimes 1)(1 \otimes x)$ is the image of x. So we have

$$(\gamma \otimes 1)F(x \otimes 1,\ 1 \otimes x) = F(t -_F a, x)$$

$$= F(F(t, [-1]_F(a)), x))$$

which, using the associativity and commutativity of F, is the same as $\alpha \circ \gamma(x)$. Thus the map γ is a $T \otimes H$-comodule homomorphism. ▮

We can also use the map γ to show that S_c is isomorphic to $H^* = \mathrm{Hom}_R(H, R)$ as H^*-modules, and we give an explicit Galois generator for S_c:

COROLLARY 3.2. S_c is a free H^*-module on the image in S_c of t^{q-1} in $R[[t]]$.

PROOF. Let I be the free rank one R-module of integrals of H. Since R is local and H is commutative and cocommutative we know that H is isomorphic to H^* as H^*-modules, with $H = H^*j$ where j is any generator of I. However, since $H = R[[x]]/(f(x))$ and $\epsilon(x^k) = 0$ for all $k > 0$, an easy calculation shows that $f(x)/x$ is a generator of I.

Viewing the situation over the faithfully flat R-algebra T, we now see that $T \otimes_R H$ is a free $T \otimes_R H^*$-module with generator $f(x)/x$. Since γ is an isomorphism of $T \otimes_R H$-comodules (i.e. $T \otimes_R H^*$-modules), $T \otimes_R S_c$ is isomorphic to $T \otimes_R H^*$ as a $T \otimes_R H^*$-module and is generated by the image in $T \otimes_R S_c$ of $\gamma(f(x)/x)$ in $T[[t]]$.

Let $w(x) = f(x)/x$. Then $\gamma(f(x)/x) = w(\gamma(x)) = w(F(t, [-1](a))$. Since $f(x)$ has Weierstrass degree q, $w(x) \equiv x^{q-1} (\mathrm{mod}\, \pi)$ and so $\gamma(f(x)/x) \equiv F(t, [-1](a))^{q-1} \equiv t^{q-1} (\mathrm{mod}\, \pi_T)$.

Let $\psi = \gamma(f(x)/x)$ in $T[[t]]$. If $\{b_1, \ldots, b_q\}$ is a T-basis of $T \otimes_R H^*$, then $\{b_1\psi, \ldots, b_q\psi\}$ is a T-basis of $T \otimes_R S_c$. This also yields a $T/\pi_T T$-basis of $T \otimes_R S_c/\pi_T T \otimes_R S_c$. But then $\{b_1 t^{q-1}, \ldots, b_q t^{q-1}\}$ also is a set in $T \otimes_R S_c$which reduces modulo $\pi_T T$ to a $T/\pi_T T$-basis of $T \otimes_R S_c/\pi_T T \otimes_R S_c$. So by Nakayama's Lemma, $\{b_1 t^{q-1}, \ldots, b_q t^{q-1}\}$ is also a T-basis for $T \otimes_R S_c$. Hence $T \otimes_R S_c = T \otimes_R H^* t^{q-1}$, and since T is a faithfully flat R-algebra, $S_c = H^* t^{q-1}$. ▮

COROLLARY 3.3. $S_c = \tilde{O}(H^*)$ and $H^* = \mathcal{A}(S_c)$.

This follows from Theorem 2.2. ▮

If we apply Weierstrass preparation to $f(t) - c$, we may write $f(t) - c = g(t)v(t)$, $g(t)$ a Weierstrass polynomial of degree q, and $v(t)$ an invertible power series. Then $S_c \cong R[t]/(g(t))$ as R-algebras. This identification confuses the H-comodule structure, however.

Now we consider special cases.

♣ Suppose $g(t)$ is irreducible over K. Then L_c is a field extension of K. If Γ, the set of roots of $f(x)$ in $\overline{m}$, is contained in K, then L_c is a (classical) Galois extension of K with Galois group G isomorphic to Γ. This follows because of

PROPOSITION 3.4. If the roots Γ of $f(x)$ are in K, then $A = K[[x]]/(f(x)) \cong K^\Gamma$. Hence L_c is a Galois extension of K, where the Galois group $G \cong \Gamma$ acts on L_c by translating (under $+_F$) the generator t of L_c by elements of Γ.

PROOF. Since $f_0(x)$ splits in K, $A \cong K[x]/(f_0(x)) \cong K^G$ where G is a set in $1-1$ correspondence with the roots of $f_0(x)$, that is, with the elements of Γ, and the map $\varphi : A \to K^G$ is induced by $\varphi(x)(s_g) = g$ for $g \in \Gamma$ and s_g the element of G which corresponds to g. Then φ may be viewed as corresponding to a pairing

$$<>: G \times A \to K$$

by

$$s_g \times m(x) \to < s_g, m(x) > = m(g)$$

where $m(X)$ is a polynomial in $R[X]$. Then the comultiplication on A defines a multiplication on G by

$$\begin{aligned} < s_g s_h, x > &= < s_g \otimes s_h, \Delta(x) > \\ &= < s_g \otimes s_h, F(y,z) > \end{aligned}$$

(identifying $A \otimes A$ as the image of $R[[x]]\hat{\otimes}R[[x]] \cong R[[y,z]]$)

$$= F(< s_g, y >, < s_h, z >)$$

$$= g +_F h$$

$$=< s_{g+_F h}, x > .$$

Thus the multiplication on G is that induced on G from the formal group multiplication on $\Gamma \subseteq F(\bar{K})$.

In case $A \cong K^{\Gamma}$, the action of the Galois group G on L_c is induced by translating the generator t by elements of Γ. To see this, observe that since $L_c = K[[t]]/(f(t) - c)$ is a K^G-Galois object, then L_c is a Galois extension of K with group G. The action of G on L_c is induced from the coaction map

$\alpha : L_c \to L_c \otimes A$, where $A = K[[x]]/(f(x))$ and $\alpha(t) = F(t, x)$, by

$$s_g \cdot t = F(t, < s_g, x >) = F(t, g) = t +_F g$$

for g in Γ corresponding to s_g in G. Thus G acts on the generator t of L_c by translating t by the roots of $f(x)$. ∎

♣ If $c \in m_K, c \notin m_K^2$, then $S_c = \mathcal{O}_{L_c}$. For the Newton polygon $N(f(x) - c)$ of $f(x) - c$ and $N(g(x))$ agree to the left of $(q, 0)$. Since $N(f(x) - c)$ has a vertex at $(0, v(c))$, so does $N(g(x))$. But then $v(g(0)) = v(c)$, and so $g(0) \in m_K, \notin m_K^2$, and $g(x)$ is Eisenstein. Therefore $S_c = \mathcal{O}_{L_c}$. If π is a generator of m_K, then c is in m_K and not in m_K^2 iff $c = u\pi$ for some u in R^*.

The intersection of these special cases gives our main local Galois module result.

THEOREM 3.5. Let F, G be formal groups of dimension one, Γ a finite subgroup of $F(K)$, $f : F \to G$ a homomorphism with kernel $= \Gamma$. Let m_K be generated by π. Then for any unit u of $\mathcal{O}_K$, $L = K[[z]]/(f(z) - u\pi)$ is a Galois field extension of K with group $\cong \Gamma$, and $\mathcal{O}_L = R[[z]]/(f(z) - u\pi)$ is a free rank one module over its associated order $\mathcal{A} = \mathcal{A}(\mathcal{O}_L)$, where $\mathcal{A}^* \cong R[[x]]/(f(x))$. ∎

Adapting methods of Lubin [$Lu79$] (see Example 4.5 below), a large number of examples of Hopf algebras H of the form described in the theorem may be constructed from congruence-torsion subgroups of formal groups, as is shown in [$CZ93$].

To explain the terminology, "Kummer extension with respect to the formal group F", we conclude this section by specializing F to the multiplicative formal group $\mathbf{G}_m$.

PROPOSITION 3.6. Let $F = G = \mathbf{G}_m$, the multiplicative formal group defined as $\mathbf{G}_m(x, y) = x + y + xy$. Let $q = p^n$ and consider the endomorphism $[q] : \mathbf{G}_m \to \mathbf{G}_m$. Suppose K contains a primitive q th root of unity. Then the Kummer extensions of K with respect to $\mathbf{G}_m$ corresponding to $f = [q]$ are classical Kummer extensions with Galois group C_q cyclic of order q.

PROOF. We consider $H = R[[x]]/([q](x))$. It is easy to see by induction that for any $m > 0$, $[m](x) = (x+1)^m - 1$, so

$$\begin{aligned} H = R[x]/([p^n](x)) &= R[x]/((x+1)^q - 1) \\ &= R[y]/(y^q - 1) \\ &\cong RC_q, \end{aligned}$$

the group ring of the cyclic group of order q, as R-algebras, where $y = x + 1$. This last isomorphism is in fact as Hopf algebras, for

$$\begin{aligned} \Delta(y) &= \Delta(x+1) = \Delta(x) + \Delta(1) \\ &= (x \otimes 1 + 1 \otimes x + x \otimes x) + 1 \otimes 1 \\ &= (x+1) \otimes (x+1) \\ &= y \otimes y \end{aligned}$$

so the generator y of H is grouplike.

Given any c in m, $S_c = R[t]/([q](t) - c) = R[z]/(z^q - (1+c))$, where $z = t + 1$. Since $c \in m$, then $1 + c$ is a unit of R.

Suppose K contains a primitive q th root of unity ζ. Then

$$\Gamma = \{\zeta^r - 1 | r = 0, 1, \ldots, q-1\} \subseteq K$$

is the set of roots of $[q](x)$. So by Proposition 3.4, L_c is a Galois extension of K with group $G \cong \Gamma$, where if s_r in G corresponds to $\zeta^r - 1$ in Γ, then for the generator t of L_c,

$$\begin{aligned} s_r \cdot t &= \mathbf{G}_m(t, < s_r, x >) \\ &= \mathbf{G}_m(t, \zeta^r - 1) \end{aligned}$$

$$= t + \zeta^r - 1 + (\zeta^r - 1)t.$$

Hence

$$\begin{aligned} s_r \cdot z &= s_r \cdot t + 1 \\ &= \zeta^r t + \zeta^r = \zeta^r z \end{aligned}$$

and the Galois group G acts on the generator z by multiplication by q th roots of unity. Thus L_c is a Kummer extension of K with group $G = C_q$. ∎

4. DESCRIBING H^*

Let F be a formal group of dimension one and finite height defined over the valuation ring R of a local field $K \supseteq \mathbf{Q}_p$. Let m_K be the maximal ideal of R, $m_K = \pi R$ for some parameter π.

In the last section we showed that given a homomorphism f with domain F and an element c in m_K, the Kummer extension S_c is isomorphic to $H = R[[x]]/(f(x))$ as an H-comodule, hence $S_c \cong H^*$ as H^*-modules. Thus it is of interest to describe H^*. Taylor $[T85], [T87]$ has found a basis of H^* as an R-module when H arises from a Lubin-Tate formal group. In this section we extend this description.

Let $G \subseteq m_K$ be a finite group under the action of F: that is, for g_1, g_2 in G, $g_1 +_F g_2 = F(g_1, g_2)$. Let F_1 be a formal group and $f : F \to F_1$ be a homomorphism of formal groups with $\ker(f) = G$, then $H = R[[x]]/(f(x))$ is a Hopf R-algebra with comultiplication induced by F, and f will have height h where $p^h = q = \mid G \mid$. The Weierstrass Preparation Theorem yields a factorization of $f(x)$ as $f(x) = h(x)u(x)$, where $h(x)$ is a Weierstrass polynomial of degree q and $u(x)$ is an invertible element of $R[[x]]$. Then

$$h(x) = \prod_{g \in G} (x - g) \text{ in } R[x] \text{ and } H \cong R[x]/(h(x)).$$

Let Γ be an abstract group isomorphic to G, and let $\chi : \Gamma \to G \subseteq K$ be an isomorphism. Then $A = K \otimes_R H \cong K[x]/(h(x)) \cong K^\Gamma$, via the map

$$\alpha : K[x]/(h(x)) \to K^\Gamma$$

induced by $\alpha(p(x))(\gamma) = p(\chi(\gamma))$ for $p(x)$ in $K[x]$. The standard duality pairing $K^\Gamma \times K\Gamma \to K$ becomes $A \times K\Gamma \to K$ given by:

$$< p(x), k_\gamma \gamma > = \sum_{\gamma \in \Gamma} k_\gamma p(\chi(\gamma)) = \sum_{g \in G} k_{\chi^{-1}(g)} p(g).$$

We wish to identify the dual of H.

We begin with Euler's formula: if G is the set of roots of $h(x)$, then

$$\frac{1}{h(x)} = \sum_{g\in G} \frac{1}{h'(g)(x-g)}$$

(To prove this one verifies that the polynomial

$$\sum_{g\in G} \left(\frac{\frac{h(x)}{x-g}}{h'(g)} \right)$$

of degree $\leq q-1$ has the value 1 on all q elements of G, hence by the uniqueness in the Chinese Remainder Theorem, must be the constant polynomial 1.)

Following Taylor ([T85], Section 2), set $x = 1/T$ in Euler's formula and expand both sides as power series in T. If

$$h(x) = x^q + b_{q-1}x^{q-1} + \ldots + b_1 x$$

with all b_j in m_K, then the left side of Euler's formula becomes

$$\frac{1}{h(1/T)} = T^q\left(\frac{1}{1+b_{q-1}T+\ldots+b_1T^{q-1}}\right) = T^q + c_{q+1}T^{q+1} + \ldots$$

with all $c_j$in πR, while the right side,

$$\sum_{g\in G} \frac{1}{h'(g)(\frac{1}{T}-g)} = \sum_{g\in G} \frac{T}{h'(g)}(1+gT+g^2T^2+\ldots)\,.$$

Equating coefficients of the powers of T, we get

$$\sum_{g\in G} \frac{g^i}{h'(g)} = \begin{cases} 0 & \text{if } 0 \leq i < q-1 \\ 1 & \text{if } i = q-1 \\ c_{i+1} & \text{if } i > q-1, \text{ where } c_{i+1} \in \pi R \end{cases}$$

(where $g^0 = 1$ for all g in G, including $g = 0$). Using this formula, we have

PROPOSITION 4.1. The dual U in $K\Gamma$ of H is the R-submodule of $K\Gamma$ with basis

$$\{\sum_{\gamma\in\Gamma} \frac{\chi(\gamma)^i\gamma}{h'(\chi(\gamma))} \mid \ i = 0, 1, \ldots, q-1\} .$$

PROOF. Let $\{e_0, e_1, \ldots, e_{q-1}\}$ be the dual basis in $K\Gamma$ of the basis $\{1, x, x^2, \ldots, x^{q-1}\}$ of H. Then $U = \sum_{i=0}^{q-1} Re_i$. and $< e_i, x^j >= \delta_{i,j}$. Let

$$f_i = \sum_{\gamma\in\Gamma} \frac{\chi(\gamma)^i\gamma}{h'(\chi(\gamma))} .$$

Then

$$\begin{aligned}
< f_i, x^j > &= \sum_{\gamma\in\Gamma} \frac{\chi(\gamma)^i}{h'(\chi(\gamma))} < \gamma, x^j > \\
&= \sum_{\gamma\in\Gamma} \frac{\chi(\gamma)^i}{h'(\chi(\gamma))} \chi(\gamma)^j \\
&= \sum_{g\in G} \frac{g^{i+j}}{h'(g)} \\
&= \begin{cases} 0 & \text{if } i+j < q-1 \\ 1 & \text{if } i+j = q-1 \\ c_{i+j+1} & \text{if } i+j > q-1. \end{cases}
\end{aligned}$$

Then

$$\begin{aligned}
f_i &= \sum_{j=0}^{q-1} \langle f_i, x^j \rangle e_j \\
&= e_{q-1-i} + \sum_{j=q-i}^{q-1} c_{i+j+1}\ e_j ,
\end{aligned}$$

or

$$(f_0, f_1, \ldots, f_{q-1}) = (e_0, e_1, \ldots, e_{q-1})M$$

where M is the $q \times q$ matrix

$$\begin{pmatrix}
0 & 0 & \ldots & 0 & 0 & 1 \\
0 & 0 & & 0 & 1 & c_{q+1} \\
0 & 0 & & 1 & c_{q+1} & c_{q+2} \\
 & & \ldots & & & \\
0 & 1 & & & & \\
1 & c_{q+1} & \ldots & & & c_{2q-1}
\end{pmatrix} .$$

Since the matrix M is in $GL_q(R)$, $\{f_0, f_1, \ldots, f_{q-1}\}$ is a basis of U. ∎

The next proposition recovers Taylor's description in $[T87]$. Let v be the valuation on K, normalized so that $v(\pi) = 1$.

PROPOSITION 4.2. Suppose $h(x)$ has the property

(4.3) $h'(0) = b$ with $v(b) = r$, and $h'(x) = \pi^r u(x)$ with $u(x)$ invertible in H.

Then $\{\sigma_0,\ \sigma_1, \ldots, \sigma_{q-1}\}$ is a basis of U, where for each $i = 0, \ldots, q-1$,

$$\sigma_i = \frac{1}{\pi^r} \sum_{\gamma \in \Gamma} \chi(\gamma)^i \gamma.$$

PROOF. Since $u(x)$ is invertible in H, we may choose as a basis of H the set $\{\frac{1}{u(x)}, \frac{x}{u(x)}, \ldots, \frac{x^{q-1}}{u(x)}\}$. Then

$$\begin{aligned}
\langle \frac{x^i}{u(x)}, \sigma_j \rangle &= \langle \frac{x^i}{u(x)}, \frac{1}{\pi^r} \sum_{\gamma \in \Gamma} \chi(\gamma)^j \gamma \rangle \\
&= \frac{1}{\pi^r} \sum_{\gamma \in \Gamma} \chi(\gamma)^j \frac{\chi(\gamma)^i}{u(\chi(\gamma))} \\
&= \sum_{\gamma \in \Gamma} \frac{\chi(\gamma)^{i+j}}{h'(\chi(\gamma))} \\
&= \sum_{g \in G} \frac{g^{i+j}}{h'(g)} \\
&= \langle f_i, x^j \rangle
\end{aligned}$$

So the matrix relating the dual basis of $\{\frac{x^i}{u(x)}\}$ with $\{\sigma_j\}$ is the invertible matrix M. Hence $\{\sigma_j | j = 0, \ldots, q-1\}$ is a basis for U. ∎

Suppose $H = R[[X]]/(f(X))$ where f is a homomorphism of formal groups from F to F_1, and $f(X) = h(X)u(X)$ where $h(X)$ is a Weierstrass polynomial of degree q and $u(X)$ is a unit in $R[[X]]$. Then $H \cong R[X]/(h(X))$. Let x be the image of X in H. When does $h(x)$ satisfy (4.3), namely, $h'(x) = h'(0)v(x), v(x)$ a unit in H? If $h(x) = h_1 x + h_2 x^2 + \ldots + h_{q-1} x^{q-1} + x^q$ and $h'(x) = h'(0)v(x)$ with $v(x)$ in $R[x]$, then, since $v(0) = 1,\ h_1 = h'(0)$ must divide q and $r h_r$ for all $r,\ 1 \leq r < q$. We conclude with three examples where (4.3) holds. The first is Taylor's $[T87]$.

EXAMPLE 4.4. Let F be a Lubin-Tate formal group defined over R which admits as an endomorphism $[\pi](x) = \pi x + x^q$, where $q = \mid R/\pi R \mid$. Then $R[x]/([\pi](x))$ is a Hopf R-algebra and $[\pi](x)$ clearly satisfies (4.3). Moreover, as Taylor points out and is easily seen by induction on n using the chain rule, $[\pi^n](x) = [\pi]([\pi^{n-1}](x)$ also satisfies (4.3).

On the other hand, if $f(x)$ and $g(x)$ are power series of finite heights whose corresponding Weierstrass polynomials satisfy (4.3), it need not follow that $(g \circ f)(x)$ has a Weierstrass polynomial which satisfies (4.3). (For an example, take $p = 3, f(x) = 3x + x^3 + x^4, g(x) = 3x + x^3$.)

EXAMPLE 4.5. Let F_t be a standard generic formal group of height h. This is a formal group defined over $\mathbf{Z}_p[[t_1, \ldots, t_{h-1}]]$ such that

$$[p](x) = pxu_0(x) + t_1x^pu_1(x) + \ldots + t_{h-1}x^{p^{h-1}}u_{h-1}(x) + x^{p^h}u_h(x)$$

where for each $i < h$, $u_i(x)$ is a unit in $\mathbf{Z}_p[[t_1, \ldots, t_i]][[x]]$, and $u_h(x)$ is a unit in $\mathbf{Z}_p[[t_1, \ldots, t_{h-1}]]$. See ([*Lu*79], p. 105). We may specialize F_t to a formal group F_a over R by replacing t_i by a_i in m_K for all $i = 1, \ldots, h-1$.

If we choose the a_i so that $v(a_i) \geq v(a_1)$ for all $i \geq 1$, then F_a will have height h and $[p]_{F_a}(x) = \sum b_ix^i$ with $v(a_1) = v(b_1) \leq v(b_i)$ for all i, $1 \leq i < p^h$. If $[p](x) = h(x)u(x)$ where $u(x)$ is a unit of $R[[x]]$ and $h(x) = \sum h_ix^i$ is a Weierstrass polynomial of degree p^h then $v(h_1) = v(b_1)$ and $v(h_i) \geq v(h_1)$ for $1 \leq i < p^h$, as is easily seen by writing $h(x) = [p](x)u^{-1}(x)$ and successively comparing coefficients of $1, x, \ldots, x^{p^h-1}$. Hence $R[x]/(h(x))$ is a Hopf R-algebra and $h(x)$ satisfies (4.3). Thus if $h(x)$ splits in K then H^* has a basis of the type described in Proposition 4.2.

EXAMPLE 4.6. Let F be a formal group of height h defined over $R \supseteq \mathbf{Z}_p$, and suppose the Newton polygon of $[p]_F$, $N([p])$, has a vertex at p. (By appropriate specialization of the generic formal group F_t of Example 4.5, such an F is easily constructed.)

Now by Lubin's Lemma (Lemma 4.1.2 of [*Lu*64], c.f. [*Z*88], p. 27), there exists an invertible power series $u(x)$ in $R[[x]]$ so that $u(F(u^{-1}(x), u^{-1}(y))) = F^u(x,y)$ has $[m]_{F^u}(x) = [m]_F^u(x) = u([m](u^{-1}(x))$ for all m in $\mathbf{Z}_p$, and $[\zeta]_{F^u}(x) = \zeta x$ for all ζ in the group μ_{p-1} of $p-1$st roots of unity in $\mathbf{Z}_p$. If $[p]_F(a) = 0$ for a in $m_{\bar{K}}$, then $[p]_{F^u}(u(a)) = 0$, and, since $u(x)$ is invertible in $R[[x]]$, the elements a and $u(a)$ have the same valuation. It follows that the Newton polygons of $[p]_F$ and of $[p]_{F^u}$ agree to the left of the abscissa p^h, since the slopes of the edges of the Newton polygon of $[p]_F$ to the left of p^h are the negatives of the valuations of the roots of $[p]_F$. In particular, the Newton polygon of $[p]_{F^u}$ will have a vertex at p iff it is so for $[p]_F$. So, without loss of generality, we shall assume that F has the property that $[\zeta]_F(x) = \zeta x$ for all ζ in μ_{p-1}.

By Lubin's Local Factorization Principle ([Lu79], p. 106), there exists a factorization $[p](x) = h(x)g(x)$ in $R[[x]]$ where $h(x)$ is a Weierstrass polynomial of degree p whose roots are 0 and the $p-1$ roots of $[p]$ in $\bar{K}$ whose valuation is equal to $-m$ where m is the slope of the edge joining $(1, v(p))$ and the vertex at p in the Newton polygon of $[p]$. In fact, $h(x)$ arises as a factor via the Weierstrass Preparation Theorem of a homomorphism $f : F \to F_1$ of formal groups, where F_1 is some formal group defined over R (as is f) and $\ker f$ = roots of $h(x)$ ([F68], Theorem 4, p. 112).

Now if $a \in m_{\bar{K}}$ is in $\ker f$, so is $[\zeta](a) = \zeta a$ for any ζ in μ_{p-1}, and $v(\zeta a) = v(a)$. Thus if a is a root of $h(x)$, then in $\bar{K}[x], h(x) = x\prod_{\zeta\in\mu_{p-1}}(x-\zeta a)$, hence $a^{p-1} = b$ in R and $h(x) = x^p - bx$. Then $H = R[[x]]/(f(x))$ is a Hopf R-algebra, and since $f(x) = h(x)u(x)$ for some invertible power series by Weierstrass preparation, $H \cong R[x]/(h(x))$ and $h(x) = x^p - bx$ satisfies (4.3). Thus if $h(x)$ splits in K, then $U = H^*$ has a basis as in Proposition 4.2.

5. HOPF GALOIS STRUCTURES

C. Greither and B. Pareigis ([GP87, p.245; [P90], p.84) have shown that the non-normal extension $\mathbf{Q}(2^{1/4})/\mathbf{Q}$ is a Hopf Galois extension for two different $\mathbf{Q}$-Hopf algebras. In this section we anticipate future research in local Galois module theory by elaborating on this example. We work locally, over $\mathbf{Q}_2$. Since x^4-2 is an Eisenstein polynomial, letting ω be a root of x^4-2, the valuation ring S of $L = \mathbf{Q}_2(\omega)$ is $S = \mathbf{Z}_2[\omega]$.

EXAMPLE 5.1. Let A_1, A_2 be the two $\mathbf{Q}_2$-Hopf algebras acting on L, and let $\mathcal{A}_i(S)$ be the Leopoldt order of S in $A_i, i = 1,2$. Then one $\mathcal{A}_i$ is a $\mathbf{Z}_2$-Hopf order and the other is not.

As Pareigis observes ([P90], p.85), field extensions L/K with more than one Hopf Galois structure are very common. For example, if L/K is a Galois extension with group $C_q, q = p^n$ with p an odd prime, then L/K has a unique Hopf Galois structure iff $n = 1$ (c.f. [Ch89] and [P90], section 5). Example 5.1 shows that choosing which Galois module structure to use on L/K relates to the attractiveness of the resulting local Galois module structure for L/K.

PROOF. The Hopf algebra $A_1 = \mathbf{Q}_2[c,s]/(c^2+s^2-1, cs)$ with comultiplication $\Delta(c) = c\otimes c - s\otimes s$, $\Delta(s) = c\otimes s + s\otimes c$. One sees that A_1 is contained in $\mathbf{Q}_2[i]C_4$, where C_4 is the cyclic group of order 4 generated by σ, as follows:

$$c = (\sigma+\sigma^3)/2, \quad s = i(\sigma-\sigma^3)/2.$$